# Relay Proxy

User Guide

Relay Proxy

Relay Proxy is a server software developed by DBL Technology.   Its main purposed is to facilitate the deployment of DBL's gateways in network environment that does not support NAT or blocks VoIP traffics.

## Two common issues encountered with VoIP deployment

Two major problems are encountered today with VoIP traffics.
1.   ISP is blocking VoIP traffics in order to protect the traditional telephone services.

    The rapid increase in the internet and intranet data bandwidth in the last two decades has triggered the rapid development and deployment of VoIP services.   This has greatly reduced the revenues of the traditional long distance services.   As a result, ISPs in certain countries are blockings VoIP traffics as shown in the diagram below.
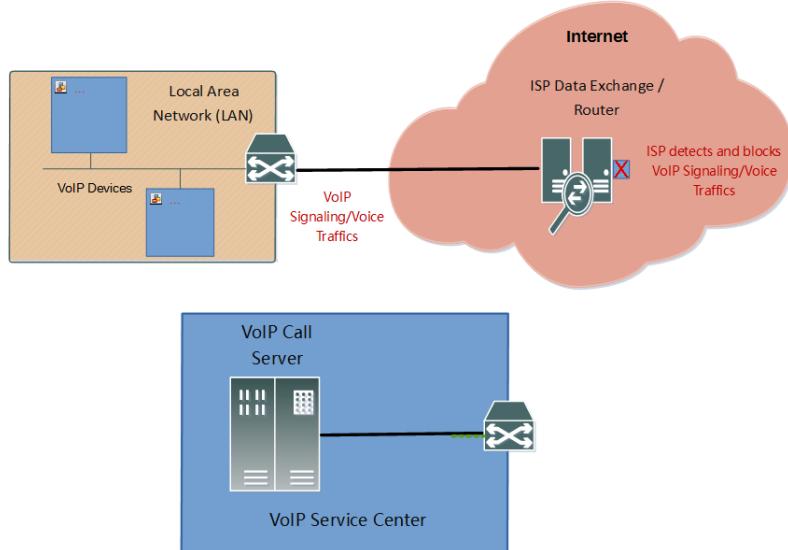

2.   VoIP traffics are not getting through due to the inability to support NAT in the Call Server when VoIP devices are installed behind a network router as shown in the diagram below.   Some VoIP Call Servers only support call signaling NAT.   This means that the VoIP device installed behind NAT can registered and make / receive calls.   However, when a call is established, only audio stream generated from the VoIP device can reach its destination.   As a result, the VoIP device end cannot hear any audio at all.
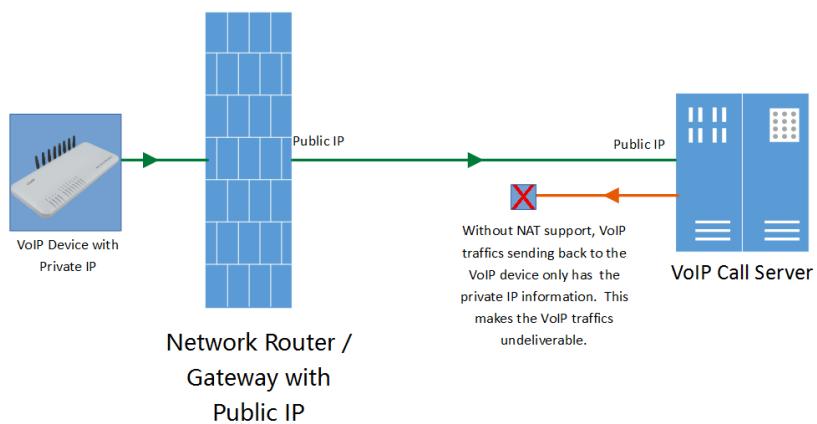
How can Relay Proxy solve both issues?

1. Relay Proxy establishes a virtual tunnel for both VoIP signaling and voice traffics with a very small increase in the data bandwidth.   This makes it more difficult for ISPs to block such data traffics.   To even protect the data traffics more, Relay Proxy also offers data encryption for both VoIP signaling and voice traffics.   The data traffics between Relay Proxy and VoIP Call Server are resumed to the standard VoIP data format.   Therefore, they must be installed in the same LAN network or an ISP network that does not block VoIP traffics.
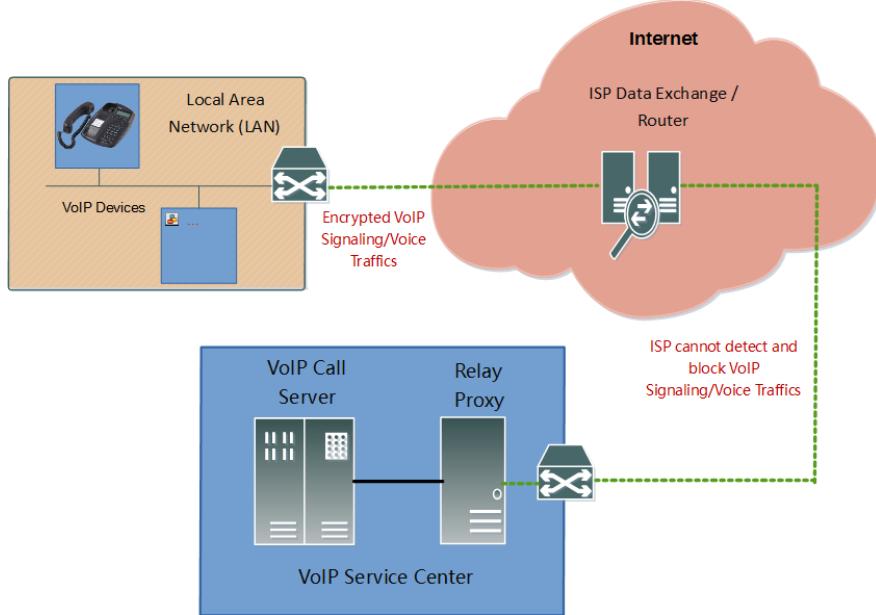
2. Relay Proxy solves the NAT issue by re-routing data traffics from VoIP devices to the VoIP Call Server and vice versa as shown in the diagram below.   All data packets now have the proper destination IP, so that they can be delivered.   In general, if SIP registration is not successful or one way audio occurs when a call is established, you can try to solve the problems with Relay Proxy.
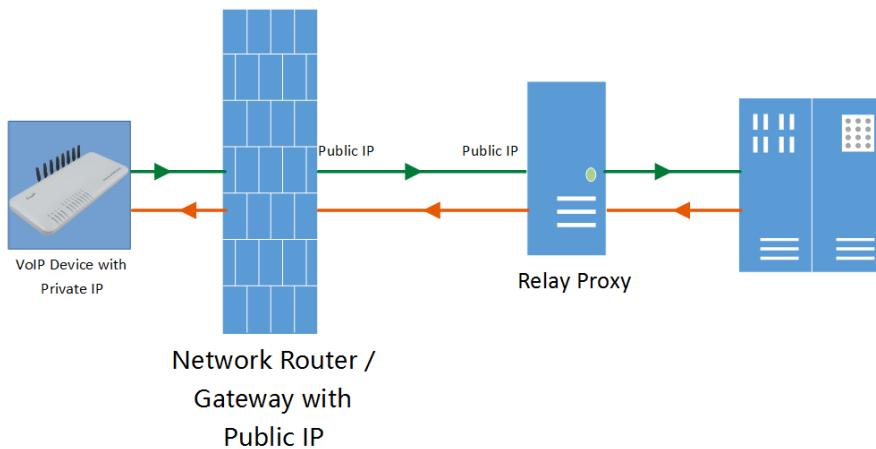
Installing Relay Proxy

1. PC hardware preparation

    Relay Proxy only supports Linux OS and it should run on most PC hardware today with good performance.   Relay Proxy has been tested for compatibility in the following Linux platforms.
    1)   RedHat
    2)   CentOS
    3)   Debian
    4)   Ubuntu

    For 64-bit OS, the following extended packages should be installed by issuing the command listed below.
    a) RedHat / CentOS
        yum install -y glibc.i686   zlib.i686   krb5-libs.i686

    b) Debian / Ubuntu
        dpkg --add-architecture i386
        apt-get update
        apt-get install lib32z1-dev
        apt-get install libgssapi-krb5-2:i386

2. Software Installation and Execution

    1)   Login to the root directory.
    2)   Type wget http://dbltek.com/update/relay_install-2.068.sh to download the Proxy Server Installation package
    3)   Type chmod 744   relay_install-2.068.sh to enable the installation property
    4)   Type ./ relay_install-2.068.sh to execute the installation script

    After the installation is completed
    5)   Type /root/relay/run_relaysrv to execute the Relay Proxy
    6)   Type /root/relay/run_sqlwebd to execute the Relay Proxy Web Interface

    Please note that a Relay Proxy startup script is installed to execute both Relay Proxy and its web interface when the hardware boots up.   For Dubian / Ubuntu platform, the startup script may not work properly.   If this occurs, please delete the line "exit 0" in the document /etc/rc.local.

3. Other commands

    1)   Killall relaysrv – type this to terminate the Relay Proxy.
    2)   Killall sqlwebd – type this to terminate the Relay Proxy web interface.

4. Default Ports

Relay Proxy uses the followings ports for both TCP and UDP communications. Please configure the server firewall accordingly.

    TCP   21080 , 1701 , 8089
    UDP   1701 , 5000~60000

Note: Please contact technical support at support@dbltek.com for assistance if needed.

Configuring Relay Proxy

1. To configure the Relay Proxy, you need to access its web interface shown below.
   ➢ Type http://<server hardware IP>:8089
   ➢ Enter "admin" as the login ID
   ➢ Enter "admin" as the login password

<p align="center">Relay Proxy configuration</p>

<p align="center">Relay Proxy Manage v1.0</p>

Agent	Username		
db1	db1	Delete	Modify

<p align="center">Add</p>

2. Click on Relay Proxy configuration to configure the Relay Proxy.

<p align="center">Relay Proxy Configuration</p>

RELAY PORT	21080
UDP PORT	1701
TCP PORT	1701
Parameter	With Sqlite authentication ∨

Save   SaveReboo   Cancel

<p align="center">Web Server Configuration</p>

Web Port	8089
Username	admin
Password	dbladmin

Save   SaveReboo   Cancel

Relay Proxy Configuration
   ➢ Modify the Relay Port, UDP Port, TCP Port if needed.
   ➢ Parameters:
      1) Default – No authentication
      2) Sql Authentication – Reserved for testing.
      3) Sqlite Authentication – Using SQLite database for authentication (choose this one by default)

4) Listen Localhost – Reserved for other use.

➢ Press [Save] to save the changes (not effective yet).

➢ Press [SaveReboo] to save and make the changes effective immediately. Browser displays a warning message of not be able to access the webpage. Please wait i10 seconds and then reload the webpage.

3. Click [Add] to add a new login account. Enter the fields as required and then click "Add" to complete. Agent is used to classify the user accounts only and it is not required for GoIP configuration. In addition, the same Username is allowed for multiple logins. This means that you can use the same account to configure all your devices to login to the same Relay Proxy.

Add User

Agent	ZhangSan
Username	user1
Password	password

[Add] [Cancel]

The default test account is "dbl". To delete an unwanted account, please click [Delete] (on the right hand side of the account name) to delete the corresponding account.

Relay Proxy configuration

Relay Proxy Manage v1.0

Agent	Username	
db1	db1	[Delete] [Modify]

[Add]

Configuring DBL's VoIP devices

Please note that all VoIP devices developed by DBL supports Relay Proxy. Either or both VoIP Signaling data and VoIP voice stream can be configured to connect to Relay Proxy.

1. Configuring VoIP Signaling data to use Relay Proxy
VoIP signaling is referring to the IP protocol used for VoIP Call establishment and management. Depending on your device, the location for its configuration varies. For GoIP, it is located under the "Advanced VoIP" as shown in the two figures below.

Locate the parameter "Signaling NAT Transversal" and select "Relay Proxy". Then the following additional parameters are displayed.

➢ Address – enter the IP address or domain name of the Relay Proxy

➢ Port – enter the **Relay Port** as configured in the Relay Proxy

➢ User – enter the username that is created for your device

➢ Password – enter the password that is defined for the username

➢ Click on the check box to enable encryption if it is required. Please note that additional network bandwidth is required if encryption is enabled.

Status	**Advance SIP**	
	SIP Listening Port Mode	Fixed ▼
Configurations	Port	5060
	SIP INVITE Response	SIP 183 ▼
Preferences	SIP Busy Code	503
Network	Call OUT PSTN Auth Mode	IP ▼
Basic VoIP	Bulit-in SIP Proxy	○ Enable ● Disable
Advance VoIP	NAT Keep-alive	● Enable ○ Disable
Media	DTMF Signaling	Inband ▼
Call Out	Signaling QoS	None ▼
	Signaling Encryption	None ▼
Call Out Auth	Signaling NAT Traversal	Relay Proxy ▼
Call In	Address	202.104.186.90
Call In Auth	Port	21080
SIM	User	user1
	Password	••••••••
Running Rule		☑ Encryption
SIM Forward	Backup Relay Server 1	
IMEI	Backup Relay Server 2	
SMS	Backup Relay Server 3	
GSM Carrier	Backup Relay Server 4	
GSM Base Station		Advanced Timing>>
		GSM-SIP Code Map>>
Tools	Save Changes	

Call Settings

Endpoint Type	SIP Phone ▼	Advanced Settings<<	
Config Mode	Config by Line ▼	SIP Local Port Mode	Fixed ▼
● Line 1 ○ Line 2 ○ Line 3 ○ Line 4		Signaling Port	5060
Phone Number	149	Bulit-in SIP Proxy	○ Enable ● Disable
Phone Number 2		NAT Keep-alive	● Enable ○ Disable
Display Name		Virtual Ringback	○ Enable ● Disable
SIP Proxy	192.168.2.2	Reigster Mode	Mode 1 ▼
SIP Registrar Server	192.168.2.2	Advanced Timing>>	
Register Expiry(s)	60	DTMF Signaling	Outband ▼
Outbound Proxy		Outband DTMF type	RFC 2833 ▼
Home Domain		RTP Payload Type	101
Authentication ID	149	Signaling QoS	None ▼
Password	•••	Signaling Encryption	None ▼
Dial Plan	18:+9	Signaling NAT Traversal	Relay Proxy ▼
Call Forward Type	Not Forward ▼	Address	202.104.186.90
Call Forward Number		Port	21080
Backup Server	○ Enable ● Disable	User	user1
Fax Line>>		Password	••••••••
		☑ Encryption	
		Backup Relay Server 1	
		Backup Relay Server 2	
		Backup Relay Server 3	
		Backup Relay Server 4	
		Media Settings<<	
		RTP Port Range	16384 - 32768
		PacketLength(ms)	30
		Jitter Buffer	Fixed ▼
		Delay(ms)	60
		Media QoS	None ▼
		Media Encryption	None ▼
		☑ Symmetric RTP	
		Media NAT Traversal	Relay Proxy ▼
		Address	202.104.186.90
		Port	21080
		User Name	user1
		Password	••••••••
		☑ Encryption	
		Relay Mode	1 ▼
		Backup Relay Server 1	
		Backup Relay Server 2	
		Backup Relay Server 3	
		Backup Relay Server 4	
		Audio Codec Preference>>	

2. Configuring VoIP voice stream to use Relay Proxy

When a VoIP call is established, voice stream are sent between the two VoIP devices. To configure the voice stream to use the Relay Proxy, please access your device webpage and then look for the "Media" as shown in the figure below or "Media Settings" as shown in the figure in the previous page.

Locate the parameter "Media NAT Transversal" and select "Relay Proxy". Then the following additional parameters are displayed.

> Address – enter the IP address or domain name of the Relay Proxy
> Port – enter the **Relay Port** as configured in the Relay Proxy
> User – enter the username that is created for your device
> Password – enter the password that is defined for the username
> Click on the check box to enable encryption if it is required. Please note that additional network bandwidth is required if encryption is enabled.

Status	**Media**	
	RTP Port Range	16384 - 32768
Configurations	PacketLength (ms)	20
	Jitter Buffer	Fixed
Preferences	Delay (ms)	60
Network	Media QoS	None
Basic VoIP	Media Encryption	None
Advance VoIP		☐ Symmetric RTP
Media	Media NAT Traversal	Relay Proxy
Call Out	Address	202.104.186.90
Call Out Auth	Port	21080
	User Name	user1
Call In	Password	••••••••
Call In Auth		☑ Encryption
SIM	Relay Mode	1
Running Rule	Backup Relay Server 1	
SIM Forward	Backup Relay Server 2	
	Backup Relay Server 3	
IMEI	Backup Relay Server 4	
SMS	RTP Disconnect Detect(s)	0
GSM Carrier		Audio Codec Preference>>
GSM Base Station	Save Changes	