Remote User NAT Traversal

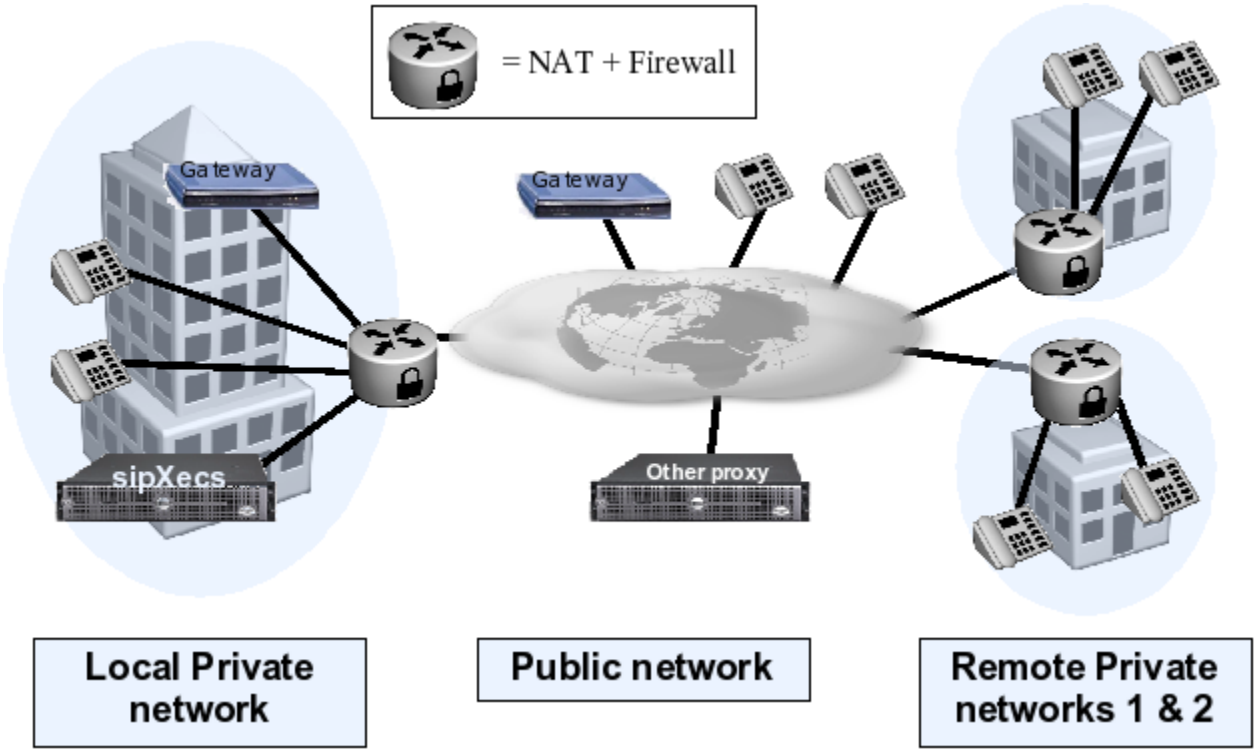
With the sipXecs 4.0 release comes a new capability generically called 'Remote User NAT traversal' that aims at compensating for far-end and near-end NATs that may be present between SIP endpoints and sipXecs. The purpose of this page is to describe the extents of that feature and describe how it is configured.

- Feature Description
  - Definitions
  - Assumptions, limitations and dependencies
- Configuring the Remote User NAT Traversal
  - Step 1 - Enabling the Remote User NAT Traversal feature
  - Step 2 - configuring public IP address of sipXecs
  - Step 3 - define your local private network topology
  - Step 5 - Create pinholes in Local NAT/Firewall to let signaling and media through
  - Step 6 - Configure Remote NATs
  - Step 7 - Configure the Remote Worker Phones
- Troubleshooting
  - General troubleshooting tips
  - Problem #1 - Remote worker cannot register with sipXecs
  - Problem #2 - Remote Worker registers but cannot make or receive calls
  - Problem #3 - Remote Worker registers and can make calls but media is blocked in one or both directions
- Annex 1 - FAQ
  - Q1- What is the distinction between remote NAT traversal and sipXbridge? Are they one and the same?
  - Q2- Can SipXBridge and the Remote User NAT Traversal feature be both enabled at the same time?
- Annex 2 - Known routers with SIP ALGs

This page does not cover the implementation details of the Remote User NAT Traversal feature. That information can be found here.

Feature Description

One of the key deployment scenarios for sipXecs is to install it inside an enterprise network and provide SIP-based telephony services to users that are connected directly on that enterprise network as well as users that are connecting remotely from their branch offices, homes, hotel rooms or other. At any of these sites, we are very likely to find a non-SIP-aware firewall/NAT that will prevent proper communication from occuring. The intent of the Remote User NAT Traversal feature is to enable unobstructed communication between sipXecs and remote users without requiring the help of SIP-aware NAT /firewalls or any external SBCs.



The network diagram above shows a sipXecs sitting in a private enterprise network behind a non-SIP-aware NAT/Firewall router and connecting to the public Internet. With the assistance of the Remote User NAT Traversal feature available in sipXecs 4.0, the following will be possible:

- Every phone in the figure will be capable of successfully registering with sipXecs;
- Every phone will be capable of calling every other phone on the network;
- All telephony features will be accessible, e.g. sim-ring, call forwarding, blind transfer, attended transfer, call pickup, conferencing, call park, paging, instant messaging, video calls, voicemail, auto-attendant, hung groups, MWI notifications and music-on-hold;

- Calls to and from gateways located on the local private network or the public network will be possible.

Note that the Remote User NAT Traversal feature is known to work with any NAT that falls into one of the following categories:

- Full cone NAT;
- Port Restricted NAT;
- Address Restricted NAT;
- Symmetric NAT.

Definitions

Before we get too deep into the details here, let's begin by defining some of the terms that will be used frequently within this page.

Term	Definition
NAT	Stands for Network Address Translator. Network device sitting at the interface between two networks. Through source IP address and port transformations, it is capable of hiding the addresses of the private network deployed behind it.
Local NAT	When sipXecs is deployed inside a private network, the NAT that is fronting that private network is called the Local NAT.
Local Private Network	Private network behind the Local NAT.
Near-End NAT	See Local NAT.
Remote NAT	When a SIP endpoint to be registered with sipXecs is deployed inside a private network that does not include sipXecs, the NAT that is fronting that private network is called the Remote NAT.
Remote Private Network	Private Network behind a Remote NAT.
Remote User	User of a SIP endpoint deployed inside a Remote Private Network.
Remote Worker	See Remote User.
Far-End NAT	See Remote NAT.
WAN-facing IP Address	With respect to a NAT, the WAN-facing IP address is the IP address that is assigned to the NAT's network interface that is facing the public network. Depending on the ISP, this IP address is either statically assigned or dynamically assigned via DHCP. Due to address transformations done in the NAT, this IP address is the address that all the IP endpoints located in the private network behind that NAT will appear to have when they send IP packets to destinations located on the WAN side.

Assumptions, limitations and dependencies

- When sipXecs is deployed behind a Local NAT, in order to be reachable from the public network, the NAT needs to be configured to relay UDP & TCP ports 5060 to the IP address of the sipXecs. Furthermore, the UDP port range utilized by the media relay function (30000-31000 by default) also needs to be relayed to the IP address of the sipXecs.
- This feature does not work for SIP endpoints that do not use symmetric ports for sending and receiving SIP messages. As such, Re-Invites sent for the purpose of performing target refresh operations break the signaling symmetry and in many cases will result in a failed call if the endpoint is located behind a NAT
- This feature does not attempt to provide any kind of topology hiding functionality. As such, SIP headers carrying private IP addresses that do not need to be manipulated to allow NAT traversal will remain untouched.
- This solution does not handle registrations that are made on behalf of another user agent. More specifically, a REGISTER needs to originate from the user agent that is actually registering.
- The only content type that the NAT traversal feature will understand and manipulate is application/sdp.
- This solution requires that endpoints register using an IP address as their contact information and not an FQDN. Registering against an FQDN is not supported and NAT traversal will be provided as best effort only.
- A sipXecs with NAT Traversal feature support cannot be used as a generic NAT traversal helper device for another non-NAT-traversal-enabled SIP Proxy.
- In order for Call Park and Call Pickup features to work through NATs,every phone in the system needs to be configured with sipXecs as its outbound proxy. This measure ensures that all INVITEs generated as a result of REFER processing are seen by sipXecs, even when the Refer-To: points to an IP address that is not the sipXecs.
- When deploying sipXecs in an HA configuration, in order for the NAT Traversal feature to work properly, the systems involved in the HA configuration cannot be separated by NATs.

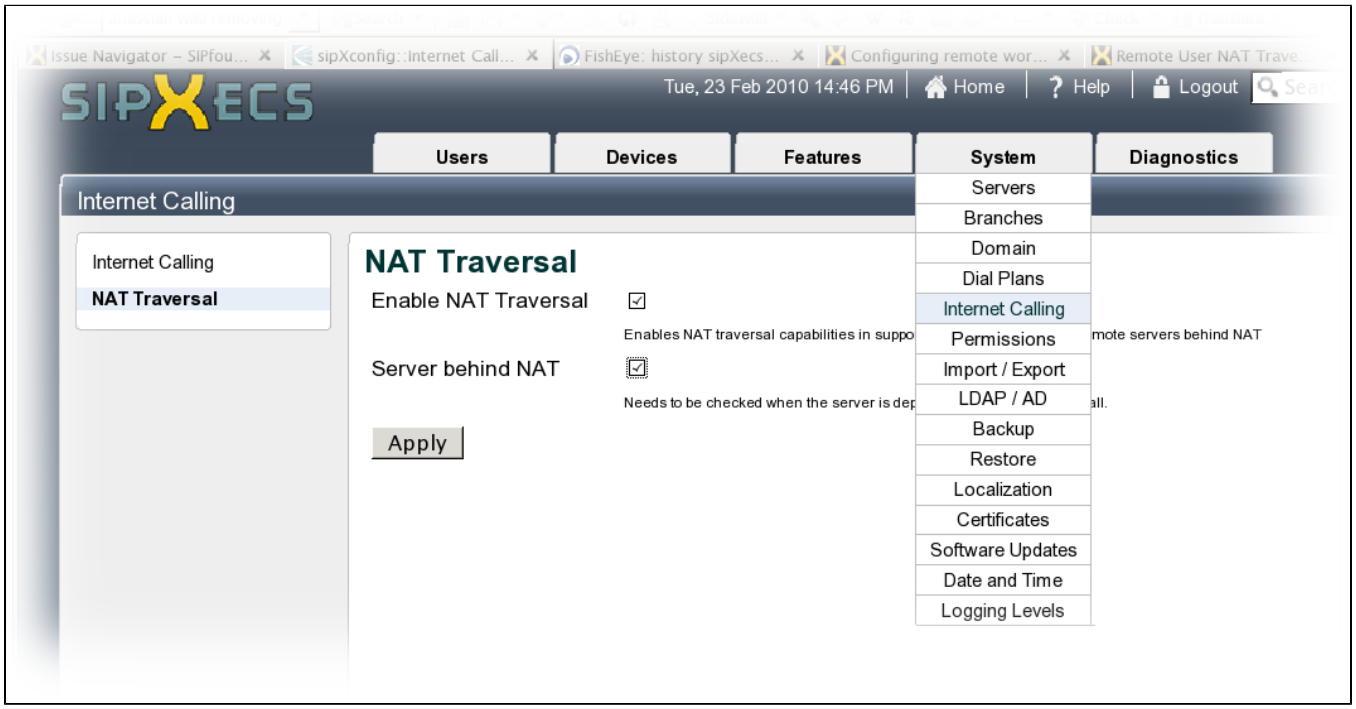
Configuring the Remote User NAT Traversal

In order to fully configure sipXecs to perform Remote User NAT Traversal, three different sipXconfig pages need to be visited and modified. This arrangement is arguably not as simple as it could be but we are hoping to improve this in a simplification effort that is slated post-4.2 release. This section will hand-hold you through the seven steps required to configure the feature.

Step 1 - Enabling the Remote User NAT Traversal feature

The purpose of this step is to turn on the Remote User NAT Traversal feature and tell it whether or not sipXecs is deployed behind a NAT. This is accomplished as follows. In sipXconfig, navigate to "System->Internet Calling->NAT Traversal" and:

- "Enable NAT Traversal": Check this box - this will effectively enable the Remote User NAT Traversal feature
- "Server behind NAT": If the sipXecs is deployed inside a private network, check this box (this internally enables the near-end NAT traversal logic), otherwise leave blank.



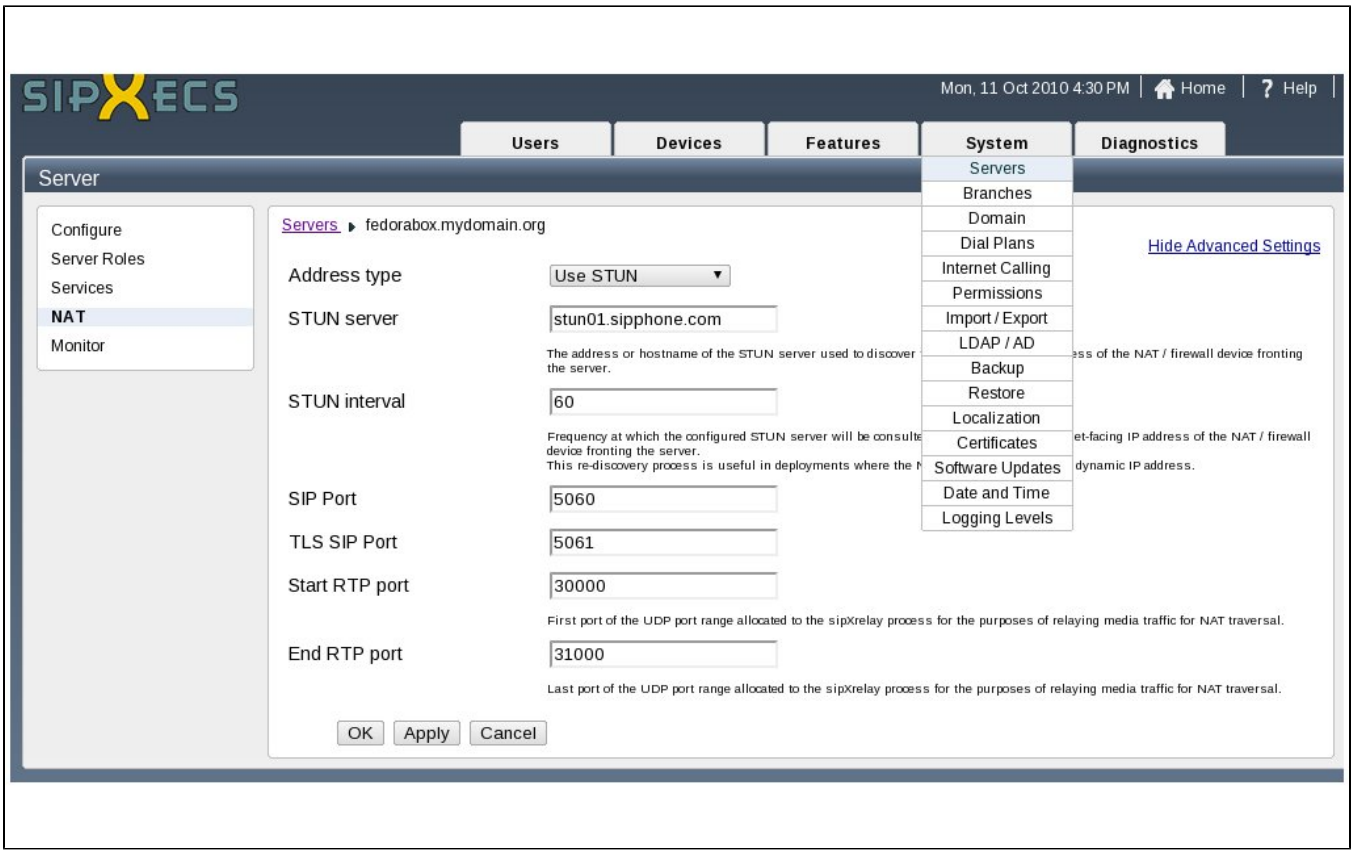
Step 2 - configuring public IP address of sipXecs

NOTE: This step is only required if the sipXecs is deployed inside a private network. If you left the 'Server behind NAT' checkbox unchecked in Step 1 above then you can skip steps 2 through 5 completely and move on to Step 6 immediately.

The purpose of this step is to tell the Remote NAT Traversal feature the Public IP, Signaling Port and Media Ports to advertise when talking with SIP endpoints that are not part of the local private network.

In sipXconfig, navigate to "System->Servers-><click on server>->NAT" and:

- If the WAN-facing IP address of the Local NAT is static then select "Specify IP address" and enter it under "Public IP Address". Instead, if the WAN-facing IP address is dynamic (i.e. your ISP changes it from time to time), select "Use STUN" and enter a STUN server address in the "STUN Server" field (stun01.sipphone.com is a somewhat reliable public STUN server that could be used here). If you are unsure, find out by asking your ISP and use 'Use STUN' until you get your definitive answer.
- Keep all other fields as defaults.



High Availability Consideration: If the sipXecs deployment is a High-Availability (HA) one, Remote NAT Traversal can still work but the HA brings about a few complexities with respect to step 2. Basically, Step 2 has to be repeated for each server found under "System->Servers" and each server must be configured with unique a 'SIP Port" value and non-overlapping RTP port ranges as defined by the 'Start RTP port' and 'End RTP port' fields found under the 'Advanced Settings". So for example, if the HA deployment has 3 servers, the following settings could be used:

1. sipXecs Server 1 has SIP Port of '5060' and RTP port range for [30000-31000[
2. sipXecs Server 2 has SIP Port of '11060' and RTP port range for [31000-32000[
3. sipXecs Server 3 has SIP Port of '12060' and RTP port range for [32000-33000[

Step 3 - define your local private network topology

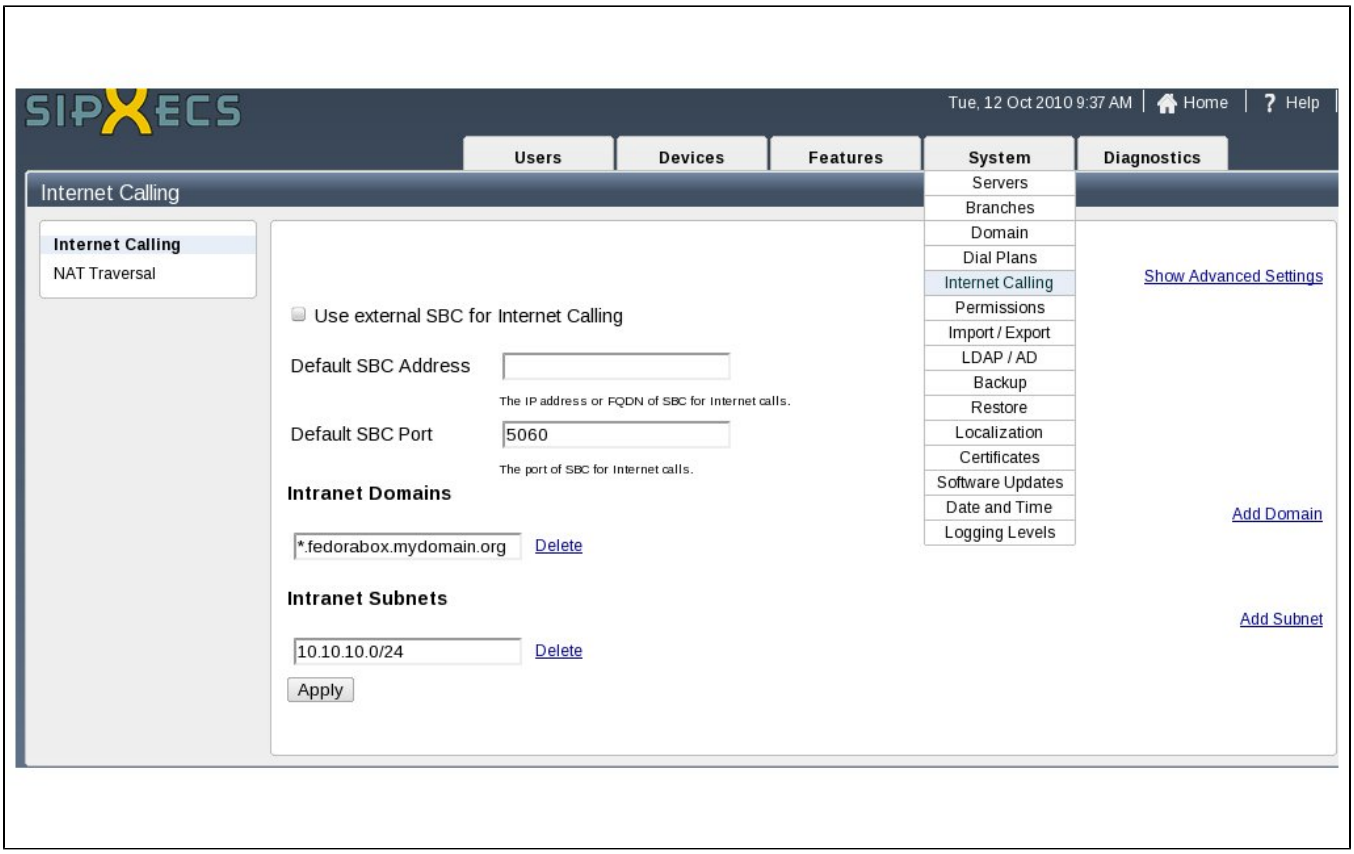
NOTE1: This step is only required if the sipXecs is deployed inside a private network. If you left the 'Server behind NAT' checkbox unchecked in Step 1 above then you can skip steps 2 through 5 completely and move on to Step 6 immediately.

NOTE2: Read this step carefully as it is often a source of problems in remote user deployments

The purpose of this step is to tell the Remote NAT Traversal feature the extent of the local private network that it is a part of. This information comes in handy when dealing with registration-less devices such as gateways and other sipXecs boxes.

In sipXconfig, navigate to "System->Internet Calling" and:

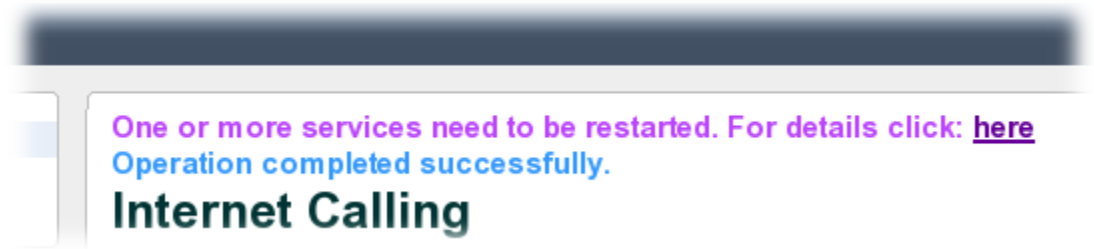
- Begin by deleting all the default entries in "Intranet subnets" as they are almost always wrong.
- In "Intranet subnets", add as many entries as required to describe the local private network that sipXecs is a part of. For example, if your sipXecs is part of the private network 10.10.10.0/24 then you need to have a single "Intranet subnets" entry of "10.10.10.0/24".
- In "Intranet Domains", the default provided is almost always all you need - leave it as is.
- [xecsuserV4r2:Important] Make sure that '**Use external SBC for Internet Calling**' check box is **disabled.** This setting may only be only useful when using a session border controller other than sipXbridge.



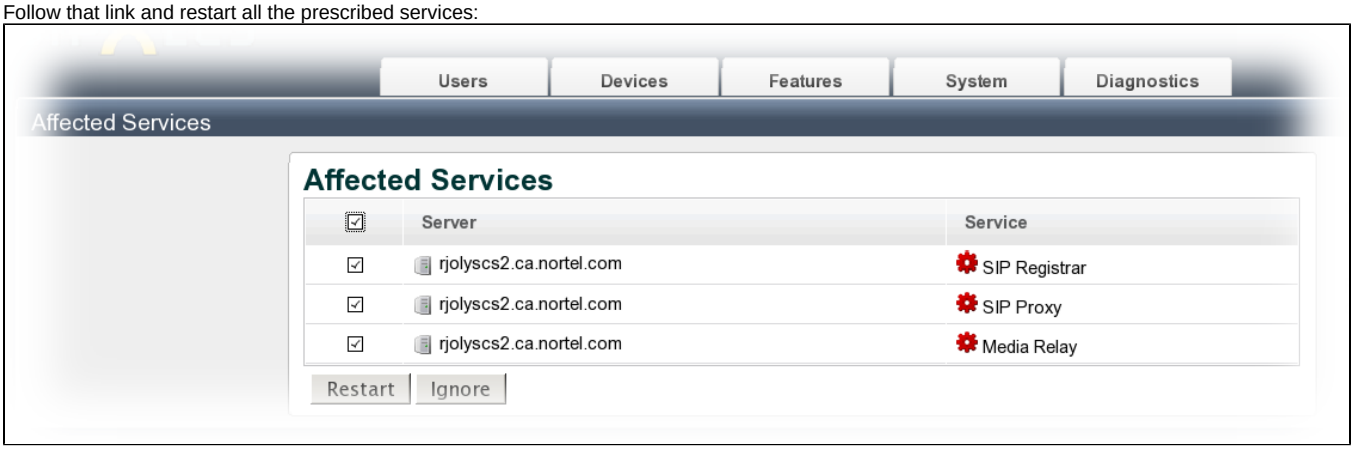
Step 4 - Restart the required services

NOTE: This step is only required if the sipXecs is deployed inside a private network. If you left the 'Server behind NAT' checkbox unchecked in Step 1 above then you can skip steps 2 through 5 completely and move on to Step 6 immediately.

Steps 1 through 3 have completely configured your sipXecs server(s) for Remote User NAT Traversal but some services need to be restarted in order for the new configuration to take effect. At the top of the page, you should see a purple banner informing you that some services need to be restarted:



Follow that link and restart all the prescribed services:



Step 5 - Create pinholes in Local NAT/Firewall to let signaling and media through

NOTE: This step is only required if the sipXecs is deployed inside a private network. If you left the 'Server behind NAT' checkbox unchecked in Step 1 above then you can skip steps 2 through 5 completely and move on to Step 6 immediately.

Now that we are done with configuring sipXecs, the focus shifts over to the Local NAT (and integrated firewall) that is fronting sipXecs. Basically, we need to create firewall rules and port forwarding rules to let the SIP traffic (signaling) penetrate and be forwarded to the sipXecs sitting in the private network. A similar exercise needs to be done for the RTP traffic (media) as well.

At this point, we do not have model-specific instructions to give, so only the general principles are going to be described here. As more people start adopting this feature, the hope is that we'll be able to build a database of known-to-be-working NATs along with the configuration required to make them work.

Log into your Local NAT management interface and:

- Disable any SIP ALG functionality in the Local NAT - such features are almost always incomplete and/or buggy and cause far more trouble than benefits.
- If the firewall is enabled, create a firewall rule that will allow TCP and UDP packets destined to the 'SIP Port' designated in Step 2.
- Create a port forwarding NAT rule that will forward TCP and UDP packets destined to the 'SIP Port' designated in Step 2 to the IP address of the sipXecs.
- If the firewall is enabled, create a firewall rule that will allow UDP packets destined to the range of ports created by the 'Start RTP port' and 'End RTP port' in step 2.
- Create a port forwarding NAT rule that will forward UDP packets destined to the port range formed by [Start RTP port - End RTP port'[to the IP address of the sipXecs.

High Availability Consideration: If the sipXecs deployment is a High-Availability (HA) one, firewall rules need to be created to allow each sipXecs server's SIP Port and RTP port range. Also, NAT forwarding rules must be created to forward each SIP Port and RT Port range to the IP address of their corresponding sipXecs. For example:

1. If sipXecs Server 1 has SIP Port of '5060' and RTP port range for [30000-31000[then ports 5060 and [30000-31000[must be allowed and forwarded to the IP address of Server 1.
2. If sipXecs Server 2 has SIP Port of '11060' and RTP port range for [31000-32000[then ports 11060 and [31000-32000[must be allowed and forwarded to the IP address of Server 2.
3. If sipXecs Server 3 has SIP Port of '12060' and RTP port range for [32000-33000[then ports 12060 and [32000-33000[must be allowed and forwarded to the IP address of Server 3.

Step 6 - Configure Remote NATs

For each remote NAT in the deployment, be sure to disable any SIP ALG functionality - such features are almost always incomplete and/or buggy and cause far more trouble than benefits.

Step 7 - Configure the Remote Worker Phones

For each remote user phone in the system, apply the following configuration on top of what is normally done to configure a SIP phone.

- Set proxy to the SIP domain of your sipXecs
- Configure the outbound proxy to be the WAN-facing address of the Local NAT (i.e. according to the definition, the NAT that is fronting the private network that sipXecs is a part of)
- Disable any NAT traversal technologies (STUN, ICE, ALGs, ...) inside the remote worker's phone as well as inside local and remote firewalls/NATs. Using Counterpath clients as an example, you would achieve this by selecting 'Use Local address' instead of 'discover global address' and uncheck 'Enable ICE'.

Troubleshooting

Deploying remote users for the first time can be a bit intimidating and sometimes things do not work 100% right out of the gate. This section will offer troubleshooting tips for the frequently encountered problems but before diving into specific problems, here is a set of troubleshooting tips that apply to any remote worker-related problem. Be sure to go through that checklist first before applying any of the more advanced troubleshooting techniques proposed in this section.

General troubleshooting tips

- Carefully review the configuration steps contained in this guide
- Phone's outbound proxy is configured with routable IP address associated with sipXecs and that address can be pinged from a machine inside the remote network
- Phone is configured with the proper SIP domain, SIP username and SIP password
- If sipXecs is behind a local NAT, ensure that the pinholes and port forwarding rules have been created as per configuration step #5.
- Verify that STUN and ICE (if supported) are disabled in the remote phone
- Verify that SIP ALGs are disabled in both the remote and local NATs
- Verify that the 'Use external SBC for Internet Calling' checkbox is unchecked in 'System->Internet Calling'

- Review the alarm history and look for reported NAT traversal-related failures. The alarm history can be found in sipXconfig under 'Diagnostics->Alarms->History'. Be sure to select a wide-enough date range to cover the last reboot of the box.

Problem #1 - Remote worker cannot register with sipXecs

- Go through the general troubleshooting tips found at the top of the 'Troubleshooting' section.
- Power down any other phone that is registering against the same SIP user as the problematic remote phone. As an example if the problematic remote phone is registering against SIP user 200@example.com and so does a local phone then that local phone should be turned off to keep logs unambiguous.
- Turn on DEBUG logging for the SIP Proxy and SIP Registrar. This can be done though sipXconfig by navigating to 'System->Logging Levels->Show Advanced Settings'. Once you have selected the DEBUG logging level, a purple banner will appear to restart those services much like what is shown in configuration step #4. Do restart the services
- Once the SIP Proxy and SIP Registrar are back to a running state, log into the sipXecs shell and execute the following command:

```
tail -f /var/log/sipxpbx/sipXproxy.log | grep "REGISTER sip" | grep  "<user>@<SIP domain>" > regdebug.log
  where: <user> is the SIP username against which the remote phone is trying to register
         <SIP domain> is the SIP domain configured in the remote phone trying to register
```

- Reboot the remote phone and wait for it to try to register. After it has failed to register, go back to the sipXecs and hit ctrl-c to stop the command and execute the following command:

```
wc -l regdebug.log
```

- If the command returns '0' then it means that the REGISTER requests emitted by the remote phone are not reaching sipXecs and that you have network connectivity issues. Re-verify the configuration of the local and remote NAT making sure that any SIP ALGs are disabled and that pinholes and port forwarding rules have been applied to the local NAT in accordance with Step 5 of the configuration guide.
- Else, if the command returns a non-zero value, it means that packets are reaching the sipXecs as they should. Proceed to execute the following command:

```
grep -i received regdebug.log | wc -l
```

- If the command returns '0', it indicates that either the phone is not a remote phone or that it has STUN enabled or that the remote NAT has a SIP ALG turned on - double-check these elements.
- If the command returns a non-zero value, things appear to be working fine from the Remote User NAT Traversal point-of-view. Refer to the general registration troubleshooting guide found here for additional help.

Problem #2 - Remote Worker registers but cannot make or receive calls

From sipXconfig, navigate to 'Diagnostics->Registrations' and find the unexpired registration for the problematic remote user by scanning the 'URI' column. Once you have identified the row, check the value found in the 'Contact' column. What you should find in there is a Contact of the general form:

```
<sip:<user>@<remote NAT WAN-facing IP address>:<remote NAT WAN-facing port>;x-sipX-privcontact=<Remote phone IP
address>%3A<Remote phone SIP port>>
   Note1 = <remote NAT WAN-facing port> and <Remote phone SIP port> may be missing
   Note2 = Extra parameters not shown here could be present as well (e.g. transport=, rinstance= ) - those can
be ignored for the purposes of this exercise.
```

Inspect the <remote NAT WAN-facing IP address> and <Remote phone IP address> to make sure they like up with what you have configured in your Remote NAT and remote phone. If not, please double check their IP addresses.

If you do not see a x-sipX-privcontact parameter but instead see a sipX-nonat, this indicates that either the remote phone has STUN turned on or that the remote NAT has a SIP ALG turned on. They must be disabled in order for the remote user NAT traversal feature to work.

If everything checks out, you'll have to provide a network trace of the problem. This can be accomplished by logging into the sipXecs shell and entering the following command:

```
tcpdump -n -nn -s 0 -i any -w remote_user_problem.cap
```

While tcpdump is running, reboot the remote user phone and once it is successfully registered, recreate the problematic call and finally, stop tcpdump by pressing ctrl-c. Post your observations on the sipX devlist and mention that you have a network trace available. A sipXecs designer monitoring the list will ask you to e-mail that trace privately so that it can be looked at.

Problem #3 - Remote Worker registers and can make calls but media is blocked in one or both directions

The main cause for these kinds of problems are configuration issues in the local NAT. Please review configuration step 5 and pay special attention to the RTP port range pinholes and forwarding rules.

Annex 1 - FAQ

Q1- What is the distinction between remote NAT traversal and sipXbridge? Are they one and the same?

A1- They are not the same. The sipXbridge is a stand-alone process within sipXecs that is responsible for providing connectivity to ITSPs. As part of its arsenal, sipXbridge implements features to facilitate interoperability. These features include local REFER handling, identity mapping and local NAT traversal but does **NOT** include remote user NAT traversal. SipXbridge is built to interact with ITSPs; not users. On the other hand, the Remote User NAT Traversal feature is built and an extension (plug-in) to the existing SIP Proxy and is responsible for facilitating local and remote NAT traversal for the users on the system.

Q2- Can SipXBridge and the Remote User NAT Traversal feature be both enabled at the same time?

A2- The sipXbridge and the remote user NAT traversal features are built to co-exist so long at sipXbridge is **not** configured as the default SBC in the System->Internet Calling page. Assuming the default port values are used, incoming traffic from ITSPs must be directed to port 5080 to hit the sipXbridge and incoming traffic from remote users must be directed to port 5060 to hit the sipXproxy which provide remote NAT compensation.

Annex 2 - Known routers with SIP ALGs

Router Make/Model/Fw version	Has SIP ALG?	Procedure to disable SIP ALG
Cisco 2811 v12.4T	Yes	no ip nat service sip tcp port 5060 no ip nat service sip udp port 5060
Motorola (Netopia) 3346n-ent	Yes	no ip nat alg sip enable