



**Documentação Técnica fone@RNP:
Homologação de instituições do fone@RNP com
encaminhamento nacional via SIP
V2.0.0**

Laboratório VoIP

Julho de 2010

Este documento descreve os procedimentos para realizar a homologação das instituições do fone@RNP que operam com encaminhamento nacional via SIP.

Sinopse

Os passos necessários para homologar uma instituição no ambiente com encaminhamento nacional via SIP são descritos neste documento.

Sumário

Documentação Técnica fone@RNP:.....	1
Homologação de instituições do fone@RNP com encaminhamento nacional via SIP.....	1
V2.0.0.....	1
Laboratório VoIP	1
Julho de 2010.....	1
.....	1
RNP/REF/0204.....	1
Sumário.....	3
1.....	5
Introdução.....	5
1.1.	8
E-mail padrão	8
2.	10
Passos antes do agendamento	10
2.1.	10
Informações preenchidas na FeGeN	10
2.2.	11
Informações complementares	11
2.3.	11
Liberações no firewall da instituição.....	11
2.4.	13
Liberações de firewalls	13
2.5.	14
Testes das liberações dos firewalls	14
2.6.	15
Configuração do registro SRV no DNS da instituição.....	15
2.7.	16
Clientes VoIP e senhas.....	16
2.8.	16
Para instituições já operacionais e que estejam migrando para o encaminhamento por SIP	16
3.	16
Agendamento	16
4.	17
Verificações do ambiente instalado.....	17
4.1.	17
Verificar se os processos das máquinas 1 e 2 estão em execução.....	17
4.2.	18
Ativação da instituição.....	18
4.3.	18
Permissão do apache da máquina 2 para a criação de usuários com a Féjeca.....	18
4.4.	19
Configuração do X-Lite.....	19
5.	21
Testes locais.....	21
6.	22
Testes com uma instituição do novo ambiente (com encaminhamento nacional via SIP).....	22
7.	23

Testes com uma instituição que opera somente com encaminhamento nacional via H.323...	23
8.	24
Testes de IVR.....	24
9.	26
Verificações finais.....	26
10.	26
RNP anuncia a nova instituição homologada.....	26

1.

Introdução

O projeto `fone@RNP` realizava inicialmente somente encaminhamento de chamadas entre instituições através do H.323. A partir de 2008, foram introduzidas mudanças no serviço `fone@RNP`, permitindo o encaminhamento nacional também via SIP e o uso de tabelas sincronizadas.

Este documento descreve os passos para homologar uma instituição que fará uso da instalação padrão baseada em Debian e nos pacotes de software desenvolvidos pelo Laboratório VoIP do NCE/UFRJ para o encaminhamento nacional via SIP. Os testes de homologação devem ser aplicados tanto no caso de uma instituição que adere ao serviço pela primeira vez, quanto no caso de uma instituição já operacional que migre para o novo ambiente.

Neste documento, quando for mencionado “novo ambiente”, refere-se à instituição operando no ambiente com encaminhamento nacional através do SIP. RTFC é a sigla para a rede de telefonia fixa comutada, ou seja, o ambiente do provedor de telefonia fixa conectado ao PBX da instituição.

Para os testes com as instituições, o LabVoIP estará utilizando preferencialmente os telefones:

n°	Telefone	Descrição
1	021 1100 00[91, 92 e 93]	Telefones IPs SIP
2	021 2598 3008 / 021 2598 3354	PBX - LabVoIP
3	021 2598 3212	PBX - mesa telefônica do NCE
4	021 2598 3100 / 021 2598 3333	PBX - portaria NCE
5	021 4004 4700 / 021 4004 4463	RTFC Rio (IVR)
6	021 4001 4001 / 021 4004 4004 / 021 2548 2742	RTFC Rio (IVR)

O Laboratório VoIP está atuando como suporte técnico da RNP na homologação e migração de instituições no serviço `fone@RNP`. Para a entrada de dados sobre a Instituição no banco de dados da RNP é utilizada a ferramenta FeGeN. No ambiente local da instituição, é usada a ferramenta Féjeca para a criação dos primeiros usuários no LDAP da instituição.

Qualquer instituição que queira fazer parte do serviço `fone@RNP` deve inicialmente contatar a RNP. Cabe à RNP avaliar a qualificação da instituição e encaminhar solicitação ao Laboratório VoIP para que proceda à homologação da instituição no serviço.

A homologação segue os passos mostrados no fluxograma de homologação do serviço `fone@RNP`, mostrado na Figura 1. No fluxograma, as etapas amarelas correspondem a ações da instituição. As etapas em azul correspondem a ações da RNP, enquanto as etapas em rosa correspondem a ações do Laboratório VoIP.

Fluxo do Serviço Fone@RNP (versão 1.0)

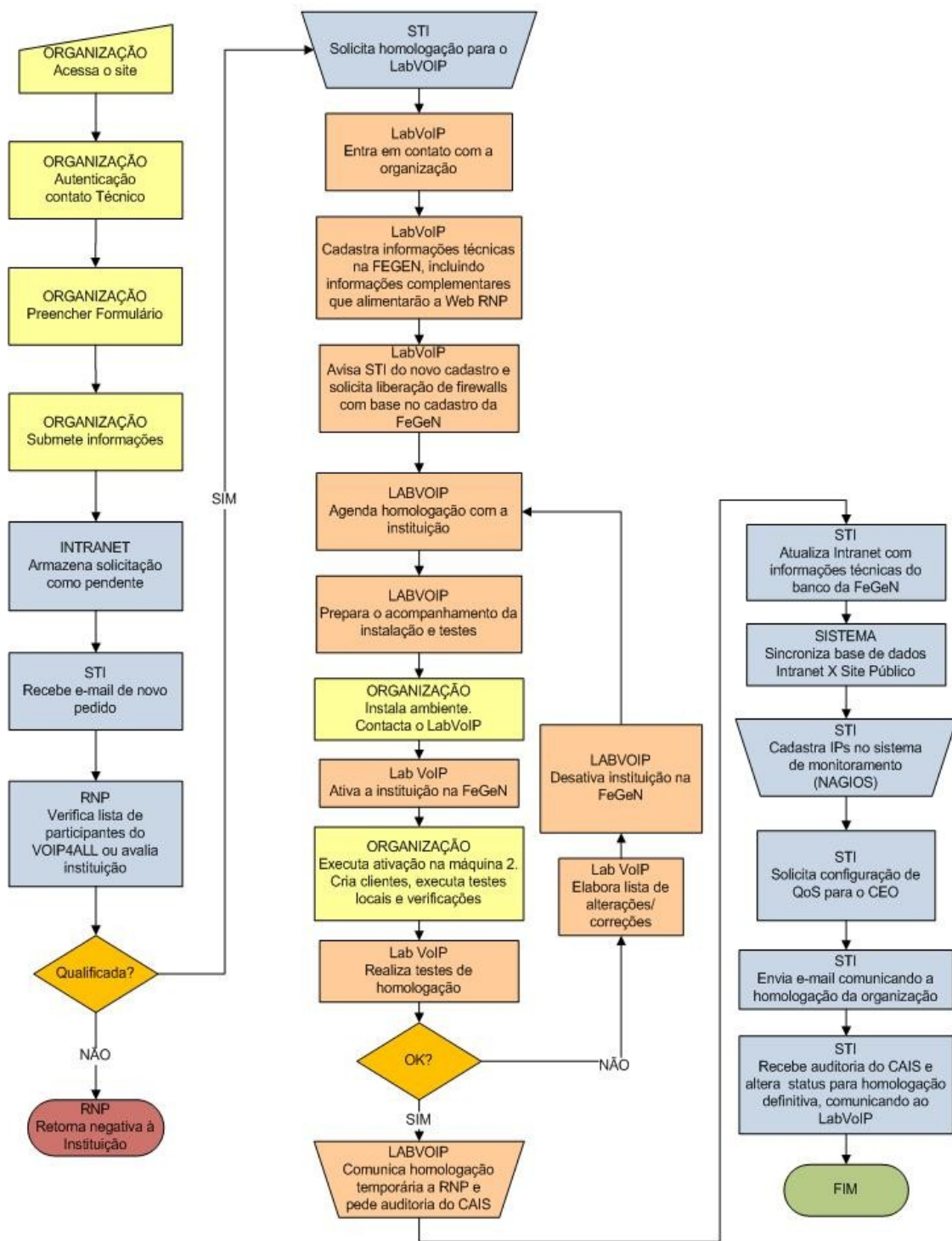


Figura1 – Fluxograma da homologação do serviço fone@RNP.

Após receber solicitação da RNP, o Laboratório VoIP faz um primeiro contato com o responsável pela homologação do VoIP na instituição, enviando o e-mail mostrado na seção 1.1

1.1.

E-mail padrão

O texto abaixo é o E-mail padrão enviado a uma instituição pelo Laboratório VoIP, como passo inicial no processo de homologação. Este e-mail é enviado tanto para as novas instituições como para as antigas que estejam desejando migrar para o encaminhamento nacional por SIP.

=====E-MAIL PADRÃO=====

Orientação para Homologação (v3.2) (alteração em 21/07/2010)

Ao responsável pela homologação:

Todos os passos abaixo devem ser completados com exatidão, antes do agendamento da homologação.

a) Enviar as informações técnicas especificadas no manual de instalação nas seções 2.1 e 2.2, para que os procedimentos de configuração e de abertura de firewalls do lado da RNP possam ser efetivados e testados pela própria instituição, a partir das máquinas que serão usadas para a implantação do serviço.

Os IPs das máquinas 1 e 2 têm que ser reais. Não podem ser usados IPs privados.

b) Instalar o **DEBIAN 4** nas duas máquinas que suportarão o ambiente. A imagem do Debian 4 a ser usada tem que ser a existente na área de homologação fone@RNP em <http://www.voip.nce.ufrj.br/> (ver manual de instalação).

c) Em caso de migração de ambiente já operacional, realizar o procedimento de backup tanto da imagem das máquinas quanto do banco de dados e do LDAP (ver manual de backup).

O backup das imagens das partições Debian das máquinas 1 e 2 pode não ser necessário se novas máquinas forem utilizadas. Ele serve para restaurar a operação antiga, em caso de falha inesperada na subida do novo ambiente.

Para que seja feito o agendamento da instituição, o backup inicial dos bancos terá que ter sido feito. Todavia, até a véspera do dia do agendamento da homologação, outros backups poderão ser feitos para que usuários habilitados e os registros de chamadas ocorridos após o backup inicial possam ser restaurados. Mas, em caso de alguma falha, o backup inicial deve ser usado. Por essa razão, recomenda-se que novos usuários não sejam habilitados após o backup inicial.

d) Configurar o DNS e a abertura de firewalls do lado da instituição, conforme instruções nas seções 2.3 e 2.5 do manual de homologação.

Os testes de firewall a partir das máquinas já com IP configurado e DEBIAN instalado devem seguir o recomendado a seguir. Executando a sequência de comandos abaixo, uma tabela com uma linha e uma coluna é mostrada com a

quantidade de registros na tabela "instituições", caso o acesso esteja liberado:

```
$ apt-get install postgresql-client-8.1
$ psql -d chamadas -h dser1.rnp.br -U clusteruser -c "select count(*) from
instituicoes"
```

Para teste do DNS, siga os exemplos abaixo, usando sua instituição no lugar da UFRJ:

```
# nslookup
> set query=svr
> _sip._udp.voip.nce.ufrj.br
Server: 146.164.247.193
Address: 146.164.247.193#53
_sip._udp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

```
# nslookup
> set query=svr
> _sip._tcp.voip.nce.ufrj.br
Server: 146.164.247.193
Address: 146.164.247.193#53
_sip._tcp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

e) Enviar para o Lab Voip (foneatrn@voip.nce.ufrj.br) as informações solicitadas no manual de homologação.

Estas informações têm que ser precisas e completas. Em especial, quando a instituição for completar chamadas para a RTFC, apenas os prefixos que o PBX aceitará completar podem ser anunciados. Em hipótese alguma uma instituição pode anunciar prefixos que serão bloqueados pelo PBX. Prefixos podem ser inseridos e deletados sem dificuldade. Em caso de dúvida no preenchimento das informações, contatar o Laboratório VoIP.

Nota: Os prefixos locais das cidades de um Estado podem ser obtidos na URL sistemas.anatel.gov.br/areaarea/N_Download/Tela.asp?varMod=Publico&SISQSmodulo=7179

Escolha os parâmetros:

Tipo de Arquivo: Central CNL
Tipo Central: Fixo
Sigla UF: ESTADO DESEJADO

Será retornado um arquivo zipado.

f) Apontar contato técnico com disponibilidade de tempo integral para agendar data de homologação.

TODAS AS ETAPAS ACIMA TÊM QUE SER EXECUTADAS E VERIFICADAS ANTES QUE UM AGENDAMENTO PARA HOMOLOGAÇÃO POSSA SER MARCADO PELO CONTATO TÉCNICO COM O LABORATÓRIO VoIP.

Os seguintes documentos devem ser obtidos em: <http://www.voip.nce.ufrj.br/dochomolog>

Documentação Técnica fone@RNP: Instalação e Configuração do ambiente fone@RNP em máquina Dell com encaminhamento SIP v4.2.5

Documentação Técnica fone@RNP: Homologação de instituições do fone@RNP com encaminhamento nacional via SIP v2.0.0

Documentação Técnica fone@RNP: Backup do ambiente VoIP V3.3.1

Documentação Técnica fone@RNP: Encaminhamento via SIP de Chamadas E.164 no fone@RNP: operação e migração v3.0

Atenciosamente,

=====

2.

Passos antes do agendamento

Passo 0: Uma instituição que deseja integrar o fone@RNP deve inicialmente contatar o serviço fone@RNP, para verificar a sua qualificação para entrada no serviço.

Uma instituição considerada qualificada pela RNP deve preencher as informações abaixo e enviar para o LabVoIP/NCE/UFRJ, usando o e-mail (sugerido: foneatrn@voip.nce.ufrj.br). Estas informações farão parte do banco de dados oficial da instituição e serão utilizadas para a configuração automática do ambiente da instituição.

OBSERVAÇÃO

Os passos a seguir precisam ser realizados antes da instituição agendar uma data para a homologação com o LabVoIP.

2.1.

Informações preenchidas na FeGeN

Enviar para a RNP (servnac@rnp.br) e para o LabVoIP (foneatrn@voip.nce.ufrj.br) as informações abaixo, como requisito para o agendamento.

	Data / Hora:	
n°	Item	Descrição
1	Nome da Instituição (apenas a sigla)	
2	Responsável(is) pelo VoIP da instituição	
3	E-mail do(s) responsável(is) pelo VoIP da instituição	
4	Prefixo da cidade (DDD)	
5	Domínio (Realm – registro SRV do DNS)	
6	Interface com o PABX (opções: FXO/R2/ISDN)	Opções:FXO R2 ISDN

7	Quantidade de interfaces com o PABX	
8	Existe H.323 Interno	SIM NÃO
9	Existe encaminhamento para RTFC	SIM NÃO
10	Endereço IP máquina 1 (tem que ser real)	
11	Endereço IP máquina 2 (tem que ser real)	
12	Prefixos IP (prefixo dos telefones IP cedido pela RNP)	
13	Prefixos PBX com seus DDD's (lista)	
14	Prefixos RTFC da cidade (atenção: PBX não pode bloquear!)	
15	Linhas privadas da instituição (pode ser uma lista)	
16	Número IVR interno (pode ser uma lista)	
17	Número IVR externo (pode ser uma lista)	
18	Números associados ao asterisk quando o FXO for utilizado (lista)	

2.2.

Informações complementares

As informações complementares abaixo precisam ser enviadas para servnac@rnp.br e para foneatrn@voip.nce.ufrj.br.

	Data / Hora:	
n°	Item	Descrição
1	Modelo do PBX:	
2	Responsável pela instituição (reitor, diretor ou etc.):	
3	E-mail de contato do responsável pela instituição (reitor, diretor ou etc.):	
4	Ramal de contato do responsável pela instituição (reitor, diretor ou etc.):	
5	Ramal de contato do(s) responsável(is) pelo VoIP:	
6	Telefones de contato do(s) responsável(is) pelo VoIP (celular ou etc.):	
7	Ramais do PBX para testes 24/7 (telefonista, FAX, portaria e etc.):	
8	Números na RTFC na cidade da instituição para testes 24/7 (IVRs de bancos, IVRs de operadoras de Telecom, IVRs de operadoras de cartão de crédito, IVRs de telemarketing, hotéis e etc.):	
9	Número da mesa telefônica da instituição (telefonista):	
10	Alterações previstas pela instituição de serem realizadas no ambiente padrão	

2.3.

Liberações no firewall da instituição

Verifique se as portas descritas nos quatro itens abaixo foram liberadas no firewall da instituição. A princípio, estas portas precisam estar liberadas pelo menos 2 dias antes do início da homologação.

Observação: As regras de *firewall* ativas para instituições operando no ambiente antigo precisam ser mantidas.

(1) Caso a instituição opere com H.323, liberar no firewall local as portas relacionadas abaixo:

PARA END IP DA MÁQUINA 1:

- 1720/TCP e 1721/TCP para toda a Internet (sinalização H.225 Q.931)

Como o DGK na arquitetura atual opera como proxy de sinalização, a troca de sinalização H.323 será sempre feita com o DGK e nunca diretamente com cada GK. A liberação para toda a internet diminui o trabalho de configuração.

- 1719/UDP o rnpdgk1.rnp.br e rnpdgk2.rnp.br (sinalização H.225 RAS)
- 30000/TCP a 30999/TCP para o rnpdgk1.rnp.br e rnpdgk2.rnp.br (sinalização H.245)
- 50000/UDP a 56999/UDP para toda a internet (tráfego RTP/RTCP)

O tráfego de mídia a ser recebido pelo GK (atuando como proxy) virá de outro GK ou do asterisk nacional. A liberação para toda a internet diminui o trabalho de configuração.

PARA END IP DAS MÁQUINAS 1 e 2:

- 5432/TCP entre o DSER1 (dser1.rnp.br) e as duas máquinas da instituição (slony)
- 5432/TCP entre o DSER2 (dser2.rnp.br) e as duas máquinas da instituição (slony)
- 123/UDP para conexões nos dois sentidos (entrada e saída) envolvendo as máquinas 1 e 2 para os servidores NTP ntp1.rnp.br e ntp.cais.rnp.br

Nota: as portas citadas não podem ser fechadas.

(2) Caso a instituição opere com SIP, liberar as portas relacionadas abaixo:

PARA END IP DA MÁQUINA 1:

- 5060/UDP e 5060/TCP para toda a internet
A troca de sinalização SIP ocorrerá com o ambiente nacional (dser e asterisk gw H.323/SIP) ou diretamente com outros proxies SIP. Dessa forma esta liberação não precisaria ser para toda a internet.
- 50000/UDP-56999/UDP para toda a internet (mídia)
O tráfego de mídia a ser recebido virá de um proxy SIP ou do asterisk nacional. A liberação para toda a internet diminui o trabalho de configuração.

PARA END IP DAS MÁQUINAS 1 e 2:

- 5432/TCP entre o DSER1 (dser1.rnp.br) e as duas máquinas da instituição.
- Porta 5432/TCP (slony e instalação dos pacotes) entre o DSER2 (dser2.rnp.br) e as duas máquinas da instituição. (slony e instalação dos pacotes)
- 123/UDP para conexões nos dois sentidos (entrada e saída) envolvendo as 2 (duas) máquinas VoIP para os servidores NTP ntp1.rnp.br e ntp.cais.rnp.br

Nota1: Essas portas não podem ser fechadas.

Nota2: As seguintes liberações envolvendo os serviços de gw asterisk H.323/SIP local na máquina 1, explicitadas em versões anteriores do documento, foram suprimidas:

- 5070/UDP e 5070/TCP para dser1.rnp.br e dser2.rnp.br
- 1730/UDP, 1730/TCP, 1740/UDP e 1740/TCP para dser1.rnp.br e dser2.rnp.br

(3) Liberar portas para o servidor da RNP chamado *carratos.na-cp.rnp.br*, utilizado para verificar se os serviços estão funcionando nas máquinas 1 e 2 via o *software* Nagios.

PARA END IP DA MÁQUINA 1:

- UDP/5060 e TCP/5060
- UDP/5070 e TCP/5070
- UDP/1730, TCP/1730, UDP/1740, TCP/1740 (asterisk gw H.323/SIP local)
- 7000/TCP (console H.323) e 1719/UDP (H.323 RAS)

PARA END IP DA MÁQUINA 2:

- 5432/TCP (postgres), 80/TCP (web), 389/TCP (LDAP), 1812/UDP (radius), 1813/UDP (radius), 5060/UDP (sinalização SIP)
- 5432/TCP, 80/TCP, 389/TCP, 1812/UDP, 1813/UDP, 5060/UDP

(4) Liberar todas as portas TCP e UDP para conexões envolvendo as máquinas 1 e 2 e o endereço IP 200.144.121.92. Esse IP é utilizado para auditoria de segurança do CAIS, podendo ser bloqueado após a auditoria.

(5) Libere para o LabVoIP (146.164.247.192/255.255.255.192) as seguintes portas/protocolos:

- Liberar o protocolo ICMP.
- 22/TCP (SSH).
- 80/TCP (HTTP) e 443/TCP (HTTPS).

2.4.

Liberações de firewalls

As portas abaixo são liberadas pela RNP para que uma instituição possa encaminhar chamadas pelo ambiente nacional. A instituição deve liberar também seus próprios firewalls.

Observação: as regras de *firewall* ativas para instituições operando no ambiente antigo precisam ser mantidas.

1) Caso a instituição opere com H.323

Liberar portas de sinalização para a comunicação entre os DGKs (rnpdgk1.rnp.br e rnpdgk2.rnp.br) e a máquina 1 da instituição (que opera como proxy de sinalização e mídia):

- Liberação de sinalização H.225 Q.931: portas TCP 1720 e 1721.
- Liberação de sinalização H.225 RAS: porta UDP 1719.
- Liberação de sinalização H.245: portas TCP de 30000 a 30999.
- Liberar a porta 5432/TCP para comunicação entre DSER1 e DSER2 (dser1.rnp.br e dser2.rnp.br) e as duas máquinas da instituição.

Para o tráfego de mídia, liberar as portas UDP dos gateways H.323/SIP (dser1.rnp.br e dser2.rnp.br) para a comunicação com a máquina 1 da instituição (que opera como proxy de sinalização e mídia):

- Liberação de tráfego RTP/RTCP: portas UDP de 50000 a 56999.

Nota: as portas citadas não podem ser fechadas.

2) Caso a instituição opere com SIP libere as portas abaixo devem estar liberadas entre os DSERs (dser1.rnp.br e dser2.rnp.br) e a máquina 1:

- 5060/UDP e 5060/TCP (proxy SIP OpenSER).
- 5070/UDP e 5070/TCP (asterisk gw H.323/SIP local).
- 1730/UDP, 1740/UDP, 1730/TCP e 1740/TCP (asterisk gw H.323/SIP local).
- Portas UDPs entre 50000-56999 (proxy de mídia).
- Porta 5432/TCP entre DSER1 e DSER2 (dser1.rnp.br e dser2.rnp.br) e as duas máquinas da instituição.

Nota: essas portas não podem ser fechadas.

3) Liberar portas do servidor da RNP chamado *carratos.na-cp.rnp.br*, utilizado para verificar se os serviços estão funcionando nas máquinas 1 e 2 via o *software* Nagios.

- Portas 5060 (sinalização SIP), 5070 (asterisk local), 1730 (asterisk canal oh323) e 1740 (asterisk com canal ooh323) UDP e TCP, para acesso à máquina 1.
- Portas 7000/TCP (console Telnet H.323) e 1719/UDP (sinalização H.323) para acesso à máquina 1.
- Portas 5432/TCP (postgres), 80/TCP (web), 389/TCP (LDAP), 1812/UDP (radius), 1813/UDP (radius), 5060/UDP (sinalização SIP) para acesso à máquina 2.
- Liberar o protocolo ICMP.

2.5.

Testes das liberações dos firewalls

Os testes de firewall a partir das máquinas já com IP configurado e DEBIAN instalado devem seguir o recomendado a seguir. Executando a sequência de comandos abaixo, uma tabela com uma linha e uma coluna é mostrada com a quantidade de registros na tabela "instituições", caso o acesso esteja liberado:

```
$ apt-get install postgresql-client-8.1
```

```
$ psql -d chamadas -h dser1.rnp.br -U clusteruser -c "select count(*) from instituicoes"
```

Para teste do DNS, siga os exemplos abaixo, usando sua instituição no lugar da UFRJ:

```
# nslookup
```

```
> set query=svr
```

```
> _sip._udp.voip.nce.ufrj.br
```

```
Server: 146.164.247.193
```

```
Address: 146.164.247.193#53
```

```
_sip._udp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

```
# nslookup
```

```
> set query=svr
```

```
> _sip._tcp.voip.nce.ufrj.br
```

```
Server: 146.164.247.193
```

```
Address: 146.164.247.193#53
```

```
_sip._tcp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

Este teste de verificação de liberação de firewall é pré-requisito para o agendamento da homologação.

2.6.

Configuração do registro SRV no DNS da instituição

A configuração do DNS é pré-requisito para o agendamento e deve ser realizada com antecedência. Adicione no DNS as linhas referentes aos registros SRV para a máquina 1. Abaixo existe um exemplo com o BIND, onde estas linhas são inseridas no arquivo de zona local:

```
_sip._udp.<REALM>.      SRV      1      1      5060    <hostname da maq1>
_sip._tcp.<REALM>.      SRV      1      1      5060    <hostname da maq1>
```

Nota: Nas duas linhas mostradas, o nome <hostname da maq1> deve ser substituído pelo nome da máquina 1. A TAG <REALM> precisa ser substituída pelo REALM da instituição. Observe que a primeira linha é o registro para o UDP e a segunda linha refere-se ao TCP.

É preciso garantir que existe um registro no DNS do tipo “A” para máquina 1, como no exemplo abaixo (no arquivo de zona local do software BIND), que garante a resolução do nome <hostname da maq1> para o endereço IP da máquina 1, <IP da maq1>.

```
<hostname da maq1> 360 IN      A      <IP da maq1>
```

Após alterar o DNS, lembre de reinicializar este serviço para que as alterações sejam ativadas.

Para testar a configuração do DNS, siga os passos mostrados abaixo substituindo o “voip.nce.ufrj.br” pelo REALM (domínio) da instituição.

```
# nslookup
> set query=srv
> _sip._udp.voip.nce.ufrj.br
Server:      146.164.247.193
Address:     146.164.247.193#53

_sip._udp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

```
# nslookup
> set query=srv
> _sip._tcp.voip.nce.ufrj.br
Server:      146.164.247.193
Address:     146.164.247.193#53

_sip._tcp.voip.nce.ufrj.br service = 1 1 5060 maq1.voip.nce.ufrj.br.
```

Nota: o primeiro teste foi realizado para UDP e o segundo para TCP; em negrito estão os comandos e parâmetros digitados pelo usuário.

2.7.

Clientes VoIP e senhas

Prepare duas estações de trabalho com um cliente H.323 (OpenPhone, como sugestão) e com um cliente SIP (X-Lite, como sugestão). Esses clientes podem ser obtidos no site www.voip.nce.ufrj.br na área de *download*. Caso utilize o linux nas estações clientes VoIP, a sugestão é utilizar o software Ekiga (<http://ekiga.org/>) que opera como cliente H.323 e SIP. Se a instituição operar internamente apenas com SIP, os cliente H.323 não precisam de ser instalados.

Na instalação serão solicitadas senhas e podem são mostradas no manual de instalação. É recomendado que estas senhas sejam escolhidas antes mesmo do dia da instalação e homologação. Apenas a senha de acesso ao banco de dados postgres precisa ser passada ao LabVoIP para configuração do ambiente nacional.

2.8.

Para instituições já operacionais e que estejam migrando para o encaminhamento por SIP

Em caso de migração de ambiente já operacional, a instituição deve realizar o procedimento de backup tanto da imagem das máquinas quanto do banco de dados e do LDAP, seguindo as recomendações em Documentação Técnica fone@RNP: Backup do ambiente VoIP V3.2.

O backup das imagens das partições Debian das máquinas 1 e 2 pode não ser necessário se novas máquinas forem utilizadas. Ele serve para restaurar a operação antiga, em caso de falha inesperada na subida do novo ambiente.

Para que seja feito o agendamento da instituição, o backup inicial dos bancos terá que ter sido feito. Todavia, até a véspera do dia do agendamento da homologação, outros backups poderão ser feitos para que usuários habilitados e os registros de chamadas ocorridos após o backup inicial possam ser restaurados. Mas, em caso de alguma falha, o backup inicial deve ser usado. Por essa razão, recomenda-se que novos usuários não sejam habilitados após o backup inicial.

3.

Agendamento

Para que a instituição agende uma data para a homologação é necessário que todos os passos na seção 2 tenham sido realizados. A instituição deverá contatar o Laboratório VoIP para agendar a data de homologação apenas quando todos os passos preliminares tiverem sido executados.

Se tudo estiver ok, será agendado um dia para a homologação e a instituição terá que garantir a presença de um técnico em tempo integral para esta tarefa na data escolhida.

É essencial que este técnico tenha lido os documentos relacionados no E-mail padrão. Apenas os passos preliminares relacionados na seção 2 serão feitos pela instituição de forma independente.

Para facilitar a interação com o LabVoIP, sugere-se o uso da ferramenta P2P como MSN Live Messenger, que permite o chat e comunicação por voz. O técnico deve criar uma conta no MSN

Messenger antecipadamente. O uso do Messenger evitará ligações DDD e limitações de ramal ocupado no laboratório.

Todo o processo de instalação de pacotes e testes de homologação serão feitos de forma conjunta entre o Laboratório VoIP e a instituição, no dia da homologação. Nenhum passo deve ser dado sem o acompanhamento e supervisão do Laboratório VoIP.

O processo de homologação deve durar apenas poucas horas, para uma instituição que esteja implantando a arquitetura de referência no serviço. Não existirão configurações manuais a serem feitas, apenas a seleção de senhas.

4.

Verificações do ambiente instalado

As verificações descritas aqui são realizadas no dia da homologação após a instalação dos pacotes (ver manual de instalação) e terão a supervisão do Laboratório VoIP.

4.1.

Verificar se os processos das máquinas 1 e 2 estão em execução

Utilize os comandos nas tabelas abaixo para se certificar que os processos estão em execução. Caso algum processo descrito não esteja em execução, o Laboratório VoIP irá definir o procedimento a seguir. Normalmente, como não há intervenção manual no processo de instalação, as verificações são apenas para garantir que não houve nenhuma falha não esperada.

Processos da máq. 1	Comandos	Parte da saída
GK	ps xua grep gnugk	/usr/sbin/gnugk -c /etc/gnugk/gnugk.ini
Openser	ps xua grep openser	/usr/sbin/openser
Asterisk	ps xua grep asterisk	/usr/sbin/asterisk -U asterisk -G asterisk
SSH	ps xua grep ssh	/usr/sbin/sshd
NTP	ps xua grep ntp	/usr/sbin/ntpd -p /var/run/ntpd.pid
Mediaproxy	ps xua grep mediaproxy	python /usr/mediaproxy/mediaproxy.py --pid /var/run/mediaproxy/mediaproxy.pid

Processos da máq. 2	Comandos	Parte da saída
Postgres	ps xua grep postgres	/usr/lib/postgresql/8.1/bin/postmaster -D /var/lib/postgresql/8.1/main -c config_file=/etc/postgresql/8.1/main/postgresql.conf
Asterisk	ps xua grep asterisk	/usr/sbin/asterisk -U asterisk -G asterisk
NTP	ps xua grep ntp	/usr/sbin/ntpd -p /var/run/ntpd.pid
SSH	ps xua grep ssh	/usr/sbin/sshd
Apache	ps xua grep apache2	/usr/sbin/apache2 -k start
LDAP	ps xua grep slapd	/usr/libexec/slapd -f /usr/etc/openldap/slapd.conf -u openldap -g openldap
Radius	ps xua grep radius	/usr/sbin/radiusd

4.2.

Ativação da instituição

Após a instalação dos pacotes e verificada a normalidade do ambiente em 3.1, a instituição será ativada para serem realizados os testes de homologação. A ativação é uma ação do Laboratório VoIP no ambiente nacional, quando o estado de configurada passa a ser de ativada. Esta é uma ativação temporária para os testes.

Após o LabVoIP informar que a instituição foi ativada, deverá ser executado o comando na máquina 2:

```
$ php /etc/fegen/clientes.php ativacao
```

Para testar o sucesso da ativação, os passos abaixo devem ser executados.

Entre como *root* na máquina 2 e verifique se as tabelas “instituicoes”, equipamentos e prefixos possuem informações.

```
$ su - postgres
$ psql -d chamadas
chamadas=# select * from instituicoes;
chamadas=# select * from prefixos;
chamadas=# select * from equipamentos;
```

Nota: caso essas tabelas não contenham informações o processo falhou e o Laboratório VoIP indicará como proceder.

Verificar se os processos da máquina 2 estão em execução após ativação

Utilize os comandos na tabela abaixo para se certificar que os processos estão em execução, após a ativação. Caso algum processo descrito não esteja em execução, o Laboratório VoIP irá definir o procedimento a seguir. Normalmente, como não há intervenção manual no processo de instalação, as verificações são apenas para garantir que não houve nenhuma falha não esperada.

Processo da máquina 2	Comandos	Parte da saída
Consolida	ps xua grep consolida	/usr/consolida/consolida.php
SLON	ps xua grep slon	slon -d 2 -s 60000 -t 1200000 clustervoip

4.3.

Permissão do apache da máquina 2 para a criação de usuários com a Féjeca

Para acessar a ferramenta Féjeca e criar contas de usuários, utilize a URL “https://<IP máquina 2>/ger2/” ou http://<IP máquina 2>/ger2/”. O acesso ao apache da máquina 2 (Féjeca) pode ser restrito, através do arquivo:

```
$ vi /etc/apache2/sites-enabled/000-default
```

Na linha 14, em baixo de “Order allow,deny”, se existir “allow from all”, comente esta linha com tralha (#). O default deve ser bloquear o acesso para todos.

```

1 NameVirtualHost *
2 <VirtualHost *>
3     ServerAdmin webmaster@localhost
4
5     DocumentRoot /var/www/
6     <Directory />
7         Options FollowSymLinks
8         AllowOverride None
9     </Directory>
10    <Directory /var/www/>
11        Options Indexes FollowSymLinks MultiViews
12        AllowOverride None
13        Order allow,deny
14
15        # This directive allows us to have apache2's default start page
16        # in /apache2-default/, but still have / go to the right place
17        RedirectMatch ^/$ /apache2-default/
18    </Directory>

```

Na linha 14, em baixo de “Order allow,deny”, coloque os IPs que devem ter permissão de acesso ao HTTP da máquina 2 (Féjeca), no exemplo abaixo substitua as tags <IP confiável 1> e <IP confiável 2> pelos IPs que podem acessar a Féjeca:

```

allow from <IP confiável 1>
allow from <IP confiável 2>

```

Depois reinicie o apache da máquina 2:

```
/etc/init.d/apache2 restart
```

Case isso não for feito, qualquer IP poderá acessar a Féjeca.

OBS.: A instituição poderá, se quiser, configurar o apache para solicitar usuário e senha para acesso a Féjeca.

OBS.: Acesse a Féjeca na máquina 2 (<http://<IP da máquina 2>/ger2/>) para criar os usuários.

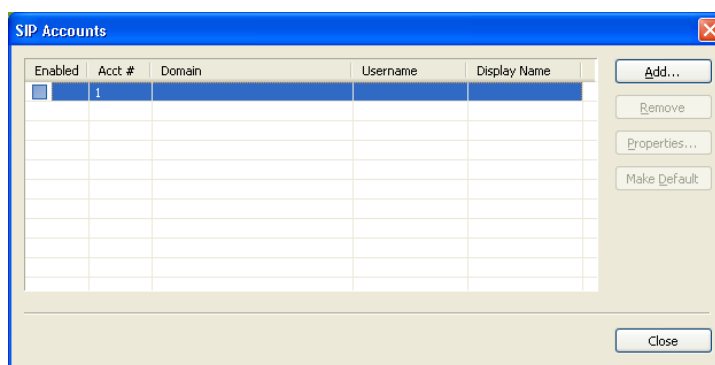
4.4.

Configuração do X-Lite

Da área de download do site <http://www.voip.nce.ufrj.br/> baixe o X-Lite 3.0 para Windows, depois instale este X-Lite. Pode ser usado o site da empresa em www.counterpath.com. Click com o botão direito no mouse o display do telefone, como mostrado abaixo e selecione “SIP Account Settings ...”.

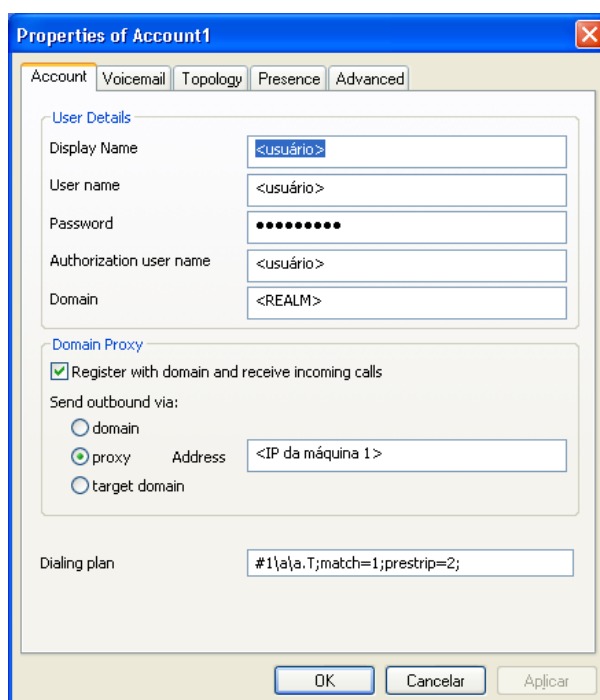


Será mostrada uma janela semelhante à figura abaixo, “Sip Accounts”. Após isso, pressione o botão “Add...” na janela para configurar a conta do usuário.



A janela a seguir é a “Properties of Account”, na aba “Account” configura a conta como é mostrada no exemplo abaixo.

Nos campos “Display Name”, “User name” e “Authorization user name” preencha o nome do usuário onde está a tag <usuário>. No campo “Password” digite a senha do usuário. A tag <REALM> deve ser substituída no campo “Domain”.



Por fim, marque na sessão "Domain Proxy" o campo "Proxy" e digite o IP ou hostname da máquina 1 em <IP da máquina 1>.

Para mais informações, consulte o manual do X-Lite no site <http://www.counterpath.com>.

5.

Testes locais

Após a instalação do ambiente, os testes locais devem ser os primeiros a serem realizados. Normalmente serão criados usuários locais que poderão estar rodando em máquinas locais e em máquinas remotas do Laboratório VoIP, durante esta fase.

Ao fim dos testes, os resultados devem ser lançados na tabela abaixo e repassados para o LabVoIP utilizando o e-mail foneatRNP@voip.nce.ufrj.br ou comunicação. A tabela abaixo define os testes.

Nota: O cadastro de usuários é realizado com a Féjeca, acessando a máquina 2 (<http://<IP máquina 2>/ger2/>) utilizando o browser FireFox. No cadastro de usuários procure preencher apenas os campos obrigatórios que são identificados por asteriscos.

Obs: Para chamadas envolvendo clientes H.323, não utilize clientes em computadores atrás de NAT.

OBSERVAÇÃO:

Testes locais realizados em conjunto com o LabVoIP.

nº	Descrição	Resultado	Observações
1	Ambiente H.323		
1.1	Cadastro de 4 usuários (<i>Fejeca máquina 2</i>)		
1.2	Registro de usuário no ambiente H.323 (<i>OpenPhone como sugestão</i>)		
1.3	Chamada entre terminais H.323		
2	Ambiente SIP		
2.1	Registro de usuário no ambiente SIP (<i>Xlite como sugestão</i>)		
2.2	Chamada entre clientes SIP		
3	Interoperação SIP/H.323		
3.1	Chamada H.323 para SIP		
3.2	Chamada SIP para H.323		

4	Contabilização de chamadas		
4.1	Coleta de CDRs via Féjeca (<i>dar tempo para a consolidação acontecer</i>)		

Nota: o cadastro de usuário do item 1 serve para criar uma conta de usuário IP utilizada no ambiente H.323 ou SIP. No cadastro de usuário IP, utilize o prefixo de telefone fornecido pela RNP (prefixo RNP).

6.

Testes com uma instituição do novo ambiente (com encaminhamento nacional via SIP)

Neste passo, serão realizados testes envolvendo duas instituições que realizam encaminhamento nacional via SIP. A primeira instituição é a que está sendo homologada no momento e a segunda instituição será preferencialmente a UFRJ, embora outra instituição já homologada pela RNP possa também ser usada, em caso da UFRJ estar indisponível por qualquer motivo.

Nestes testes, a sinalização SIP envolverá apenas as duas instituições SIP. Será verificado se as regras de firewalls foram devidamente liberadas no que tange ao protocolo SIP e se a conversão local entre H.323 e SIP está operando de acordo.

Utilize no item 1, apenas usuários que estejam registrados no proxy SIP local; no item 2, utilize apenas usuários registrados no GnuGK.

Obs.: para chamadas envolvendo clientes H.323, não utilize clientes em computadores atrás de NAT.

OBSERVAÇÃO:	
Testes realizados em conjunto com o LabVoIP.	

nº	Descrição	Resultado	Observações
1	Cliente VoIP registrado no ambiente SIP da instituição a ser homologada		
1.1	Iniciar chamada para um telefone SIP do Lab. VoIP (11000092)		
1.2	Receber uma chamada de um telefone SIP do Lab. VoIP		
2	Cliente VoIP registrado no ambiente H.323 da instituição a ser homologada		
2.1	Iniciar chamada para um telefone SIP do Lab. VoIP (11000092)		
2.2	Receber uma chamada de um telefone SIP do Lab. VoIP		

OBS: Todas as chamadas de teste acima serão encaminhadas entre as instituições via SIP. A conversão local entre SIP e H.323 será testada.

7.

Testes com uma instituição que opera somente com encaminhamento nacional via H.323

Serão realizados testes envolvendo uma instituição que não faz encaminhamento nacional via SIP. Esta instituição será definida pela RNP ou pelo Lab. VoIP.

Nestes testes, a sinalização SIP, pelo menos no item 1, obrigatoriamente, passará através do ambiente nacional. Assim, aqui verificaremos se a instituição encaminha chamadas via o ambiente nacional passando pelo DGK e DSER. Este teste será importante para garantir que a instituição sendo homologada consegue interagir com as instituições do `fone@RNP` que ainda não migraram para a nova estrutura.

Utilize no item 1 apenas usuários que estejam registrados no proxy SIP local. No item 2, utilize apenas usuários registrados no GnuGK.

Obs.: para chamadas envolvendo clientes H.323, não utilize clientes em computadores atrás de NAT.

OBSERVAÇÃO: Testes realizados em conjunto com o LabVoIP.

nº	Descrição	Resultado	Observações
1	Cliente VoIP registrado no ambiente SIP da instituição a ser homologada		
1.1	Iniciar chamada para um telefone H.323 da instituição H.323		
1.2	Receber uma chamada de um telefone H.323 da instituição H.323.		
2	Cliente VoIP registrado no ambiente H.323 da instituição a ser homologada		
2.1	Iniciar chamada para um telefone H.323 da instituição H.323		
2.2	Receber uma chamada de um telefone H.323 da instituição H.323.		

8.

Testes de IVR

Os testes de IVR precisam ser realizados com atenção, certificando que as chamadas de origem externa ao serviço sejam apenas completadas para destinos internos ao serviço `fone@RNP`. Atenção redobrada nos itens 1.5, 1.6 e 4.2, que são bloqueadas pela inserção do dígito 1 entre o código de área e o número E.164. Pela nova arquitetura, as chamadas não permitidas serão bloqueadas pelo próprio OpenSER local, sem serem encaminhadas ao DSER.

Obs.: para chamadas envolvendo clientes H.323, não utilize clientes em computadores atrás de NAT.

OBSERVAÇÃO:
Testes realizados em conjunto com o LabVoIP.

nº	Descrição	Resultado	Observações
1	Chamadas externas originadas da rede de telefonia pública (RTFC) via IVR		
1.1	Chamada para ramal chave do PBX (<i>teste do IVR</i>)		
1.2	Chamada para telefone IP local da instituição que está sendo homologada		
1.3	Chamada para ramal do PBX da instituição que está sendo homologada (<i>tem que ser bloqueada</i>)		
1.4	Chamada para RTFC da cidade da instituição que está em homologação (<i>tem que ser bloqueada</i>)		
1.5	Chamada para RTFC de uma cidade via instituição com encaminhamento nacional H.323 (<i>tem que ser bloqueada</i>) (019 4001-4001 ou 019 3731-2300)		
1.6	Chamada para RTFC de uma cidade via instituição com encaminhamento nacional SIP (<i>tem que ser bloqueada</i>) (021 4001 4001 ou 021 2548 2742)		
1.7	Chamada para PBX de uma instituição com encaminhamento nacional H.323 (019 3787-3300)		
1.8	Chamada para PBX de uma instituição com encaminhamento nacional SIP (021 2102 9660)		
1.9	Chamada para telefone IP de uma instituição com encaminhamento nacional H.323		
1.10	Chamada para telefone IP de uma instituição com encaminhamento nacional SIP		
2	Chamadas originadas da rede Interna (PBX) via IVR		
2.1	Chamada para ramal chave do PBX (<i>teste do IVR</i>)		
2.2	Chamada para telefone IP local da instituição que está sendo homologada		
2.3	Chamada para ramal do PBX da instituição que está sendo homologada (<i>tem que ser bloqueada</i>)		
2.4	Chamada para RTFC da cidade da instituição que está sendo homologada (<i>tem que ser bloqueada</i>)		
2.5	Chamada para RTFC de uma cidade via instituição com encaminhamento nacional H.323 (019 4001-4001 ou 019 3731-2300)		
2.6	Chamada para RTFC de uma cidade via instituição com encaminhamento nacional SIP (021 4001 4001 ou 021 2548		

	2742)		
2.7	Chamada para PBX de uma instituição com encaminhamento nacional H.323 (019 3787-3300)		
2.8	Chamada para PBX de uma instituição com encaminhamento nacional SIP (021 2102 9660)		
2.9	Chamada para telefone IP de uma instituição com encaminhamento nacional H.323		
2.10	Chamada para telefone IP de uma instituição com encaminhamento nacional SIP (021 1100 0092)		
3	Chamada via telefone IP da instituição que está sendo homologada		
3.1	Chamada para ramal do PBX de uma instituição com encaminhamento nacional H.323 (019 3787-3300)		
3.2	Chamada para RTFC de uma instituição com encaminhamento nacional H.323 (019 4001-4001 ou 019 3731-2300)		
3.3	Chamada para ramal do PBX de uma instituição com encaminhamento nacional SIP (021 2102 9660)		
3.4	Chamada para RTFC de uma instituição com encaminhamento nacional SIP (021 4001 4001 ou 021 2548 2742)		
3.5	Chamada para o PBX da instituição sendo homologada (se a instituição tiver interface com PBX)		
3.6	Chamada para a RTFC da instituição sendo homologada (se alguma instituição da cidade tiver interface com PBX)		
4	Chamada via telefone IP de uma instituição com encaminhamento nacional apenas via H.323		
4.1	Chamada para ramal do PBX da instituição que está sendo homologada		
4.2	Chamada para RTFC da cidade da instituição que está sendo homologada		
5	Chamadas via Telefones IPs de uma instituição com encaminhamento nacional apenas via SIP (por exemplo: UFRJ ou RNP Rio)		
5.1	Chamada para ramal do PBX da instituição que está sendo homologada		
5.2	Chamada para RTFC da cidade da instituição que está sendo homologada		
6	Restrições no GnuGK e no OpenSER		
6.1	Restrição de ligações para o número chave da instituição (tem que ser bloqueada)		
6.2	Restrição de ligações para os ramais associados ao Asterisk		

	(tem que ser bloqueada)		
6.3	Restrição para o celular deve incluir o zero antes do código de área (default é ser bloqueada)		

FIM Homologado temporariamente no novo ambiente. LabVoIP envia e-mail para o CAIS e para a RNP.			
--	--	--	--

9.

Verificações finais

A tabela abaixo é a última etapa da homologação. Esta tabela tem como finalidade apenas validações (habilitar ou desabilitar serviços, teste de conectividade, acesso a telefonista, auditoria de segurança e necessidade de habilitação de QoS).

nº	Descrição	Resultado	Observações
1	Validação		
1.1	Coleta de CDRs via Féjeca (dar tempo para a consolidação acontecer)		
1.2	A instituição deve configurar QoS no seu roteador de borda		

10.

RNP anuncia a nova instituição homologada

O LabVoIP comunica a RNP (voipadm@rnp.br) que a instituição está homologada. Em seguida, a RNP executa procedimentos administrativos e técnicos. Formato do e-mail para a RNP:

To: voipadm@rnp.br Subject: Homologada a <INSTITUICAO> Informo a RNP que a/o <INSTITUICAO> finalizou o processo de homologação com o LabVoIP. IPs das máquinas: Máquina 1: <IP máquina 1> Máquina 2: <IP máquina 2>

LabVoIP envia e-mail para o CAIS solicitando auditoria. Formato do e-mail para o CAIS:

To: cais-audit@cais.rnp.br Subject: Auditoria VoIP <INSTITUICAO>
--

Solicito ao CAIS/RNP auditoria nas máquinas da <INSTITUICAO> conforme acordado com o SI da RNP.

IPs das máquinas:

Máquina 1: <IP máquina 1>

Máquina 2: <IP máquina 2>