Serviço fone@RNP:
descrição da arquitetura

Maio de 2005

Esse documento descreve a arquitetura do serviço **fone@RNP**.

RNP/REF/0343a
Versão Final

Sumário

1.
Arquitetura

Na arquitetura do serviço **fone@RNP**, telefones IP poderão ser disseminados entre os usuários das instituições acadêmicas, com um custo relativamente pequeno de investimento. Basicamente, será preciso disponibilizar uma máquina com sistema operacional de código aberto (ex.: Linux) para hospedar os aplicativos de domínio público envolvidos e, opcionalmente, um equipamento para interconexão com o PBX da instituição (*gateway*).

O protocolo VoIP que é adotado inicialmente é o ITU-T H.323, sendo que o uso do protocolo IETF SIP e de *gateway* H.323/SIP estão sendo objeto de pesquisa nesse momento.

A arquitetura básica nas instituições participantes será composta de um *gatekeeper* H.323 (GK) para registro de terminais H.323, de um servidor Radius (com SQL associado) para contabilização das chamadas, de um servidor LDAP para autenticação de usuário e de um *gateway* de voz para a interconexão do PBX, conforme mostrado na Figura 1.1. Os usuários de PC multimídia, rodando software de cliente H.323, são telefones IP com numeração E.164, sendo registrados no GK. O ATA, mostrado na Figura 1.1, é um exemplo de equipamento que interconecta com a rede e suporta a conexão de um ou mais telefones analógicos, que passam a operar como terminais H.323, também registrados no GK. As instituições podem ter também telefones IP dedicados, que são conectados à rede de dados e registrados diretamente no GK, e que operam funcionalmente como terminais H.323.

O *gateway* estará conectado ao PBX da instituição e será responsável por encaminhar as chamadas para os ramais internos ou para telefones públicos, com base em prefixos que serão adotados no plano de numeração. Estão previstas duas formas de conexão ao PBX: a primeira através de ramais analógicos, quando são utilizadas portas FXO (*Foreign Exchange Office*); e a segunda através de interfaces digitais do tipo E1.

Um elemento essencial no H.323 é o *gatekeeper*, cuja principal função é o registro dos usuários on-line e a localização do destino das chamadas. Como o *gatekeeper* será responsável pelo controle de terminais H.323 e *gateways,* é necessário que cada instituição participante disponha de seu próprio *gatekeeper*, cuja gerência será de responsabilidade da instituição, mas com permissão total de acesso pela gerência da RNP.

Como padrão do serviço será utilizado o *gatekeeper* GnuGK, de código fonte aberto, que pode ser instalado em servidores Unix e Windows. Apesar de não haver restrições em relação ao sistema operacional que deve ser utilizado, é recomendável o uso do sistema operacional Linux, facilitando o gerenciamento remoto e a instalação de outros softwares que serão utilizados.

Todos os terminais e *gateways* H.323 deverão se registrar em um dos *gatekeepers* existentes, através de registro estático ligado ao IP, ou através de autenticação dinâmica, via protocolo H.235 (conta/ senha). Este registro será utilizado para a localização de usuários, e todos os *gatekeepers* envolvidos devem ser configurados para permitirem chamadas somente para terminais[1] registrados.

[1] No contexto do projeto, os termos terminal e usuário são utilizados com a mesma função, indicando terminais H.323, e a ramais telefônicos alcançáveis através dos *gateways* de voz. Cada *gateway* será responsável por um conjunto de ramais identificados por um prefixo associado ao plano de numeração da instituição.

A localização dos usuários de outras instituições será feita inicialmente a partir do plano de numeração operando sobre uma estrutura de *gatekeepers* em árvore, com os GKs das instituições nas folhas e um *Directory Gatekeeper* (DGK) na raiz. O DGK permitirá que os *gatekeepers* das instituições possam localizar o destino das chamadas de acordo com os prefixos que serão adotados no plano de discagem.

O DGK será responsável em redirecionar os pedidos de localização (LRQ – *Location Requests*) para o *gatekeeper* onde deverá estar registrado o terminal a que se destina uma chamada. As instituições terão que utilizar o DGK como o *gatekeeper* padrão para a localização de usuários. O *gatekeeper* da instituição somente deverá aceitar chamadas iniciadas através do DGK. O DGK permitirá também a localização de usuários de instituições que participam da Internet2.

O *gatekeeper* terá outras funções associadas à admissão das chamadas, garantindo que somente usuários autorizados possam fazer uso do serviço. A instituição participante terá a responsabilidade de garantir que o seu *gatekeeper* esteja configurado corretamente em relação aos usuários autorizados. A autorização poderá ser baseada no endereço IP dos terminais H.323 ou em autenticação dinâmica via conta/senha, usando o protocolo H.235. Neste último caso, a instituição deverá ter seu mecanismo particular de cadastro de usuários.

Para a configuração de *gateway* analógico deve-se atentar para o número de portas FXO disponíveis, pois são elas que irão limitar o uso do serviço (chamadas simultâneas). Estas portas de voz podem ser conectadas a qualquer ramal analógico, utilizando a sinalização *loop-start (*mais utilizado) ou *ground-start*.

Um *gateway* que utilize interface E1 terá o número de ligações limitado pela quantidade de DSP's (*Digital Signal Processor*) instalados. Os *gateways* desse tipo poderão está configurados com interface que permita realizar até 30 chamadas simultâneas, enquanto outros poderão ter limitação no número de chamadas simultâneas, dependendo da complexidade do *codec* utilizado na comunicação sobre IP. A sinalização recomendada por questões de eficiência do serviço é a ISDN (*Integrated Services Digital Network*), podendo, opcionalmente, usar a E1/R2.

As configurações adotadas permitem a conectividade de *gateways* com um mínimo de mudanças na configuração dos PBX's. Quando forem utilizadas portas FXO, não é necessária qualquer alteração na programação do PBX, sendo sugerido que um número único apenas seja associado aos ramais conectados ao *gateway*, para facilitar o uso do serviço. No caso das portas E1 será necessária uma configuração no PBX, associando um número único de ramal aos 30 troncos. As instituições devem providenciar a configuração do PBX, adequando-o a estas necessidades. Este procedimento de configuração do PBX é considerado básico e deverá ser feito internamente, pela própria instituição. Para permitir a separação de escopo de permissão entre chamadas internas e chamadas originadas externamente, vindas da rede pública de telefonia, cuidados especiais serão tomados na configuração do PBX e *gateway*.

A implantação do servidor Radius em cada instituição é fundamental para garantir robustez ao processo de autenticação via H.235 e para que o serviço possa ser gerenciado adequadamente. Associado ao Radius, deverá ser instalado um banco de dados SQL e um servidor de diretórios LDAP. No banco de dados estarão sendo coletadas as estatísticas de uso relacionadas a chamadas envolvendo o *gateway* local e o *gatekeeper*. No servidor de diretórios serão armazenadas as informações (conta/senha/alias) que permitirão aos usuários de ramais IP se registrarem no GK da instituição. O servidor Radius, o banco de dados SQL e o servidor de diretórios poderão ser instalados

na mesma máquina em que roda o *gatekeeper*, não necessitando de um equipamento dedicado. O requisito, entretanto, é que todos operem 24h, sem interrupção. O Radius, o LDAP e o banco SQL podem ser replicados para aumento de confiabilidade e disponibilidade.

O serviço também prevê o uso de equipamentos dedicados, como por exemplo, Cisco ATA188 configurados com duas portas de voz e uma ethernet, permitindo ter até dois telefones analógicos conectados à rede IP. Estes tipos de equipamentos devem se registrar no GK da instituição.

Utilizando os elementos descritos acima, serão possíveis dois cenários nas instituições participantes:

- **Cenário 1** – ambiente completo; composto de PBX, *gateway, gatekeeper*, Radius, SQL e LDAP. Eventuais terminais H.323 podem ser PC's, telefones IP ou ATA's. Este é o cenário recomendado;
- **Cenário 2** – ambiente composto de *gatekeeper*, Radius, LDAP e SQL. Eventuais terminais H.323 podem ser PC's, telefones IP ou ATAs.

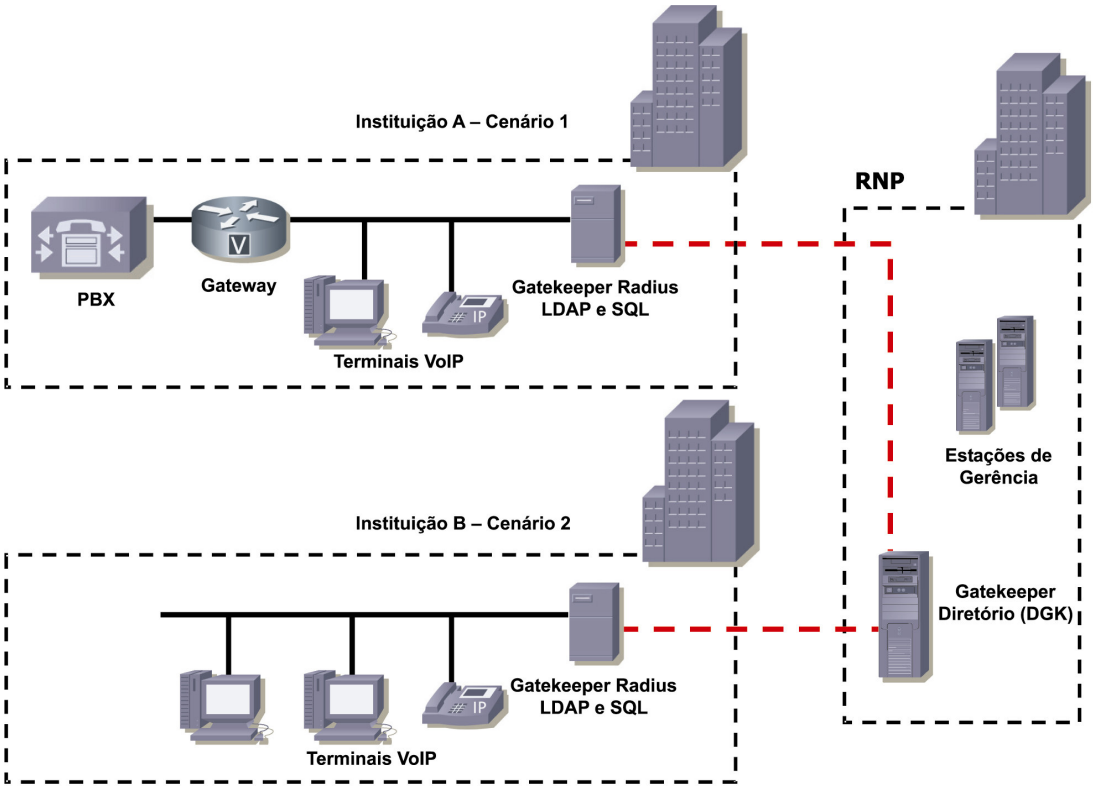

Figura 1.1 - Cenários básicos VoIP no serviço fone@RNP

1.1. Plano de numeração

Para entendermos o plano de numeração e endereçamento do serviço, é necessário ter em mente os tipos básicos de terminais relevantes:

- **Terminais VoIP** – São softwares instalados em computadores (Ohphone, Openphone, GnomeMeeting, Windows NetMeeting etc.), dispositivos adaptadores para telefones analógicos e dispositivos IP dedicados. Um terminal VoIP também é conhecido como telefone IP.

- **Terminais de PBX** - São os ramais convencionais dos sistemas privados de telefonia das instituições participantes, conectados via *gateway*.

- **Terminais da rede de telefonia pública** - São telefones ordinários, fixos ou móveis (celulares), conectados às operadoras de serviço público comercial.

1.1.1. Regras para formação dos identificadores

- **Terminais VoIP**

Os identificadores serão da forma:

<CA>1<ORG><TERM>

CA: Código de Área (2 dígitos) - o mesmo código DDD usado na telefonia convencional da cidade onde se localiza a instituição;

1: Identifica explicitamente a natureza do número. A presença do "1" marca bem o fato de ser esse um telefone IP, e evita possíveis confusões com telefones válidos da rede pública;

ORG: Prefixo VoIP da instituição (3 dígitos) - a ser adotado independentemente da localização geográfica da instituição. O prefixo é único dentro da mesma área de DDD, portanto, podendo vir a se repetir em regiões onde o Código de Área não for o mesmo. Cabe a RNP a decisão final pela escolha deste número;

TERM: identificador do terminal VoIP, sempre na forma de quatro dígitos numéricos XXXX.

- **Terminais de PBX**

Os identificadores serão herdados da telefonia convencional.

<CA><Prefixo><Ramal>

CA: Código de Área (2 dígitos) - o mesmo código DDD usado na telefonia convencional da cidade onde se localiza a instituição;

PREFIXO: Deve ser utilizado o mesmo prefixo já associado ao PBX da instituição. Caso a instituição utilize mais de um prefixo no seu plano de numeração da telefonia, será possível a associação de mais de um prefixo à instituição, quando autorizado pela gerência do serviço;

RAMAL: Será utilizado para identificar o ramal PBX do usuário dentro da instituição.

Exemplo de números utilizados:

Telefone IP: 21 1 100 4201, onde:

- 21 → identifica uma instituição que funciona na cidade do Rio de Janeiro;
- 1 → identifica um telefone IP, ou seja, é um identificador associado a um terminal da rede VoIP;
- 100 → prefixo VoIP da instituição, no caso a UFRJ;
- 4201 → número de ramal IP, identifica o usuário do telefone IP.

Telefone PBX: 21 2598 3354, onde:

- 21 → identifica uma instituição localizada na cidade do Rio de Janeiro;
- 2598 → prefixo da telefonia convencional, no caso a UFRJ;
- 3354 → número de ramal PBX, identifica o usuário.

1.1.2. Regras de discagem

Para manter certa similitude com a rede pública e tornar intuitivo o uso do sistema, todos os terminais serão atingidos a partir do fone@RNP com as seguintes regras de discagem:

- **Chamadas nacionais**

```
0 + <código de área> + <número telefônico>
```

Exemplo: 0 19 3787 3300 (chamada para um telefone convencional na cidade de Campinas-SP)

- **Chamadas locais**

```
<número telefônico>
```

Exemplo: 1005 3300 (chamada para um telefone IP da mesma cidade)

O serviço também permite chamadas internacionais (para instituições parceiras). A regra de discagem também é semelhante à encontrada na telefonia convencional:

- **Chamadas internacionais**

```
00 + <código do país> + <código de área> + <número telefônico>
```

Exemplo: 00 1 216 555 1234 (chamada para um telefone dos Estados Unidos)

Importante:
As regras de discagem nacional e internacional devem estar disponíveis para todos os terminais de voz. Mesmo que essas opções, em um primeiro momento, não façam sentido, elas representam uma alternativa a mais para os usuários do serviço. Já a regra para chamadas locais é opcional, podendo ser implementada a critério da instituição, e só será corretamente interpretada para um destino na mesma área DDD do terminal de voz que origina a chamada.

O DGK está configurado para encaminhar os pedidos de localização (LRQs) para os *gatekeepers* das instituições, de acordo com o plano de numeração definido. Uma instituição deve configurar seu *gatekeeper* para direcionar para o terminal correspondente as chamadas recebidas tendo como destino um prefixo alocado a ela. Por outro lado, uma chamada recebida no GK e destinada para outros prefixos deve usar o DGK para localizar o GK de destino.

No caso do destino de uma chamada ser um ramal do PBX local, o GK deve encaminhar a chamada para o *gateway*, que a encaminhará para o PBX. O *gateway* deve ser configurado para usar o *gatekeeper* para o encaminhamento de chamadas não associadas ao PBX. Opcionalmente, o *gateway* pode ser configurado para encaminhar ao PBX chamadas direcionadas à telefonia pública. Nesta situação, o *gateway* direciona a chamada ao PBX, para que este a encaminhe para a concessionária pública. Este procedimento só deve ser permitido para chamadas internas ao VoIP, isto é, provenientes de ramais de PBX ou de terminais VoIP.

O roteamento de chamadas destinadas a telefones da rede de telefonia pública, através do PBX de uma instituição, é um serviço estendido disponível apenas para a comunidade acadêmica. Procedimentos especiais estão adotados para garantir esta forma de operação e evitar que o serviço fone@RNP venha a infringir o marco regulatório vigente.

A fim de permitir o uso do serviço a partir de ramais do PBX ou da telefonia pública sem alterações na configuração do PBX, o usuário fará a opção explícita pela utilização do fone@RNP, discando para um número de ramal, associado às portas do *gateway*. Estas portas, FXO ou E1, serão associadas a aplicações IVR (*Interactive Voice Response*), de forma que o usuário receba uma mensagem de voz, ao ser atendido pelo *gateway*. Esta mensagem irá orientá-lo no uso do serviço. O usuário deverá então discar para um ramal seguindo a numeração e regras de discagem apresentadas acima.

Caso uma instituição utilize um *gateway* sem suporte a IVR interno, é possível a utilização de IVR externo, caso o *gateway* suporte a transferência de chamada padronizada na recomendação H.450.

1.2. Segurança

O protocolo H.323 apresenta um comportamento bastante desafiador para os requisitos de segurança de uma rede. Uma chamada H.323 envolve uma série de fluxos IP, alguns associados à sinalização e outros aos próprios canais de mídia. Na sinalização são utilizados os protocolos H.225 (mensagens RAS e Q.931) para o estabelecimento e a finalização das chamadas e o H.245 para a negociação, estabelecimento e controle dos canais de mídia. Já a mídia é transmitida através do protocolo RTP (*Real Time Protocol*), ao qual está associado o protocolo RTCP (*Real Time Control Protocol*). Considerando que os canais de mídia são unidirecionais, são necessários pelo menos dois canais para a transmissão da voz. Desta forma, para que uma chamada ocorra, serão necessários pelo menos 4 fluxos, alguns utilizando TCP, como é o caso da sinalização, e outros, UDP.

Outro detalhe importante é que somente o protocolo H.225 trabalha com portas TCP fixas e definidas, enquanto os outros fluxos usam portas estabelecidas dinamicamente pelos elementos H.323 envolvidos, anunciadas durante a sinalização. Como as chamadas podem ser iniciadas a partir da rede externa para a interna, ou vice-versa, um *firewall* teria que ser configurado para permitir a abertura de um grande número de portas, como apresentado na Tabela 1.1, o que deixaria a rede interna desprotegida.

As informações sobre as portas TCP ou UDP utilizadas pelos fluxos do protocolo H.323 são definidas na sinalização, ao nível de aplicação. Isso causa problemas quando usamos NAT na rede, pois as traduções de IP e de portas (no caso de PAT) só são realizadas ao nível da camada de rede, não sendo feito nenhum ajuste ao nível de aplicação, dificultando o uso de H.323 com NAT.

Função	***Protocolo***	***Porta***
Gatekeeper Discovery	UDP	1718
Gatekeeper RAS	UDP	1719
Q.931 Call Setup	TCP	1720
H.245 Control Channel	TCP	1024-65535
RTP/RTCP	UDP	1024-65535
H.235 (Segurança)	TCP	1300

Tabela 1.1 - Portas utilizadas por aplicações VoIP H.323

Várias alternativas podem ser utilizadas para permitir o uso de H.323 em conjunto com NAT e firewalls. O GnuGK pode ser configurado para realizar as adaptações necessárias na sinalização, quando os fluxos passam através de NAT. Para isto, é necessário que toda a sinalização seja encaminhada através do GK, ou seja, toda a sinalização entre dois elementos H.323 deve passar através do GK. Este então fará as adaptações necessárias. Este comportamento é realizado com a correta configuração do GK. Desta forma, é necessário que todos os terminais e *gateways* H.323 sejam configurados para utilizar o GK, caso contrário não poderão se comunicar. Este modo de operação garantirá o funcionamento do serviço em ambientes utilizando NAT, não sendo uma solução para redes onde é empregado NAT/PAT entre terminais ou *gateways* H.323 e o *gatekeeper*.

O GnuGK também deve ser configurado para atuar como *proxy* dos fluxos de mídia, solucionando o problema associado aos *firewalls*. Posicionando o GK em uma DMZ é possível configurar o firewall para permitir fluxos TCP e UDP para esta máquina, tanto de redes externas, quanto de redes internas. Através da configuração do GK, a faixa de portas TCP e UDP utilizadas pelos fluxos H.323 pode ficar restrita a uma faixa pré-estabelecida, facilitando a configuração do *firewall*. O uso do GK como proxy irá também facilitar o estabelecimento de QoS na RNP.

O *gatekeeper* operando como *proxy* dos fluxos RTP/RTCP deve ter acesso direto às redes interna e externa. Como esta configuração provocaria um sério problema à segurança da rede interna é recomendado que o GK, junto com o *gateway* de voz, seja instalado em uma rede DMZ (atrás de firewall, mas aberta para acessos externos). Neste caso, o GK deve ser capaz de encaminhar pacotes IP para a rede interna sem que estes sejam traduzidos por NAT.

RECOMENDAÇÃO IMPORTANTE: O *gateway* e o *gatekeeper* devem ter IPs válidos, com acesso à rede externa sem passar por equipamentos que implementem NAT.

1.3. Autenticação de usuários

O registro no *gatekeeper* (requisições RRQ e ARQ) deve ser restrito ao *gateway* de voz da instituição e a terminais H.323 autorizados pela instituição.

A restrição baseada em IP é adequada para a utilização de um telefone IP em um local definido da instituição.

Para suporte a mobilidade, recomenda-se o uso de telefones IP (terminais H.323) com suporte ao protocolo H.235, que possibilita a autenticação baseada em conta/senha. Neste caso, o usuário, que é pré-cadastrado, tem suas informações de conta/senha/*alias* salvas no LDAP. A informação de *alias* é o número de telefone IP do usuário. Rotinas para cadastro e inserção automática das informações no serviço de diretórios estão disponíveis para as instituições.

Quando da autenticação no GK, o usuário precisa configurar apenas conta/senha em seu telefone IP. Qualquer que seja o número IP (*alias)* configurado no seu aplicativo de telefone IP, ele será reescrito com a informação já constante do LDAP. Este procedimento é muito importante, pois evita que um usuário registre um número IP errado, inibindo o registro do real detentor daquele número.

O uso de clientes H.323 que não suportam H.235, como Netmeeting, deve ser restrito apenas a autenticação por IP.

O uso de requisições LRQ entre *gatekeepers* deve ficar restrito às provenientes do DGK. O DGK será configurado para permitir requisições LRQ provenientes dos *gatekeepers* das instituições participantes e da Internet2.

1.4. Configuração QoS na rede

A qualidade de uma conexão VoIP depende diretamente da performance e disponibilidade de recursos da rede de dados sendo utilizada. Perda de pacotes, atrasos (*delay*) e variações de atraso (*jitter*) contribuem para a degradação da qualidade de voz. Além disto, congestionamentos na rede (mais precisamente, saturação de *buffers* em algum ponto da rede) podem ocorrer a qualquer momento durante a conexão VoIP.

Para se obter a qualidade do serviço VoIP desejada, é necessário implementar mecanismos que reduzam o número de pacotes descartados em momentos de congestionamento na rede e minimizem o atraso e o *jitter* existentes durante a conexão.

1.4.1. Requisitos de QoS para conexões VoIP

A qualidade de voz é diretamente afetada pelos seguintes fatores de QoS: perda, atraso e jitter.

A perda de pacotes torna a conexão “picotada” e com falhas. Alguns algoritmos de codificação podem corrigir até 30 ms de pacotes de voz perdidos. Atrasos começam a causar degradação na qualidade de voz somente quando superiores a 200 ms. Quando o atraso atinge 250 ms, por exemplo, obtém-se aquela sensação desconfortável de demora na recepção da voz, como ocorre em ligações feitas utilizando-se satélites de comunicação. O padrão ITU para VoIP (G.114) especifica que o atraso máximo em um sentido deve ser de 150 ms para conexões de alta qualidade, no entanto a utilização de 200 ms como atraso máximo tem se mostrado ainda satisfatória. Dependendo dos buffers adaptativos de compensação de jitter, utilizados em aplicações VoIP, variações de 20 a 50 ms podem ser compensadas.

O máximo e o mínimo recomendados para o tamanho do buffer de compensação de jitter são 25 ms e 100 ms, respectivamente. No caso do Openphone, os tamanhos recomendados a serem configurados são 50 ms e 200 ms, mínimo e máximo, pois de fato os valores utilizados são as metades dos especificados.

A largura de banda necessária para uma conexão VoIP não é muito significativa, quando comparada com outros tipos de aplicação. Depende diretamente do CODEC sendo utilizado, do tamanho da taxa de amostragem e do tipo de enlace, podendo variar entre 21 Kbps e 106 Kbps.

Resumindo, os seguintes valores, numa comunicação fim a fim, devem ser considerados para atender os requisitos de VoIP:

- A **perda** de pacotes dever ser no **máximo de 1%**;
- O **atraso** entre origem e destino (*one-way latency)* **não deve ultrapassar 150-200 ms**;
- O *jitter* médio não deve ser superior a 30 ms;
- **21-106 kbps** devem ser **garantidos por chamada estabelecida**, dependendo da taxa da amostragem, o *codec* sendo utilizado e *overhead* do encapsulamento do nível 2 sendo utilizado no meio físico.

1.4.2. Configuração QoS na rede interna da instituição

Para se obter uma boa qualidade em VoIP, a rede local da instituição também deve ser levada em consideração. Com este objetivo, devem ser observados os seguintes itens:

- A rede local não deve estar saturada e os elementos que farão parte do serviço VoIP (*gateways, gatekeepers* e terminais H.323) devem ser atendidos através de uma rede totalmente comutada;
- Cuidado especial deve ser tomado em relação aos buffers das interfaces para que não haja descarte de pacotes. Quando possível, utilizar a especificação IEEE 802.1Q e 802.1p, que permite priorização de tráfego ao nível da camada de enlace. O valor normalmente associado ao serviço de voz é COS 5.