PROXYSIP BRIDGE: UMA ABORDAGEM PARA CRIAR UMA INFRAESTRUTURA VOIP DIFERENCIADA

PROXYSIP BRIDGE: AN APPROACH TO CREATE A DIFFERENTIATED VOIP INFRASTRUCTURE

Fernando **BARRETO** [1]

[1] Universidade Tecnológica Federal do Paraná – UTFPR – Câmpus Apucarana – PR / Brasil - fbarreto@utfpr.edu.br

RESUM O

Este artigo apresenta um estudo da tecnologia Voz sobre IP (VoIP) para a elaboração de uma infraestrutura VoIP diferenciada utilizando a abordagem proposta ProxySIP Bridge. Essa abordagem é um aperfeiçoamento da abordagem TURN simplificado (TURN-S), que é designada para contornar Firewall e NAT. O ProxySIP Bridge isola o tráfego de voz dos demais tráfegos de propósito geral, possibilita o tráfego de voz ocorrer direto entre origem e destino quando possível, e reduz a sobrecarga de sua interface de rede. Uma implementação dessa infraestrutura VoIP diferenciada com ProxySIP Bridge é apresentada, mostrando ser uma alternativa à abordagem TURN-S.

Palavras-chave: ProxySIP Bridge, Infraestrutura VoIP, TURN-S, Firewall, NAT.

ABSTRACT

This article presents a study for Voice over IP (VoIP) technology to elaborate a differentiated VoIP infrastructure with the proposed approach ProxySIP Bridge. This approach enhances the simplified TURN (TURN-S) approach, which is designated to bypass Firewall and NAT. The ProxySIP Bridge isolates the voice traffic from the remaining general purpose traffic, enables direct voice traffic from source to destination whenever possible, and reduces overloading of its network interface. An implementation of this differentiated VoIP infrastructure with ProxySIP Bridge is presented, which shows to be an alternative to TURN-S approach.

Keywords: ProxySIP Bridge, VoIP infrastructure, TURN-S, Firewall, NAT.

1. INTRODUÇÃO

Com a difusão e os avanços das tecnologias de redes de computadores, as infraestruturas de rede de dados IP e de telefonia estão hoje cada vez mais próximas no provimento de serviços de voz. No entanto, ambas trabalham de forma diferente: as infraestruturas de rede IP utilizam a comutação por pacotes, enquanto as infraestruturas convencionais de telefonia adotam a comutação por circuito (*Public Switched Telephone Network* - PSTN). A comutação por circuito fornece um ambiente propício para realizar tráfego de voz, uma vez que reserva recursos entre origem e destino. A comutação por pacotes foi planejada para tráfego em geral de dados, pois não há uma reserva de recursos entre origem e destino. No entanto, com os avanços das tecnologias de Voz sobre IP (VoIP), essas redes de dados IP se tornaram propícias para o tráfego de voz a um nível considerado aceitável.

O uso de redes IP para tráfego de voz possibilita o surgimento de uma variedade de inovações na forma como ocorre uma comunicação por voz entre pessoas. Recentemente pessoas procuram cada vez mais diversificar as formas de comunicação (e-mail, voz, vídeo, mensagens instantâneas). As redes de telefonia convencional, que funcionam por comutação por circuito, não são preparadas para atender a essa grande variedade de comunicações multimídia e é nesse ambiente que as redes de dados IP estão se mostrando mais atrativas (COLLINS, 2002).

No caso específico de voz, empresas com um ambiente corporativo de várias filiais identificam no VoIP uma grande chance para redução de gastos com telefonia. No ambiente acadêmico, essa redução de custos também se mostra interessante, principalmente se uma universidade é composta por vários campi, como a Universidade Tecnológica Federal do Paraná (UTFPR). A UTFPR possui vários campi espalhados pelo estado do Paraná e a comunicação por voz ocorre, na sua totalidade, via telefonia convencional, o que acarreta altos custos nas ligações.

Não existe um padrão definido para elaborar uma infraestrutura VoIP, no entanto existem vários pontos importantes que devem ser considerados, principalmente em se tratando de *Firewall* e *Network Address Translation* (NAT) (BOULTON et al., 2011).

Este artigo realiza um estudo desses pontos e das soluções para elaborar uma infraestrutura VoIP que necessite de poucas modificações, tanto no *Firewall* e NAT, quanto no software dos equipamentos do usuário final. Com esses requisitos, acredita-se que a complexidade de uma infraestrutura VoIP passe a ser reduzida. Dentre as soluções apresentadas nesse estudo, a abordagem TURN simplificado (GONÇALVES, 2010), que é derivado da abordagem TURN (MAHY et al., 2010), consegue atender à infraestrutura VoIP desejada. Para facilitar a identificação da abordagem TURN simplificado no texto, utiliza-se TURN-S.

Ao realizar um estudo detalhado da abordagem TURN-S, foram identificados problemas relacionados à carga da interface de rede, ao uso permanente do TURN-S como intermediário de qualquer sessão de tráfego de voz e à concorrência do tráfego de voz com tráfego de propósito geral no *Firewall*/NAT.

Esses problemas podem comprometer a correta operação de um ambiente VoIP, o que motivou o desenvolvimento deste trabalho para apresentar a abordagem *ProxySIP Bridge*. Essa abordagem aperfeiçoa a abordagem TURN-S para contornar esses problemas e, ao mesmo tempo, permite elaborar uma infraestrutura VoIP diferenciada com políticas personalizadas para melhor distribuir o tráfego de voz entre equipamentos VoIP. A abordagem *ProxySIP Bridge* com a infraestrutura VoIP diferenciada foi implementada para testes com sucesso em um campus da UTFPR utilizando aplicativos de software livre para poder ser adaptado e amplamente utilizado pela comunidade acadêmica.

Este artigo apresenta na seção 2 um breve estudo da tecnologia VoIP identificando pontos importantes, principalmente nos casos de *Firewall* e NAT. Na sequência, é apresentado várias abordagens com soluções para os problemas apresentados. A abordagem TURN simplificado é apresentada na seção 3. A seção 4 apresenta a abordagem proposta *ProxySIP Bridge*. A seção 5 apresenta o planejamento da infraestrutura VoIP diferenciada com *ProxySIP Bridge* em um campus da UTFPR e os testes realizados. Por fim, os trabalhos futuros e uma conclusão são apresentados.

2. VOZ SOBRE IP

A tecnologia VoIP não é recente, teve sua origem na década de 80 e a sua adoção começou a se difundir no final da década de 90. Da mesma forma que na PSTN, para estabelecer uma chamada VoIP é necessário grande parte dos procedimentos de uma chamada telefônica: discar o número do telefone destino, localizar e sinalizar o telefone destinatário para efetuar um toque sonoro, informar a origem que o telefone destino está tocando, quando o destino atender deve-se sinalizar e estabelecer o fluxo de voz de ida e volta entre os telefones, ao desligar deve encerrar o fluxo de voz e indicar o desligamento de telefone para ambas as partes. Todos esses procedimentos também devem ser realizados na tecnologia VoIP.

Para organizar a sinalização e estabelecimento de uma chamada telefônica VoIP, utiliza-se protocolos de comunicação definidos ou pela norma H.323 (H.323, 1998) ou pelo padrão *Session Initiation Protocol* (SIP) (ROSENBERG, 2002). Tanto o H.323 quanto o SIP podem utilizar os protocolos TCP ou UDP da pilha TCP/IP para transporte de dados referentes à sinalização de chamada. Para transportar o fluxo de dados contendo o áudio da voz digitalizado, tanto o H.323 quanto o SIP utilizam o protocolo *Real-Time Transport Protocol* (RTP) (SCHULZRINNE,

2003), e para monitorar as mensagens RTP utiliza-se o *RTP Control Protocol* (RTCP) (SCHULZRINNE, 2003). O RTP e RTCP utilizam o protocolo de UDP, pois o fluxo do tráfego de áudio é sensível ao tempo de entrega.

2.1 H.323

A norma H.323 (H.323, 1998) é definida pela *International Telecommunication Union* (ITU) e apresenta um conjunto completo de recomendações detalhadas com protocolos específicos para codificação de som, estabelecimento de chamadas, sinalização e transporte de dados. Essas recomendações têm por objetivo padronizar a sinalização de sessões multimídia, tanto de voz quanto de vídeo, em redes de dados IP. O H.323 começou a ser implementado em equipamentos no final da década de 90, no entanto foi observado que esse padrão era demasiadamente extenso, pouco flexível e com grande complexidade o que encarecia os equipamentos VoIP e dificultava a sua adoção.

2.2 SIP

Dada a complexidade dos protocolos definidos no H.323, a *Internet Engineering Task Force* (IETF) propôs um protocolo leve, simples e extensível para organizar a sinalização de sessões de áudio denominado *Session Initiation Protocol* (SIP) (ROSENBERG, 2002). Essa simplicidade acarretou em uma implementação facilitada com uma consequente queda no custo de equipamentos VoIP e aumento da sua utilização em relação ao H.323.

A identificação dos usuários (usuários SIP) ocorre por meio de *Uniform Resource Identifier* (URL), por exemplo: *sip:fulano@utfpr.edu.br* identifica um usuário SIP *fulano* que pertence ao domínio SIP *utfpr.edu.br*. Um sistema que age em nome de um usuário e implementa o protocolo SIP (ex: telefone VoIP) é denominado *User Agent* (UA).

Dentre os métodos definidos no protocolo SIP e utilizados por um UA na configuração de uma chamada VoIP são: inicialização (INVITE), confirmação (ACK), término (BYE). Os métodos INVITE e BYE necessitam de uma resposta do UA remoto para confirmar a ação do método.

A mensagem INVITE carrega, além de informações para identificar o UA destino e o UA origem, informações adicionais para o protocolo RTP referentes à sessão de voz do UA origem. Essas informações adicionais são descritas no corpo da mensagem INVITE de acordo com o protocolo *Session Description Protocol* (SDP) (HANDLEY; JACOBSON; PERKINS, 2006), como detalhes de Codec, endereço IP e porta. Essas informações são utilizadas pelo UA destino para configurar a sessão de voz a ser enviado por RTP. O UA destino, ao aceitar a mensagem INVITE (sinalizado pelo atendimento do telefone pelo usuário), responde com uma mensagem contendo um código de resposta OK.

O corpo da resposta OK contém informações no SDP referente à sessão de voz do UA destino.

Quando a mensagem OK chega ao UA origem, ambos possuem as configurações necessárias para iniciar a sessão de voz com RTP, e o UA origem envia um ACK para o UA destino confirmando a sessão de voz e assim inicia a transmissão do áudio. O UA destino, ao receber a confirmação ACK, também inicia a sua transmissão de áudio.

Tanto o UA origem quanto UA destino podem encerrar a sessão de voz ao enviar uma mensagem BYE, que deve ser confirmada pelo UA remoto com uma mensagem OK e assim encerrar a sessão. Para maiores detalhes do fluxo de mensagens do protocolo SIP ver em (ROSENBERG, 2002).

Em ambientes maiores com vários UAs pertencentes a um mesmo domínio SIP, é recomendado utilizar um serviço centralizado de *Proxy* (ROSENBERG, 2002), denominado aqui de *ProxySIP*.

Um *ProxySIP* permite controlar e autenticar os registros dos UAs ao incorporar um *SIP registrar server* (ROSENBERG, 2002). Os UAs localizam o *ProxySIP* pelo seu endereço IP anunciado em um registro SRV no serviço de DNS como sendo o responsável pelo domínio SIP. O *ProxySIP* facilita a localização dos UAs em um domínio SIP. Além da localização dos UAs, o *ProxySIP* pode gerenciar o roteamento das mensagens SIP trocadas entre os UAs com o objetivo de controlar o fluxo de mensagens SIP. Para tanto, a especificação SIP define os campos *VIA* e *Record-Route/Route* para conseguir rotear toda a transação (qualquer mensagem de requisição com sua respectiva resposta, por exemplo INVITE e uma resposta OK) e diálogo SIP (desde o INVITE até o BYE) entre os UAs (ROSENBERG, 2002).

2.3 Codec e Qualidade de Serviço

A sessão de voz transportada por RTP é configurada através do SDP, que também identifica qual o codificador/decodificador (Coder/Decoder ou Codec) de compressão será utilizado para digitalizar o áudio de voz.

Existem vários Codecs disponíveis padronizados por organizações como a ITU. O uso de Codec pode requerer ou não licença para uso e a diferença entre os Codecs está no funcionamento do algoritmo de compressão/descompressão de áudio, largura de banda necessária e qualidade. Para maiores detalhes sobre Codecs ver em (G.SERIES, 2011) (CISCO SYSTEMS, 2002). A qualidade pode ser mensurada através de índices como o *Mean Opinion Score* (MOS) (P.800, 1996) (CISCO SYSTEMS, 2002). Esse índice pode variar entre 1 (péssimo) a 5 (excelente) em relação à percepção de mudança na voz depois de aplicação do Codec. A Tabela 1 apresenta alguns dos principais Codecs da ITU.

A Largura de Banda p/ Voz é a taxa de bits necessária para transmissão do Codec. A Largura de

Banda Total considera o *overhead* de todos os cabeçalhos TCP/IP necessários (Cabeçalho Ethernet + IP + UDP + RTP + Fim Ethernet = 78 bytes) e um *voice payload* (amostras de voz por pacote IP) de 20ms para esses Codecs. O valor de 20ms é adotado como padrão em várias implementações, como a apresentada no IOS Cisco (CISCO, 2006b).

Escolher quais Codecs poderão ser usados em uma infraestrutura VoIP torna-se importante, uma vez que influencia diretamente na escolha dos equipamentos por suportar ou não um determinado Codec. O Codec G.711 é o único suportado por todos os UAs disponíveis, uma vez que é o Codec nativo da telefonia digital convencional.

Além dos Codecs, é necessário estipular garantias para que os tráfegos das sessões de voz atendam à qualidade esperada de uma transmissão de voz. Ao contrário de uma rede de telefonia, o tráfego de sessão de voz em redes IP concorre com tráfego de propósito geral, e nesse caso é importante considerar quesitos de Qualidade de Serviço (QoS): vazão mínima, atraso, *payload* reduz a influência do *overhead* dos cabeçalhos TCP/IP, no entanto aumenta o atraso dos pacotes IP por aguardar o seu preenchimento com as amostras de áudio (CISCO, 2006b) (HARDY, 2003). Essa Largura de Banda Total na Tabela 1 refere-se apenas a uma direção de tráfego (ida ou volta), portanto em uma infraestrutura VoIP é importante considerar esse tráfego em *full-duplex*.

O atraso dos pacotes IP afeta o tempo de transmissão da voz, da boca até o ouvido do receptor (*Mouth-to-Ear delay*) (JIANG; KOGUSHI; SCHULZRINNE, 2003), que não deve ultrapassar 150ms para a transmissão ser transparente aos usuários (G.114, 1996). Próximo dos 250ms é considerado aceitável, mas em torno de 400ms já inviabiliza uma transmissão de voz (G.114, 1996) (CISCO, 2006a). Vários fatores podem influenciar esse atraso: Codecs, *jitter buffer*, rotas, *Firewall*/NAT, atraso na propagação dos enlaces e valor de *voice payload* (CISCO, 2006a) (G.114, 1996).

A variação do atraso é a variação entre as chegadas dos pacotes, geralmente acarretadas por congestionamentos. Essa variação faz com que um sinal de voz não fique na taxa de bits constante para operação

* Tabela 1 – Alguns dos Principais Codecs da ITU

Codec	**Largura de Banda p/ Voz**	**Largura de Banda Total (*voice payload* 20ms)**	**MOS** (CISCO SYSTEMS,2002)
G.711	64 Kbps	95.2 Kbps	4.1
G.726	32 Kbps	63.2 Kbps	3.85
G.728	16 Kbps	47.2 Kbps	3.61
G.729a	8 Kbps	39.2 Kbps	3.9

do Codec (ver Tabela 1), inviabilizando o Codec de regerar a onda analógica de voz. O uso de *jitter buffer* no UA destino pode amenizar esse problema ao armazenar as mensagens de voz para manter uma taxa constante do Codec. No entanto, esse recurso não pode ultrapassar o tempo de atraso de 250ms (JAMES; CHEN; GARRISON, 2004).

A taxa de pacotes perdidos pode ser influenciada por descartes causados por congestionamentos ou pelo *jitter buffer*. O *jitter buffer* pode descartar um pacote caso chegue muito atrasado em relação ao tempo previsto de chegada (regerar a onda analógica de voz) (G.114, 1996). Caso utilize um *voice payload* alto, o descarte de um pacote acarreta várias amostras de áudio descartadas, o que deteriora significativamente o sinal de voz (HARDY, 2003). Em testes práticos, uma taxa de perdas para tráfego de voz < 1% é considerada aceitável (JAMES; CHEN; GARRISON, 2004).

2.4 Problemas de Firewall x SIP

Conforme descrito na seção 2, tanto o protocolo SIP quanto SDP utiliza endereçamentos IP e porta nos campos de seus cabeçalhos. Esses campos não são suportados em implementações comuns de *Firewall*.

A maioria das implementações de *Firewall* são projetadas para operar até a camada de transporte do modelo TCP/IP. Seu objetivo é filtrar tráfego que entra ou sai entre duas ou mais redes por questões de segurança. A base de sua operação é atuar através do par endereço IP e porta, tanto de origem quanto destino. O *Firewall* possui dificuldades em liberar o tráfego de voz RTP, pois os UAs de origem e destino escolhem portas aleatórias para a sessão de voz. Como essas portas aleatórias são anunciadas entre os UAs através do protocolo SDP, a implementação do *Firewall* não verifica o conteúdo das mensagens para interpretar o protocolo SDP o que resulta no bloqueio do tráfego de sessão de voz.

Uma solução para esse problema é liberar, além da porta 5060 para tráfego SIP (ROSENBERG, 2002), uma faixa de portas UDP comum aos UAs para tráfego RTP. Essa faixa possibilita definir no *Firewall* uma regra para permitir apenas a saída de mensagens UDP da rede interna para a rede externa. Como a maioria das implementações de *Firewall* é *stateful* (consegue liberar as respostas relacionadas a uma requisição previamente permitida), o tráfego RTP da rede externa será liberado pelo *Firewall* apenas quando o tráfego RTP interno passar, pois está relacionado ao mesmo.

Essa solução pode acarretar em alguns poucos pacotes perdidos do tráfego externo no início da sessão de áudio, o que não se mostra um problema. Em vários testes práticos, verificou-se a perda entre 0 a 15 mensagens RTP iniciais, não havendo uma percepção de queda de qualidade pelo usuário. No entanto, essa solução pode ocasionar problemas relacionados à segurança de rede e não há garantias que um UA externo utilize a mesma faixa de portas UDP. Caso o

Firewall for *stateless*, então é necessário liberar explicitamente essa mesma faixa de portas da rede externa para a rede interna, o que compromete ainda mais a segurança de rede.

Se um *Firewall* for projetado para operar até o nível de aplicação com suporte ao protocolo SIP e SDP, o tráfego RTP pode ser tratado corretamente. Nesse caso, o *Firewall* é capaz de identificar quais são as portas aleatórias dinâmicas para RTP que estão sendo definidas e assim permitir a sessão multimídia. Como exemplos desse tipo de implementação temos o *IPTables* com o módulo *NetFilter conntrack_sip* (HENTSCHEL, 2005) e o suporte das *Access Control Lists* (ACL) em alguns IOS Cisco (CISCO SYSTEMS, 2005).

2.5 Problemas de NAT x SIP

Da mesma forma que o *Firewall*, as implementações comuns de NAT também não possuem suporte a mensagens SIP e SDP (BOULTON et al., 2011), o que inviabiliza a adoção de uma infraestrutura VoIP na existência de NAT.

O NAT é uma solução que surgiu na década de 90 para resolver o problema da falta de endereçamento IPv4. Mesmo o endereçamento IPv4 ter atingido o seu limite, ainda é necessário lidar com os problemas do NAT devido ao período de transição para o IPv6. Para tanto, algumas propostas estão surgindo para ainda considerar o NAT com IPv6, como o *NAT6* (JENNINGS, 2008).

A solução do NAT consiste na utilização de uma pequena faixa de endereços inválidos para uma rede privada, que são mapeados no equipamento NAT (geralmente no roteador com *Firewall*) para um ou mais endereços válidos da rede pública. Para maiores detalhes ver em (EGEVANG; FRANCIS, 1994). No entanto, a maioria das implementações de NAT atua apenas no nível de rede IP e transporte TCP/UDP, desconsiderando o conteúdo dos pacotes. Portanto, os endereços IPs e portas existentes nas mensagens SIP e SDP não são considerados o que impede a sinalização SIP e consequentemente o tráfego RTP.

Se uma implementação de NAT operar até o nível de aplicação com suporte ao protocolo SIP e SDP, tanto as mensagens SIP e SDP quanto o tráfego RTP podem ser tratados corretamente. Um NAT, que geralmente atua em conjunto com o *Firewall*, consegue modificar os campos necessários dos cabeçalhos SIP e SDP e assim instruir o *Firewall* a liberar o tráfego RTP da sessão de voz. Como exemplos desse tipo de implementação temos o *IPTables* com o módulo *NetFilter nat_sip* (HENTSCHEL, 2005) e alguns IOS Cisco (CISCO SYSTEMS, 2005).

Como essas implementações em nível de aplicação não são maioria, deve-se adotar uma abordagem para contornar o problema do NAT (BOULTON et al., 2011). Várias soluções conhecidas

surgiram como o *Session Traversal Utilities for NAT* (STUN) (ROSENBERG, 2008), *Traversal Using Relays around NAT* (TURN) (MAHY et al., 2010), *Interactive Connectivity Establishment* (ICE) (ROSENBERG, 2010) e *Universal Plug and Play* (UPnP) (STERMAN, 2004).

A abordagem STUN necessita de um servidor STUN com endereço IP público e de UAs que suportem o cliente STUN. Um UA utiliza o servidor STUN para obter informações sobre o NAT. Com essas informações o UA pode gerar as mensagens SIP contendo endereço IP e porta públicos. No entanto o STUN não opera corretamente em implementações de NAT simétrico (ROSENBERG, 2008) (BOULTON et al., 2011).

A abordagem TURN é uma extensão ao STUN e define um servidor intermediário TURN público que é usado pelo UA para enviar as mensagens SIP e RTP. Como o servidor TURN atua como intermediador de tráfego RTP, ambos os UAs (origem e destino) conseguem estabelecer uma sessão de voz com o servidor TURN independente da configuração NAT (BOULTON et al., 2011).

A abordagem ICE descreve um mecanismo para qualquer sessão multimídia, utilizando STUN e TURN. Além disso, suporta negociação da qualidade da sessão multimídia entre UAs origem e destino (LIN; TSENG, 2010).

A abordagem UPnP utiliza um protocolo UPnP para o UA consultar o NAT (com suporte a UPnP). Essa consulta identifica qual o IP público e porta será utilizado no mapeamento NAT, caso o UA opte por receber dados em uma determinada porta. O NAT responde com o IP público e porta da rede externa.

As abordagens STUN, TURN, ICE e UPnP obrigatoriamente necessitam de suporte do UA, o que nem sempre existe nos equipamentos VoIP e foge da solução procurada para uma infraestrutura VoIP transparente. No entanto, duas abordagens foram identificadas por conseguir resolver o problema do *Firewall*/NAT que seja independente do suporte dos UAs: *Back-to-Back User Agent* (B2BUA) e TURN simplificado.

Um B2BUA é previsto na especificação SIP (ROSENBERG, 2002) e consiste de uma entidade SIP que atua como um UA intermediário entre todas as mensagens SIP entre UAs origem e destino. Diferentemente de um *ProxySIP*, que realiza roteamento SIP, o B2BUA mantém um diálogo separado para cada UA (origem e destino) (MARJOU; ELZ; MUSGRAVE, 2008). Com esse recurso, o B2BUA consegue inserir um gerenciamento preciso de chamadas podendo encerrar, contabilizar, ocultar a identificação da origem e realizar transferência de uma chamada (RADVISION, 2007). Uma implementação de código aberto B2BUA é o *Sippy* B2BUA (B2BUA, 2011). No entanto, um B2BUA quebra a comunicação VoIP tanto no UA origem quanto no UA destino, pois ele atua como UA destino para o UA origem e como o UA origem para o UA destino. Essa quebra no diálogo impede a identificação dos UAs origem e destino,

tornando o ambiente SIP inflexível. Além disso, necessita controlar/gerenciar todos os diálogos entre os UAs.

Uma abordagem TURN diferenciada em relação à abordagem TURN original (MAHY et al., 2010) é utilizada em (GONÇALVES, 2010). Essa abordagem foi denominada aqui como abordagem TURN simplificada (TURN-S), pois não troca mensagens de sinalização TURN com um UA para que este consiga modificar os cabeçalhos SIP e SDP com os IP e portas externos do NAT. Por não utilizar mensagens TURN, os UAs não necessitam do suporte TURN.

Quem realiza as modificações SIP e SDP é o equipamento com a abordagem TURN-S. Essa abordagem consiste de um *ProxySIP* com recursos extras para modificar as mensagens SIP e SDP. Além disso, possui suporte para configurar um *proxy RTP* de forma a ser um intermediário da sessão de áudio entre os UAs.

O *proxy RTP* age apenas recebendo uma sessão de áudio de um UA e a repassa para o outro UA da mesma sessão e vice-versa (não existe quebra de diálogo do B2BUA). Como essa abordagem atua como um *ProxySIP*, ela não possui toda a complexidade de um B2BUA, pois não atua como um UA intermediário. A operação do TURN-S é descrita na próxima seção. Para simplificar sua representação no texto, a abordagem TURN-S com um *proxy RTP* localizado em um mesmo equipamento é denominado aqui de TURN-S.

3. ABORDAGEM TURN-S

A abordagem TURN-S permite que os UAs o utilizem normalmente como um *ProxySIP* de seu domínio. Além do comportamento padrão de *ProxySIP*, o TURN-S realiza modificações nos cabeçalhos SIP e SDP das mensagens afim de corrigir os endereços IP e porta não tratados pelo NAT.

Quando um UA se registrar em seu *ProxySIP*, ele identifica que o UA está atrás de NAT e mantém o seu mapeamento ativo no *Firewall*/NAT através de mecanismos de *keep-alive* (JENNINGS; MAHY; AUDET, 2009). Nas mensagens SIP, os campos corrigidos são o *VIA*, com a adição de parâmetros *received* e *rport* (ROSENBERG; SCHULZRINNE, 2003), e o *Contact*, alterando o endereço IP e porta desse campo para conter o endereço IP e porta válidos obtidos do cabeçalho IP/UDP já modificados pelo NAT. Já no cabeçalho SDP, os campos alterados são o *c* (*Connection Data*) e *m* (*Media Descriptions*), que revelam respectivamente qual o endereço IP e porta a serem usados na sessão de voz (HANDLEY; JACOBSON; PERKINS, 2006). Esses campos do SDP são alterados para que os UAs origem e destino obrigatoriamente utilizem o endereço IP e porta do *proxy RTP* como intermediário na sessão de voz.

Como alguns campos dos protocolos SIP e SDP necessitam de modificações, algumas estratégias de criptografia SIP e SDP *end-to-end* (entre UA origem e destino) definidas em (ROSENBERG, 2002) (SALSANO; VELTRI; PAPALIO, 2002) ficam afetadas uma vez que impedem a alteração desses campos. No entanto, as estratégias de criptografia *hop-*

by-hop (entre duas entidades SIPs sucessivas no caminho das mensagens SIP entre UA origem e destino) não são afetadas, pois o TURN-S atua como *ProxySIP* e este é uma entidade SIP.

Com as modificações nas mensagens SIP e SDP aplicadas, o TURN-S configura e aciona dinamicamente o *proxy RTP* para receber e enviar tráfego da sessão de voz (RTP) de acordo com as modificações realizadas. Essa sessão de voz é mantida até que seja identificada a sua finalização na troca de mensagens SIP entre os UAs (método BYE ou por *timeout* (ROSENBERG, 2002)).

Considere um domínio X que necessite de um *ProxySIP* responsável por esse domínio. Todas os UAs de X devem utilizar o *ProxySIP* para o tráfego de mensagens SIP.

A Figura 1 apresenta como ficaria o fluxo de tráfego SIP (segmentos pontilhados) e RTP (segmentos contínuos) de um UA no domínio X para um UA remoto utilizando um *ProxySIP* comum. Já a Figura 2 mostra esses mesmos fluxos utilizando um TURN-S.

Observa-se que todos os fluxos de tráfego SIP e RTP utilizam o TURN-S, ao contrário do *ProxySIP* comum que é incapaz de lidar com *Firewall*/NAT.

Assim, "UA em X" consegue estabelecer uma sessão de voz com um UA remoto mesmo atrás de *Firewall*/NAT, pois os campos das mensagens SIP/SDP são modificados de forma que o tráfego da sessão de voz (tanto UA origem quanto destino) passem pelo *proxy RTP*. A configuração do *Firewall* fica facilitada, pois necessita apenas permitir tráfego destinado/originado ao TURN-S.

Algumas implementações atuais de *ProxySIP* com código aberto conseguem operar de acordo com a abordagem TURN-S descrita, dentre elas estão o OpenSIPS (http://www.opensips.org) e o Kamailio (http://www.kamailio.org). A abordagem TURN-S é a utilizada no OpenSIPS em (GONÇALVES 2010) para contornar *Firewall*/NAT. Para operarem

Figura 1 – Fluxos de Tráfego SIP e RTP em ambiente com ProxySIP Bridge

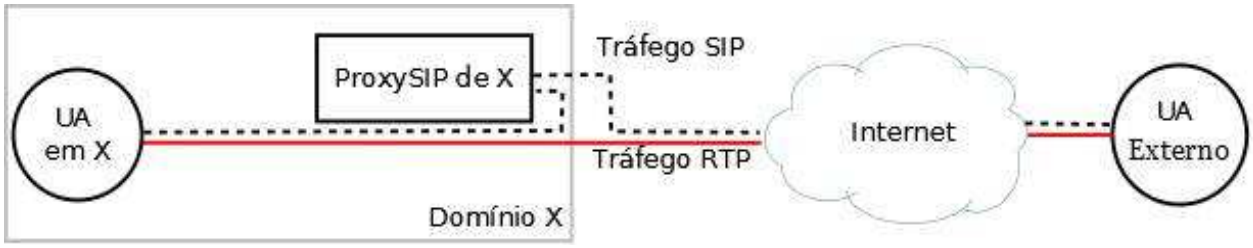
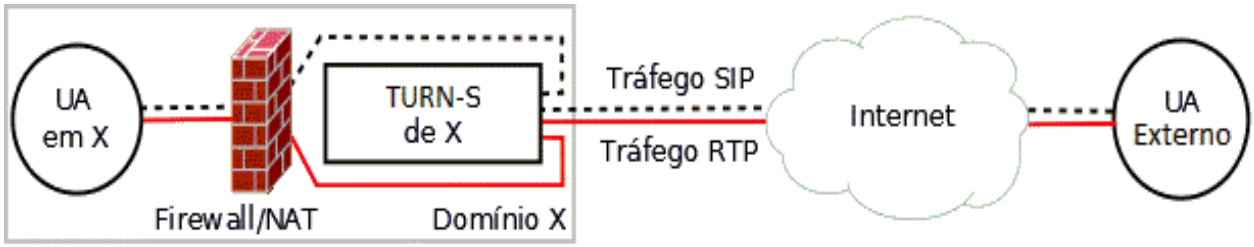


Figura 2 – Fluxos de Tráfego SIP e RTP em ambiente com TURN-S



conforme o TURN-S, tanto o OpenSIPS quanto o Kamailio detêm módulos que adicionam recursos ao *ProxySIP* para identificar a presença de *Firewall*/NAT, realizar modificações nos cabeçalhos SIP e SDP e configurar um *proxy RTP* para tráfego RTP. As implementações de código aberto para *proxy RTP* suportadas tanto pelo OpenSIPS quanto pelo Kamailio são o RTPProxy (RTPPROXY, 2011) e o MediaProxy (MEDIAPROXY, 2011).

O TURN-S permite criar uma infraestrutura VoIP que contorne os problemas de *Firewall*/NAT sem grandes modificações na configuração dos mesmos, e independa do suporte dos UAs.

No entanto, essa abordagem pode ocasionar sobrecargas no equipamento TURN-S ao acionar o *proxy RTP* para todos os tráfegos RTP gerados e/ou destinados ao domínio X (mesmo os UAs origem e destino estando no domínio X deverão usar o *proxy RTP*), pois é a sua configuração padrão (GONÇALVES, 2010) (VOIP INFO, 2009a). Mesmo alguns experimentos revelando o *proxy RTP* com capacidade para suportar em torno de 2000 ligações simultâneas utilizando Codec G.729 em um equipamento P4 2.5-3.0 GHz (VOIP INFO, 2009b), há ainda o fato da interface de rede do TURN-S receber e enviar um mesmo tráfego RTP. Essa carga na interface acarreta desperdício de largura de banda, o que limita o seu uso dependendo da velocidade do enlace. Além disso, existe a concorrência do tráfego de voz com os demais tráfegos de propósito geral (ex: HTTP, FTP, P2P, etc...) para atravessar o equipamento *Firewall*/NAT, o que influencia diretamente no atraso dos pacotes e no *jitter* devido ao tempo de processamento necessário (RAMASWAMY; WENG; WOLF, 2009).

Este trabalho propõe uma abordagem com uma arquitetura e operação modificada do TURN-S para solucionar esses problemas, denominado *ProxySIP Bridge*.

4. ABORDAGEM PROPOSTA: PROXYSIP BRIDGE

A abordagem *ProxySIP Bridge* é um aperfeiçoamento do TURN-S para permitir uma infraestrutura VoIP diferenciada, que consiste no reposicionamento do *ProxySIP Bridge* na infraestrutura de rede e na política de configuração das sessões de voz.

Da mesma forma que a abordagem TURN-S, o *ProxySIP Bridge* é um *ProxySIP* com recursos extras e um *proxy RTP* no mesmo equipamento, porém o *ProxySIP Bridge* necessita ao menos de duas interfaces de rede para estar conectado à rede interna e à rede externa. O tráfego SIP ocorrerá apenas na interface externa, pois esta possui um endereço IP público divulgado no registro SRV no DNS (ROSENBERG, 2002) para os UAs consultarem. As mensagens SIP trocadas entre os UAs de um domínio SIP com o *ProxySIP Bridge*, responsável pelo domínio, são autenticadas através do *HTTP Digest Authentication* (ROSENBERG, 2002). Essa autenticação é aplicada antes do registro de uma UA (*Registrar Server*) e antes

da realização ou aceitação de uma chamada, conforme recomendado em (ROSENBERG, 2002) e (SALSANO; VELTRI; PAPALIO, 2002).

O *ProxySIP Bridge* necessita modificar os mesmos campos dos cabeçalhos SIP e SDP (*VIA*, *Contact*, *c*, *m*) modificados na abordagem TURN-S, no entanto, essa modificação deve obedecer às políticas de configuração da sessão de voz, que são aplicadas conforme o cenário de uma ligação VoIP (seção 4.1 e 4.2). Dependendo do cenário de ligação VoIP, o tráfego da sessão de voz ocorre em ambas as interfaces com o *proxy RTP* operando em *bridge* (*bridge RTP*), por isso o nome *ProxySIP Bridge*. O acionamento do *bridge RTP* é similar ao descrito no TURN-S, porém obedece às políticas da seção 4.1 e 4.2.

O tráfego RTP de voz não ocorre via *Firewall*/NAT, mas sim através do *bridge RTP* que atua como um intermediador de mídia, O *bridge RTP* opera em nível de aplicação para realizar o chaveamento da sessão de voz da rede interna para a rede externa e vice-versa. Ao desviar o tráfego de voz para o *ProxySIP Bridge*, remove-se o tempo de processamento necessário pelo *Firewall*/NAT (RAMASWAMY; WENG; WOLF, 2009) que existiria para o tráfego de voz, o que reduz o atraso dos pacotes (*Mouth-to-Ear Delay* (JIANG; KOGUSHI; SCHULZRINNE, 2003)).

Como o *ProxySIP Bridge* não realiza roteamento entre suas interfaces e o *bridge RTP* é acionado apenas quando existir um determinado fluxo RTP válido a partir de uma sinalização SIP autenticada (*HTTP Digest Authentication*), o risco de segurança para a rede interna tende a ser reduzido. Da mesma forma que o TURN-S, o *ProxySIP Bridge* possui restrições quando aos processos de criptografia *end-to-end* que cifram os campos *Via*, *Contact*, *c* e *m* dos cabeçalhos SIP e SDP. Outros processos de autenticação *hop-by-hop* descritos em (ROSENBERG, 2002) e (SALSANO; VELTRI; PAPALIO, 2002) podem ser aplicados para aumentar o nível de segurança do *ProxySIP Bridge*.

A única implementação de código aberto no momento para um intermediador de mídia com suporte ao *bridge RTP* e com interface para o OpenSIPS ou Kamailio é o RTPProxy. Mecanismos de segurança para criptografar o tráfego de voz do RTP, como *Secure RTP* (SRTP), podem ser aplicados entre UA origem e destino mesmo utilizando o RTPProxy como *bridge RTP*, pois o este não realiza modificações no tráfego RTP que possam corromper o protocolo SRTP (RTPPROXY,2011).

As políticas de configuração das sessões de voz efetuadas pela abordagem *ProxySIP Bridge* são descritas na seção 4.1 e 4.2 de acordo com o cenário de ligação VoIP. A aplicação dessas políticas somente é possível devido à flexibilidade fornecida, tanto pelo OpenSIPS quanto pelo Kamailio, na capacidade de manipular seus scripts de roteamento SIP.

4.1 Chamada entre UAs Internos

Se em um domínio, denominado X, ocorrer uma chamada entre UAs internos desse domínio (quando UAs origem e destino são registrados no domínio SIP X), o *ProxySIP Bridge* não realiza modificações no cabeçalho SDP para permitir uma comunicação direta entre os UAs sem a ação do *bridge RTP*. O fluxo de tráfego SIP e RTP entre UAs interno é apresentado na Figura 3. A troca de mensagens SIP é roteada pelo *ProxySIP Bridge* e o tráfego RTP ocorre diretamente entre os UAs internos. Ao contrário da abordagem TURN-S, essa política reduz drasticamente a carga no *ProxySIP Bridge*, pois a grande maioria das ligações, se considerar um campus universitário, ocorre entre telefones internos.

4.2 Chamada entre UAs Interno/Externo

Se uma chamada envolver um UA externo (um UA, origem ou destino, não registrado no domínio SIP X), então o *ProxySIP Bridge* modifica o cabeçalho SDP para forçar o uso do *bridge RTP* na sessão de voz entre os UAs. A Figura 4 apresenta o fluxo de tráfego entre UA interno e externo ou vice-versa. A troca de mensagens SIP é roteada pelo *ProxySIP Bridge* e o tráfego RTP é intermediado pelo *bridge RTP*, que é inicializado de acordo com a sessão de áudio configurada na troca de mensagens SIP. Essa política retira o tráfego de voz do *Firewall*/NAT, o que evita concorrência com o tráfego de propósito geral além de remover um *hop* do caminho seguido pelo tráfego RTP entre UA origem e destino (reduz o atraso por pacote).

Com o *ProxySIP Bridge*, torna-se possível criar uma infraestrutura VoIP diferenciada, pois consegue-

Figura 3 – Fluxo de tráfego entre UAs internos

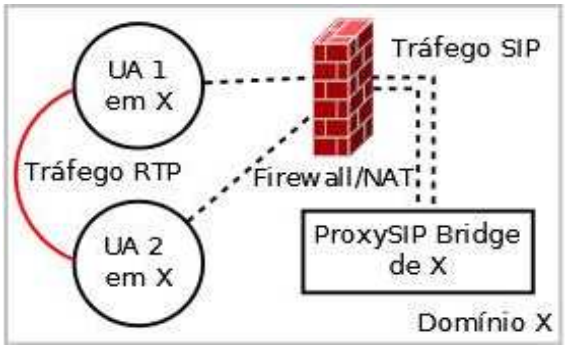
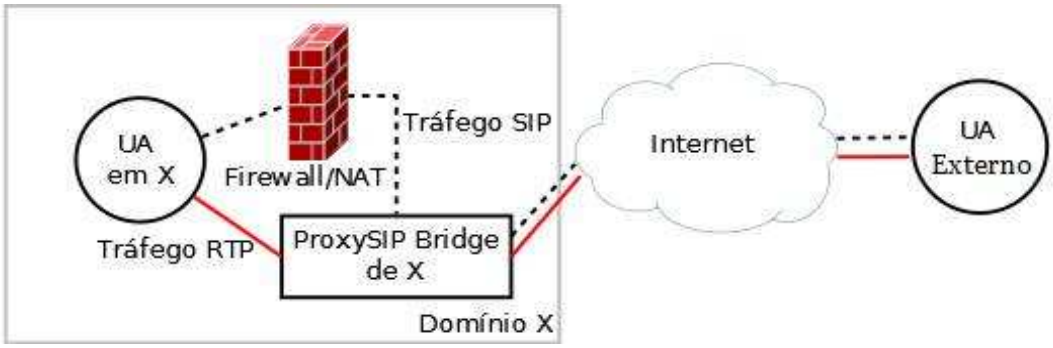


Figura 4 – Fluxo de tráfego entre UA interno e UA externo



se desviar o tráfego de voz dos demais tráfegos do *Firewall*/NAT e com isso, reduzir o atraso por pacote. Além disso, reduz a sobrecarga no *ProxySIP Bridge* ao evitar a utilização do *bridge RTP* (chamadas entre UAs internos), e ameniza a sobrecarga que existiria em uma interface de rede apenas (padrão usado pela abordagem TURN-S) ao adotar duas interfaces de rede (rede interna e externa) com *bridge RTP*.

5. PROXYSIP BRIDGE NA UTFPR

Para verificar a abordagem *ProxySIP Bridge* em um ambiente real, foi realizado um planejamento de uma infraestrutura VoIP para a UTFPR. Nesse planejamento, primeiramente foi identificado as características da infraestrutura de rede da UTFPR e depois a elaboração da infraestrutura VoIP.

5.1 Infraestrutura de rede na UTFPR

A UTFPR está distribuída em todo o estado do Paraná. Todos os campi estão conectados em uma infraestrutura contratada com uma empresa terceirizada. Todos os campi possuem acesso à Rede Nacional de Pesquisa (RNP) através do campus Curitiba. A Figura 5 apresenta a topologia e os enlaces *full-duplex* em Megabits/s que interconectam os campi da UTFPR. Esses enlaces dedicados estão contratados para fornecer apenas serviço de QoS de melhor esforço, portanto sem garantias de serviços necessárias para VoIP.

Cada campus da UTFPR possui um pessoal responsável pela administração de rede com autonomia para adotar, cada um, a sua abordagem de administração.

Realizou-se uma entrevista por e-mail e telefone com cada equipe de administração de rede dos campi para obter informações sobre a infraestrutura de rede. Todos os campi utilizam endereçamento IPv4 e recurso de NAT, uma vez que o uso do IPv6 ainda não está planejado para a UTFPR. A maioria dos campi adotam um *Firewall* com implementação padrão (suporte ao nível IP e transporte UDP/TCP) e do tipo *stateful*. No campus de Curitiba também existe um *Firewall* que filtra o tráfego da RNP destinado aos campi. Todos os campi utilizam o recurso de NAT com implementação padrão (suporte ao nível IP e transporte UDP/TCP) em suas redes. Cada campi utiliza uma faixa de endereçamento IP inválido, sem existir um padrão entre os campi.

Todos os campi adotam políticas de QoS para garantir o serviço do sistema acadêmico e de videoconferência. Outras políticas são aplicadas por cada campi, mas sem um padrão comum.

5.2 Infraestrutura com ProxySIP Bridge

Dada a heterogeneidade da infraestrutura de rede IP e a independência de administração de rede que cada campus da UTFPR utiliza, buscou-se elaborar

uma infraestrutura VoIP que pudesse ser implantada nesses campi com o *ProxySIP Bridge*.

Nesse primeiro momento, o local para testes escolhido foi o campus Apucarana, pois é o local do autor desse artigo e onde houve permissão para elaborar essa infraestrutura. Esse campus utiliza várias VLANs para segmentação lógica da rede. O enlace externo contratado é de 4Mbps *full-duplex* e não fornece quesitos de QoS para voz, conforme seção 5.1.

Como o atraso das mensagens de voz deve ficar em torno de 250 ms para ser aceitável (seção 2.3), um teste simples foi feito para verificar qual seria esse atraso na UTFPR. A ferramenta escolhida foi o *Ping*, pois o autor não possui acesso às redes dos demais campi para utilizar outras ferramentas. O intervalo de geração entre pacotes foi definido em 20 ms e o tamanho total das mensagens foi estipulado em 238 bytes (emular um tráfego de voz Codec G.711 considerando todos os cabeçalhos). O teste foi realizado em horário de pico de tráfego a partir do *gateway* do campus Apucarana para cada *gateway* dos demais campi. Cada teste para cada campus da UTFPR utilizou 10 *pings* simultâneos, com duração de 1 minuto (emular 10 ligações VoIP G.711. Como o *Ping* apresenta o *Round Trip Time*, que contabiliza o tempo de ida e volta de uma mensagem, os resultados foram divididos por 2 para estimar qual seria o atraso de ida ou de volta. No pior caso, o atraso máximo identificado foi de 45.3 ms para alguns pacotes apenas. Em média, o atraso encontrado foi de 12.7 ms, com desvio padrão de 7 ms. Esses dados revelam que uma infraestrutura VoIP pode ser aplicável, mesmo tendo um contrato de enlace dedicado sem garantias de QoS necessárias para VoIP.

Foi criada uma VLAN dedicada para interligar os equipamentos internos destinados apenas para tráfego de voz (VLAN VoIP). Essa VLAN permite um isolamento das redes internas do campus para impedir tráfego desnecessário gerado por *Desktops*. Além disso, a configuração da VLAN VoIP permite acesso apenas aos equipamentos VoIP de um determinado fabricante com base no *Organizationally Unique Identifier* (OUI) do endereço *Media Access Control* (MAC) (IEEE, 2011). Nessa avaliação, foi homologado apenas OUI dos equipamentos VoIP da *LinkSys*, o que aumenta o nível de segurança ao impedir o uso indevido de computadores *Desktop* nessa VLAN uma vez que pertencem a outras OUI.

Para implementar a abordagem *ProxySIP Bridge*, foi alocado um equipamento PC com processador 2.13GHz, 1GByte de memória e duas interfaces de rede Gigabit Ethernet. Foram instalados o sistema operacional Debian 6 e os softwares OpenSIPS e RTPPRoxy. O OpenSIPS e o RTPProxy foram adaptados para se comportar conforme a descrição do *ProxySIP Bridge*, sendo o responsável pelo domínio SIP de Apucarana. O recurso de roteamento entre as interfaces de rede foi desabilitado. Utiliza-se a interface de rede externa com um IP público delegado ao campus Apucarana para que o *ProxySIP Bridge* atue como *ProxySIP*. A interface de rede interna

está conectada à VLAN VoIP. Foi configurado um *Firewall* no equipamento *ProxySIP Bridge* para permitir apenas tráfego UDP 5060 (mensagens SIP) e tráfego UDP em uma grande faixa de portas (para tráfego RTP) na interface externa. Na interface interna o *Firewall* permite somente a mesma faixa grande de portas UDP. Como o equipamento não faz roteamento entre as interfaces, essas portas são apenas utilizadas quando o *proxy RTP* estiver acionado. O *ProxySIP Bridge* utiliza autenticação de *Proxy* (ROSENBERG, 2002) tanto para o registro quanto para estabelecimento de chamadas oriundas dos UAs internos pertencentes ao domínio de Apucarana. Essa autenticação faz uso de um servidor LDAP do campus. Utilizou-se quatro equipamentos *LinkSys PAP2*, doados da Receita Federal, como UAs internos. Todos os UAs internos foram configurados para se registrarem no domínio SIP de Apucarana *(ProxySIP Bridge*). A Figura 6 ilustra essa infraestrutura VoIP diferenciada.

Todas as mensagens SIP dos UAs internos atravessam o *Firewall*/NAT para acessar o *ProxySIP Bridge*. Essas mensagens são encaminhadas segundo as configurações de roteamento padrão das VLANs do campus, necessitando apenas de liberação na regra do *Firewall*/NAT para mensagens UDP na porta 5060 (SIP) destinado ao IP público do *ProxySIP Bridge*.

De acordo com o comportamento previsto pelo *ProxySIP Bridge*, o tráfego RTP de um UA interno ocorrerá pela *bridge* RTP e sairá pela interface externa apenas quando o destino for um UA externo (de outro domínio) ou vice-versa. Se o destino for uma UA interna, o tráfego RTP ocorrerá dentro da VLAN VoIP, sem utilizar a *bridge* RTP. O *Firewall*/NAT não roteia tráfego RTP.

Para garantir alguns quesitos de QoS para o tráfego de voz, foi adicionado uma restrição ao uso do link externo pelo *Firewall*/NAT. Essa restrição limita a saturação do enlace externo a no máximo 3 Mbps. Esse limite reserva 1 Mbps para o *ProxySIP Bridge*. O objetivo é garantir o fluxo de tráfego de voz entre os UAs internos/externos. A quantidade de ligações possíveis em 1 Mbps depende de quais Codecs são utilizados pelos UAs e do tráfego adicional que possa existir (mensagens SIP, tráfego RTCP, *Address Resolution Protocol* – ARP, *Spanning Tree* e *Protocolos de Roteamento*).

Dentre os Codecs disponíveis para áudio (G.SERIES, 2011) (CISCO SYSTEMS, 2002), foram estabelecidas prioridades para selecioná-los dentre aqueles suportados pelos UAs internos. O Codec com maior prioridade é o G.729a, em seguida o G.726 e por último o G.711. Essa ordem de prioridade tem como base o consumo de Largura de Banda Total usado pelo tráfego RTP, conforme apresentado na Tabela 1.

O tráfego extra ocasionado pelas mensagens SIP ocorre antes, para inicializar a sessão de voz, ou no término da sessão. Portanto, o tráfego RTP não é afetado significativamente pelas mensagens SIP, sendo

desconsiderado. Em relação ao tráfego RTCP, é recomendado que atinja no máximo 5% da largura de banda total necessária para o tráfego RTP (SCHULZRINNE, 2003). O tráfego referente às mensagens ARP é reduzido não afetando significativamente o tráfego RTP, pois existem apenas o *Firewall*/NAT do campus, o roteador da empresa terceirizada e a interface externa do *ProxySIP Bridge* interconectados no mesmo barramento. Tráfegos referentes ao *Spanning Tree* e *Roteamento* não existem.

A Tabela 2 apresenta o número máximo de ligações simultâneas externas por Codec comportadas em 1 Mbps considerando o tráfego extra. Utilizou-se para esse cálculo um *voice payload* de 20ms, pois é o adotado como padrão em vários equipamentos (ver seção 2.3) e por isso foi adotado nos *LinkSys PAP2* usados. A fórmula para o cálculo do número de ligações é: 1000Kbps/(L. Banda Total do Codec + 5% da L. Banda Total do Codec). O pior caso ocorre quando todas as ligações simultâneas utilizarem o Codec G.711, pois possui o maior consumo de largura de banda total. Outros Codecs não listados na Tabela 2 não são adotados pelos UAs internos.

No caso do campus Apucarana, o número de ligações externas simultâneas com Codec G.729a para os demais campi é de no máximo 24, independente do serviço de telefonia convencional. Se todos os campi da UTFPR utilizarem essa infraestrutura VoIP diferenciada, então cada campi poderá realizar no máximo 24 ligações simultâneas entre os campi utilizando apenas 1Mbps.

O número máximo de ligações internas depende da largura de banda dos enlaces e VLAN internos, a qual é de 100 Mbps. Essa largura de banda permite, em teoria, acomodar aproximadamente 2400 ligações simultâneas se os UAs utilizarem Codec G.729a. No entanto, testes exaustivos devem ser feitos para certificar se essa demanda é atendida pelos equipamentos de interconexão.

5.3 Avaliação do ProxySIP Bridge na UTFPR

Com o ambiente instalado e configurado, realizaram-se duas baterias de testes simples para verificar se a abordagem *ProxySIP Bridge* apresenta o comportamento esperado. Utilizou-se o analisador de protocolos *ngrep* (*http://ngrep.sourceforge.net*) para verificar o tráfego nas interfaces interna e externa do *ProxySIP Bridge*.

A primeira bateria de testes realizou uma combinação de chamadas entre os UAs internos envolvendo os usuários do campus. Todas as chamadas realizadas entre os quatro equipamentos *LinkSys PAP2* ocorreram com sucesso e o tráfego de voz ocorreu dentro da VLAN VoIP. Foram realizadas várias conversas simples entre os usuários variando de vários segundos a minutos. Houve nesses testes uma variação dos Codecs utilizados. Os usuários foram instruídos para ficarem atentos à qualidade das conversas. Para

coletar uma nota do usuário, foi apresentada uma classificação de cinco níveis que são semelhantes ao utilizados em MOS (Excelente, Bom, Razoável, Ruim, Péssimo). A opinião coletada dos usuários foi "Excelente", não percebendo diferença expressiva entre os Codecs e nem em relação ao telefone convencional.

A segunda bateria de testes ocorreu entre UAs internos e UAs externos e vice-versa. Os quatro UAs externos utilizaram outros quatro *LinkSys PAP2* fora do domínio Apucarana, em outros campi da UTFPR. Esses UAs externos utilizaram contas no serviço SIP gratuito fornecido pela empresa IpTel (*http://www.iptel.org/service*). Teve também uma participação de um UA externo pertencente à UFSC. Em todos os testes, o *bridge* RTP foi acionado para trocar tráfego de voz entre UAs internos e UAs externos, conforme planejado na abordagem *ProxySIP Bridge*. Em relação à opinião dos usuários, foi seguido o mesmo padrão adotado na primeira bateria de testes. A opinião dos usuários foi em geral "Excelente" e alguns "Bom" independente dos Codecs utilizados. Ao repetir a ligação em seguida, essa variação na opinião não foi apresentada novamente e manteve-se em "Excelente". Essa variação ocorreu devido à falta de previsibilidade da infraestrutura externa do campus (o enlace de 4Mbps contratado não fornece quesitos de QoS para voz), pois apenas em algumas ligações e em momentos aleatórios das ligações os usuários reportaram um pequeno retardo na voz, mas logo se estabilizando. Esse retardo foi verificado pelos dados do analisador *ngrep* através da variação do tempo de chegada dos pacotes.

Esses resultados realçam a necessidade de alteração do contrato do enlace de dados externo para prover QoS para voz, e assim ter uma qualidade de voz compatível com a telefonia convencional.

6. TRABALHOS FUTUROS

Um próximo passo é adotar essa infraestrutura VoIP diferenciada com *ProxySIP Bridge* nos demais campi da UTFPR para realização de mais testes. Inserir nessa infraestrutura um *MediaGateway* com o software de código aberto Asterisk (*http://www.asterisk.org*) para prover acesso à telefonia convencional também é um trabalho futuro. Testes iniciais com o Asterisk nesse ambiente já apresentaram resultados promissores. O uso de uma infraestrutura IPv6 também deve ser investigada para que o *ProxySIP Bridge* tenha esse suporte. Novas baterias de testes com software de testes exaustivos SIP devem ser realizadas para verificar a segurança da abordagem. Outro trabalho é adaptar essa infraestrutura VoIP para o projeto VoIP4All (*http://voip4all.rnp.br*) da RNP.

CONCLUSÃO

Realizou-se um estudo da tecnologia VoIP para identificar os seus pontos principais que afetam uma infraestrutura VoIP. Nesse estudo, foram identificados

vários problemas e suas respectivas soluções para *Firewall*/NAT. Verificou-se que a abordagem TURN-S consegue fornecer uma infraestrutura VoIP com poucas alterações no *Firewall*/NAT e independente do suporte dos UAs. Este artigo apresenta a abordagem *ProxySIP Bridge*, que é um aperfeiçoamento da abordagem TURN-S, para prover uma configuração de infraestrutura VoIP diferenciada. O *ProxySIP Bridge* consegue nessa infraestrutura desviar o tráfego de voz do *Firewall*/NAT, evitar sobrecarga na interface de rede do *ProxySIP Bridge*, e permitir o tráfego direto de voz entre UAs quando possível. Essa abordagem foi implementada e testada com sucesso em um campus da UTFPR, revelando-se uma abordagem promissora como alternativa à abordagem TURN-S.

REFERÊNCIAS

B2BUA. **Sippy B2BUA**. 2011. Disponível em: <http://www.b2bua.org>. Acesso em: 25 jun. 2011.

BOULTON, C., et al. NAT Traversal Practices for Client-Server SIP. **IETF 6314**, 2011.

CISCO SYSTEMS. **Voice internetworking: VoIP quality of service**. Cisco Press, 2002.

CISCO SYSTEMS. **Cisco IOS firewall design guide**. Cisco Press, 2005.

CISCO. **Understanding delay in packet voice networks**. 2006a. Disponível em: <http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml>. Acesso em: 25 jun. 2011.

CISCO. **Voice over IP - per call bandwidth consumption**. 2006b. Disponível em: <http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml>. Acesso em: 25 jun. 2011.

COLLINS, D. **Carrier grade voice over IP**. 2. ed. McGraw-Hill, 2002.

EGEVANG, K.; FRANCIS, P. The IP Network Address Translator (NAT). **IETF RFC163**, 1994.

G.114. **One-way Transmission Time**. International Telecommunications Union, 1996.

GONÇALVES, F., **Building telephony systems with OpenSIPS 1.6**. Packt Publishing, 2010

G.SERIES. **G Series: Transmission systems and media, digital systems and networks**, 2011. Disponível em <http:// http://www.itu.int/net/itu-t/sigdb/speaudio/Gseries.htm>. Acesso em: 25 jun. 2011.

H.323. **Packet-based multimedia communications systems**. International Telecommunications Union, 1998.

HANDLEY, M.; JACOBSON, V.; PERKINS, C. SDP: Session Description Protocol. **IETF RFC 4566**, 2006.

HARDY, W. **VoIP service quality measuring and evaluating packet-switched voice**. Mcgraw-Hill, 2003.

HENTSCHEL, C. **SIP connection tracking and NAT for Netfilter**. 2005. Disponível em <http://www.iptel.org/sipalg/>. Acesso em: 25 jun. 2011.

IEEE. **Organizationally unique identifier (OUI). 2011. Disponível em < http://standards.ieee.org/develop/regauth/oui/index.html>. Acesso em: 25 jun. 2011.**

JAMES, J. H.; CHEN, B.; GARRISON, L. ImpIementing VoIP: a voice transmission performance progress report. **IEEE Communications Magazine**. 2004.

JENNINGS, C. NAT for IPv6-only hosts. **IETF draft-jennings-behave-nat6-01**, 2008.

JENNINGS, C.; MAHY, R.; AUDET, F. Managing Client-Initiated Connections in the Session Initiation Protocol (SIP). **IETF RFC 5626**, 2009.

JIANG, W.; KOGUSHI, K.; SCHULZRINNE, H. QoS Evaluation of VoIP End-Points. **IEEE International Conference on Telecommunications**, 2003.

LIN, Y., TSENG, C. et al. How NAT-Compatible Are VoIP Applications?. **IEEE Communications Magazine**, 2010.

MAHY, R., et al. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). **IETF RFC 5766**, 2010.

MARJOU, X.; ELZ, I.; MUSGRAVE, P. Best Current Practices for a Session Initiation Protocol (SIP) Transparent Back-To-Back User-Agent (B2BUA). **IETF draft marjou-sipping-b2bua-01**, 2008.

MEDIAPROXY. **Media relay for RTP/RTCP**. 2011. Disponível em <http:// mediaproxy.ag-projects.com/>. Acesso em 25 jun. 2011.

P.800, **Methods for subjective determination of transmission quality**, International Telecommunications Union, 1996.

RADVISION. **Back-to-Back User Agent (B2BUA) SIP Servers Powering Next Generation Networks**. Radvision, 2007.

RAMASWAMY, R.; WENG, N.; WOLF, T. Analysis of network processing workloads. **Journal of Systems Architecture**, 2009.

ROSENBERG, J., et al. Session Traversal Utilities for NAT (STUN). **IETF RFC 5389**, 2008.

ROSENBERG, J.; SCHULZRINNE, H. An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing. **IETF RFC 3581**, 2003.

ROSENBERG, J. Interactive Connectivity Establishment (ICE). **IETF RFC 5245**, 2010.

ROSENBERG, J., et al. SIP: Session Initiation Protocol (SIP). **IETF RFC 3261**, 2002.

RTPPROXY. **Sippy RTPProxy**. 2011. Disponível em <http://www.rtpproxy.org>. Acesso em 25 jun. 2011.

SALSANO, S.; VELTRI, L.; PAPALIO, D. SIP Security Issues: The SIP Authentication Procedure and its Processing Load. **IEEE Network**, 2002.

SCHULZRINNE, H., et al. RTP: A Transport Protocol for Real-Time Applications. **ETF RFC 3550**. 2003.

STERMAN, B.; SCHWARTZ, D. **NAT Traversal in SIP**, Delta-Three Corp, 2004.

VOIP INFO. **OpenSER and RTPProxy**, 2009. Disponível em <http://www.voip-info.org/wiki/view/OpenSER+And+RTPProxy> . Acesso em 25 jun. 2011.

VOIP INFO. **RTPProxy Performance**, 2009. Disponível em <http://www.voip-info.org/wiki/view/RTPProxy>. Acesso em 25 jun. 2011.

Artigo submetido em 20 de julho de 2011

Artigo aceito em 17 de dezembro de 2012