UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO SOFTWARE LIVRE APLICADO A TELEMÁTICA

SIDERLEI TARCIZO PINHEIRO FILHO

COMUNICAÇÃO VOIP UTILIZANDO REDES WIRELESS

MONOGRAFIA

CURITIBA
2012

SIDERLEI TARCIZO PINHEIRO FILHO

COMUNICAÇÃO VOIP UTILIZANDO REDES WIRELESS

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Software Livre Aplicado a Telemática, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná. Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2012

RESUMO

FILHO, Siderlei Tarcizo Pinheiro. **Comunicação VoIP em Redes Wireless**. 2012. 54 p. Monografia (Especialização em Software Livre Aplicado a Telemática) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Este trabalho tem por objetivo realizar testes de desempenho de uma rede VoIP (*Voice over Internet Protocol* – Voz sobre Protocolo Internet) sobre uma rede sem fio, analisando parâmetros como: *Jitter*, latência, perda de pacotes, entre outros, por meio da utilização de softwares livres como o próprio PABX, onde foi utilizado o famoso *Asterisk*, *Iperf* para simulação de tráfego concorrente na rede, *wireshark* para análise dos pacotes e por fim, um software não livre, porém gratuito, o *softphone X-lite* para realização das chamadas testes. Estes serão realizados em um ambiente *indoor* com foco na coleta e comparação dos dados adquiridos durante os experimentos interpretados como parâmetros da qualidade de serviço VoIP.

Palavras-Chaves: VoIP. Asterisk. *Wireless*, QoS. Simulação.

ABSTRACT

FILHO, Siderlei Tarcizo Pinheiro. **VoIP Comunications in Wireless Networks**. 2012. 54 p. Monografia (Especialização em Software Livre Aplicado a Telemática) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

This work aims at testing the performance of a network VoIP (Voice over Internet Protocol) over a wireless network, analyzing parameters such as jitter, latency, packet loss, among others, through the use of free software as its PABX, where we used the famous Asterisk, Iperf for traffic competitor simulation in network, wireshark for analysis packages and finally a proprietary software, but free softphone X-lite calls for completion of tests. These will be held in an indoor environment with a focus on the collection and comparison of data acquired during the experiments interpreted as parameters of quality of VoIP service.

Keywords: VoIP. Asterisk. Wireless, QoS. Simulation

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Atualmente, devido ao grande avanço tecnológico que vivenciamos, é notória a constante integração de serviços sobre redes de comunicação. Nesse contexto, tem-se destacado a tecnologia VoIP (*Voice over Internet Protocol* – Voz sobre Protocolo Internet), pois apresenta uma alternativa de baixo custo se comparados aos serviços ofertados nas redes de telefonia atuais. Por esse motivo, o VoIP esta provocando uma reformulação na infraestrutura das operadoras de telecomunicações. Essa atualização vem para beneficio do usuário final, abrindo horizontes para serviços inovadores por valores mais baixos, assim como as operadoras, que podem reduzir seus custos e agregar valor aos seus serviços sem precisar expandir drasticamente sua infraestrutura.

Assim como a telefonia IP, outra tecnologia que vem se destacando no cenário atual, ganhando cada vez mais espaço, são as redes sem fio ou, do inglês, *wireless networks*. Capazes de expandir as redes cabeadas, proporcionando maior flexibilidade e escalabilidade. Em uma comunicação utilizando o VoIP, deve-se levar em consideração parâmetros que definem a percepção da qualidade da chamada: codec utilizado, *Jitter* ou variação do atraso, atraso fim-a-fim e perda de pacotes. Esses dados determinam a compreensão da informação transmitida durante a comunicação. Em ambientes *wireless,* que por sua vez são bem mais sensíveis aos fatores citados anteriormente, fica evidente a importância do bom planejamento e comissionamento da rede, visto que qualquer variação brusca nesses quesitos apresentados, interferências externas ou internas na rede podemos ter o serviço de voz sobre IP comprometido.

Este trabalho tem como objetivo, fazer um teste de desempenho de um ambiente VoIP *wireless*, analisando o tráfego das informações no cenário citado e comparando os valores dos parâmetros de qualidade apresentados anteriormente. Para os testes será configurado, em um sistema operacional Linux Debian, um PABX utilizando o software livre Asterisk, que para muitos é considerado uma revolução na área de telefonia IP e PABX baseados em softwares. Para coleta dos dados será instalado em um dos clientes um software, também livre, chamado *wireshark*, o qual ficará “escutando” a interface de rede do *host* em questão. Para testar a qualidade das chamadas, será injetado na rede um tráfego concorrente por

meio da utilização do aplicativo chamado *Iperf.* Por fim, as ligações serão originadas pelo software proprietário, porém gratuito, chamado X-lite.

Mediante esses experimentos será possível verificar até que ponto pode-se caminhar na direção da escalabilidade e flexibilidade, que as redes sem fio proporcionam, sem afetar a qualidade das chamadas.

1.1 PROBLEMA

Problemas em redes *wireless* muitas vezes não passam despercebidos pelos usuários. As redes sem fio são mais sensíveis a fatores intrínsecos e extrínsecos, como por exemplo: *Jitter* ou variação do atraso, atraso fim-a-fim, perda de pacotes, interferências externas, etc. Portanto, o mau planejamento pode comprometer seriamente o desempenho das chamadas de uma rede VoIP em um ambiente *wireless.* A flexibilidade e escalabilidade que as redes sem fio proporcionam, devem ser avaliadas com cuidado em se tratando de serviços VoiP empregados na rede. Problemas são mais impactantes do que nas redes cabeadas convencionais, pois existe concorrência de acesso ao meio por outras aplicações, interferências no ambiente e outros problemas como atenuação de sinal e propagação que variam muito de acordo com o local.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Implementar uma rede VoIP em um ambiente *wireless,* utilizando software livre Asterisk*,* e verificar o desempenho das chamadas analisando parâmetros como: *Jitter* ou variação do atraso, atraso fim-a-fim, perda de pacotes.

1.2.2 Objetivos Específicos

- Implementar e configurar uma rede sem fio;
- Instalar e configurar o PABX Asterisk;

- Instalar o *Softphone* nas maquinas clientes;
- Efetuar chamadas entre os clientes;
- Coletar os pacotes das chamadas com o *software Wireshark*;
- Injetar tráfego concorrente na rede utilizando o software *Iperf*;
- Analisar os dados coletados com *Wireshark* através de gráficos;

1.3 JUSTIFICATIVA

Tendo conhecimento dos possíveis problemas inerentes dos ambientes *wireless*, busca-se evitar problemas futuros nas redes VoIP através da compreensão de fatores que podem prejudicar o desempenho da rede. Com o auxilio dos experimentos em questão será possível visualizar com mais clareza os problemas mencionados anteriormente.

1.4 PROCEDIMENTOS METODOLÓGICOS

Os recursos físicos necessários foram computadores com os requisitos mínimos para o funcionamento dos *softwares* e periféricos requisitados. Não foram necessários mais recursos humanos para execução das atividades, e para auxiliar e proporcionar entendimentos sobre a utilização de *softwares* e demais equipamentos, assim como tecnologias empregas, foi realizada uma pesquisa bibliográfica e, adicionalmente, pesquisa documental utilizando manuais e tutoriais disponíveis na Internet.

2 REFERENCIAL TEÓRICO

2.1 Redes sem fio ou *Wireless Networks*

Redes de comunicação sem fio ou *Wireless Networks* estão sendo cada vez mais empregadas em razão de sua excelente mobilidade, pois em determinados ambientes as redes cabeadas convencionais não são a melhor opção a ser escolhida devido há limitação físicas existentes.

Os dois grandes pilares da tecnologia de redes sem fio são representados pela portabilidade e a praticidade. Garantindo menores custos de operação e implantação, pois proporcionam mais facilidade em sua operação e menos tempo em sua implantação.

Redes sem fio são consideradas extensões de redes cabeadas. Para que isso ocorra de maneira eficaz é necessário que haja padronização. Sendo assim faz-se uma perfeita integração com redes cabeadas convencionais possibilitando conectividade entre as redes sem alterar drasticamente a infraestrutura já implementada (OLIVEIRA, 2012).

2.1.1 Comparação entre Ethernet e *Wireless*

Há semelhanças entre Ethernet e *Wireless* LANs. As duas tecnologias proporcionam troca de frames entre os elementos da rede, são definidas pelo IEEE, através dos padrões 802.3 e 802.11, ambas possuem maneiras de determinar quando um elemento de rede pode ou não transmitir CSMA/CD no caso Ethernet e CSMA/CA para *Wireless*.

O modo como a informação é transmitida define a maior diferença entre as tecnologias. No padrão Ethernet os dados são transmitidos através de sinais elétricos em cabos metálicos ou pulsos luminosos em fibras óticas. Porém, em redes sem fio os dados trafegam através de ondas eletromagnéticas.

Ao optar pelo uso de redes sem fio, deve-se conviver com alguns problemas inerentes a tecnologia. Como por exemplo, o padrão Ethernet pode transmitir dados em *full duplex.* Já em redes sem fio, quando dois ou mais elementos transmitem ao mesmo tempo em um mesmo espaço, utilizando mesma frequência, os sinais sofrerão interferência causando perda de parcial ou total das informações. Portanto,

de preferencia, redes sem fio utilizam modo *half-duplex.* Com o objetivo de garantir o modo de transmissão em *half-duplex*, e evitar o número de colisões na rede, as redes sem fio utilizam o protocolo CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*) (FILIPPETTI, 2008).

2.1.2 Conceitos básicos de redes sem fio

Redes sem fio diferenciam-se em dois tipos: redes em modo infraestrutura e redes em modo *ad-hoc*.

O modo infraestrutura define-se pela comunicação dos elementos da rede por intermédio de um ponto de acesso ou *Access Point*. Dessa maneira todos os elementos da rede se comunicam diretamente como ponto de acesso e esse por sua vez faz o roteamento dos pacotes. Sendo assim toda a comunicação da rede passa pelo ponto de acesso. Portanto todos os dispositivos devem estar em seu alcance. Os pontos de acessos podem ou não estar ligados a outros pontos de acesso. Seja através de cabos ou a própria interface de rede sem fio. Sendo assim, caracterizando-se 2 tipos de serviços BSS (*Basic Service Set*) e ESS (*Extended Service Set*). O modo BSS utiliza apenas um ponto de acesso para formar a rede, já o ESS utiliza dois ou mais pontos de acesso, proporcionando mobilidade ou *roaming* de uma célula para outra. A figura 1 mostra o modo de operação infraestrutura sob o serviço ESS e BSS. Essa configuração permite atingir maiores níveis de segurança através do ponto de acesso centralizado, tornando-se mais simples o estabelecimento de controle da rede.

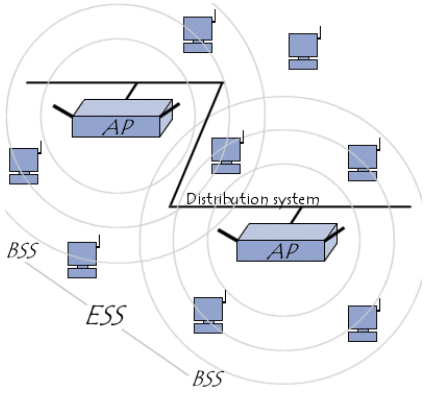

Figura 1: Modo de operação ESS e BSS
Fonte: http://static.commentcamarche.net/

O recurso de mobilidade proporcionado pelo modo ESS permite ao usuário, de maneira transparente, mover-se de uma célula a outra sem a necessidade de obter um novo endereço IP. O dispositivo utilizado pelo usuário, percebe que o sinal de sua célula começa a ficar fraco e, automaticamente, busca por um sinal mais forte de uma célula adjacente.

No modo *ad-hoc* dispositivos *wireless* podem se comunicar sem o intermédio de um ponto de acesso, bastando estar em alcance mutuo (figura 2). Cada dispositivo é capaz de rotear dados na rede (OLIVEIRA, 2012).

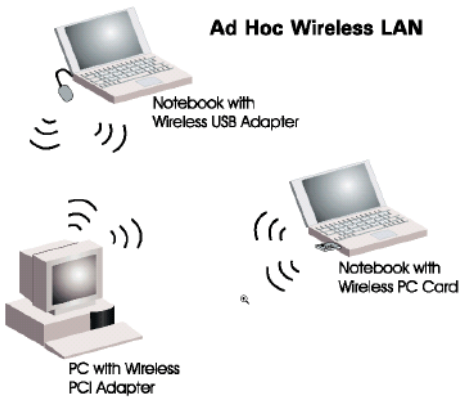

Figura 2: Modo de operação *ad-hoc*.
Fonte: http://img.vivaolinux.com.br/

2.1.3 Transmissão sem-fio

Órgãos reguladores, como por exemplo, a ANATEL, determinam a obtenção de licenças para determinadas frequências em que se deseja transmitir. Porém foi estabelecidas faixas de frequências que não precisam de qualquer licença para sua utilização. As frequências de 900 KHz, e 2,4 GHz e 5 GHz são exemplos de faixas que não necessitam de licenças. O quadro 1 descreve as três faixas citadas anteriormente (FILIPPETTI, 2008).

Faixa de frequência	Nome	Exemplos de dispositivos
900 kHz	Industrial, Scientific, Mechanical (ISM)	Telefone sem fio mais antigos.
2,4 GHz	ISM	Telefones sem fio mais modernos e dispositivos WIFI 802.11, 802.11b, 802.11g.
5 GHz	Unlicensed National Information Infrastructure	Telefones sem fio mais modernos e dispositivos WIFI 802.11a, 802.11n.

Quadro 1: Faixas de frequências liberadas de licença
Fonte: (FILIPPETTI, 2008).

2.1.4 Tipos de Modulação

Dentre as técnicas de modulação existentes, destacam-se três: *Frequency Hopping Spread Spectrum* (FHSS), *Direct Sequence Spread Spectrum* (DSSS) e *Orthogonal Frequency Division Multiplexing* (OFDM).

A FHSS funciona utilizando todas das frequências disponíveis, alternando, saltando de uma para outra. Dessa forma um dispositivo tende a evitar interferências de outro dispositivo utilizando a mesma faixa. Utilizada pelo padrão 801.11 original, no entanto os padrões recentes não utilizam.

Já a DSSS é destinada para uso da faixa de 2.4 GHz. Utiliza um ou vários canais diferentes. Essa faixa varia de 2.402 GHz até 2.483 GHz com uma largura de banda de 82 MHz. Portanto, são obtidos 14 canais parcialmente sobrepostos, porém são utilizados comumente 11. Os canais 1, 6 e 11 não se interseccionam, logo, não interferem um no outro. Isso possibilita a utilização desses canais em uma mesma rede sem fio (FILIPPETTI, 2008).

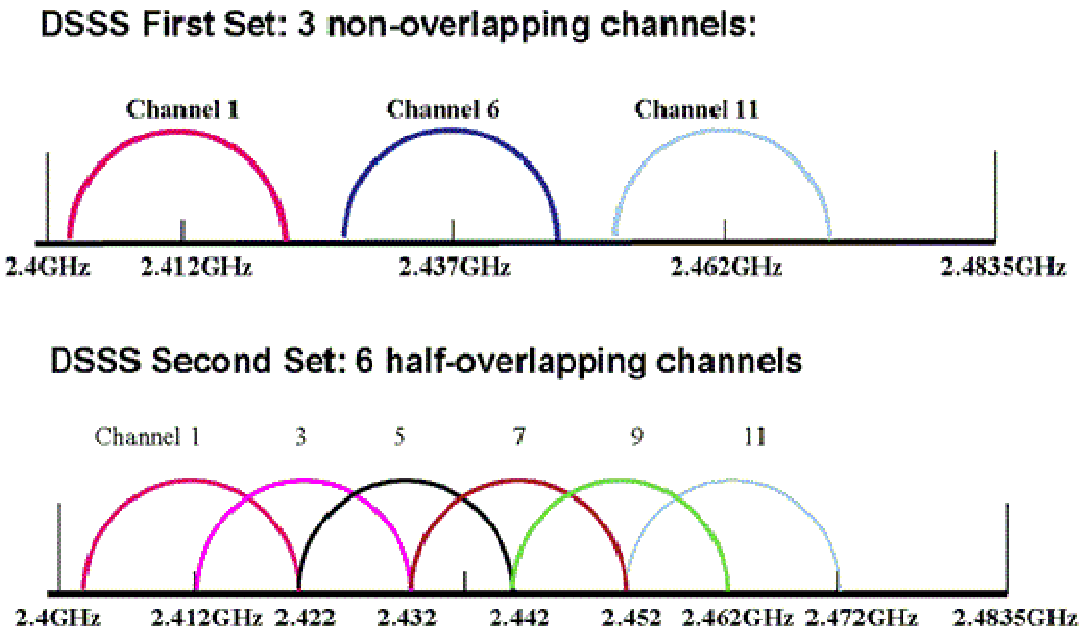

Figura 3: Espectro de frequências de 2.4 GHz.
Fonte: http://transition.fcc.gov/

Por fim a OFDM que de modo análogo ao DSSS, utiliza vários canais não sobrepostos. Conhecida como modulação multiportadora, subdividindo um canal em vários, assim otimizando o uso do mesmo. São transmitidas N portadoras simultaneamente com frequências distintas. O padrão 802.11n utiliza OFDM (FILIPPETTI, 2008).

2.1.5 O padrão 802.11

Em 1997, foi formulado o primeiro padrão IEEE 802.11, atuando na faixa de 2,4 GHz e com taxas de 1 a 2 Mbps. Devido a reclamações constantes, por parte dos usuários, de que o padrão era muito lento, em 1999 começaram a surgir variações do padrão, como a proposta do 802.11a. Atingia a velocidade de 54 Mbps sob a frequência de 5 GHz. Desenvolveu-se o padrão 802.11b, mudando sua técnica de modulação, foi atingido velocidade de 11 Mbps sob a frequência de 2,4 GHz. Surgiu outra variação que utilizava a mesma técnica de modulação do 802.11a e a mesma frequência do 802.11b, alcançando 54 Mbps, denominado 802.11g.

Também em 1999, definiu-se uma norma denominada "*Wireless LAN Medium Access Control* (MAC) *and Physical Layer* (PHY) *Specifications*". O padrão 802.11, assim como todos os padrões da família, determina as camadas PHY (*Physical*) e

MAC (*Medium Access Control*). Padrão que continua em desenvolvimento constante (OLIVEIRA, 2012). A figura 4 representa o padrão 802.11 no modelo OSI.

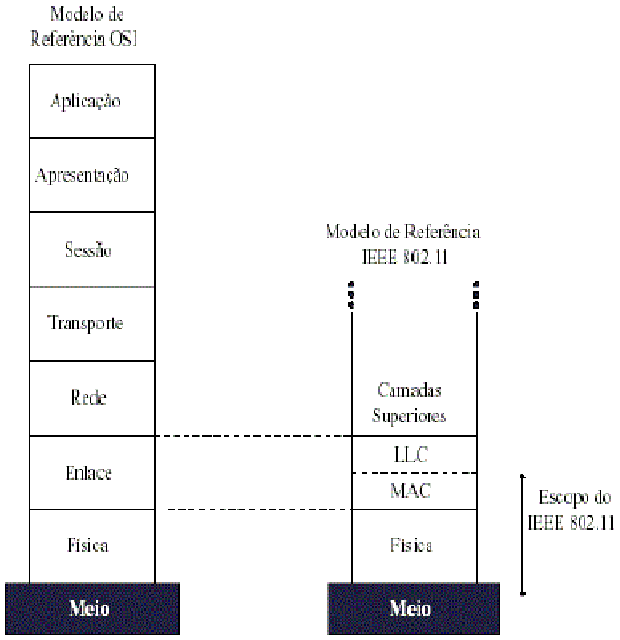

Figura 4: 802.11 no modelo OSI.
Fonte: http://bdtd.bczm.ufrn.br

Em 2009, com o objetivo de atingir velocidades superiores as redes cabeadas de 100 Mbps, surgiu a proposta do padrão 802.11n. Para atingir a velocidade planejada o padrão 802.11n utiliza a tecnologia MIMO (*Multiple-Input, Multiple-OutPut*) juntamente com melhoras em algoritmos de transmissão. Sendo assim, a velocidade teórica passa a ser de 300 Mbps (OLIVEIRA, 2012).

2.1.6 Controle de acesso ao meio

Para que possam existir redes sem fio com vários computadores, foi desenvolvido um protocolo de controle de acesso ao meio. Responsável por evitar colisões de pacotes entre maquinas que estejam utilizando o mesmo canal, é implementado na camada MAC.

Nas comunicações sem fio, o mecanismo de acesso ao meio é chamado de *Distributed Coordination Function* (DCF). Esse mecanismo é baseado no CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). O método de acesso ao meio pode ser descrito da seguinte forma: um dispositivo que deseja transmitir

escuta o meio, se estiver livre a transmissão ainda sim pode ser rejeitada. O dispositivo só poderá transmitir quando o meio estiver livre por um intervalo de tempo DIFS (*Distributed Inter Frame Space*), então transmite o pacote. Se o meio estiver ocupado o dispositivo terá que esperar um tempo de DIFIS e entrar numa fase de contenção. É escolhido um *backoff time* aleatório dentro de uma janela de contenção, então tenta acessar novamente o meio depois desse tempo aleatório. Se o meio estiver ocupado novamente, terá que esperar mais um tempo DIFS, em que o meio esteja livre, e repetir o processo.

Após todo processo para garantir disponibilidade do meio, se o meio estiver livre, primeiramente é transmitida uma solicitação para transmissão (RTS – *Request to Send*). Após recebimento do RTS, o receptor envia um CTS (Clear to Send), permitindo o remetente enviar o pacote. Com o recebimento do CTS o transmissor espera um tempo de SIFS (*Short Inter Frame Space*) e envia o pacote. O receptor verifica se o pacote esta correto e sem erros, aguarda um tempo SIFS e envia um pacote ACK (*Acknowledgment*). Sendo assim o transmissor, ao receber o ACK, sabe que o pacote foi transmitido com sucesso. Se o ACK não for recebido o transmissor enviará novamente o pacote (ARAÚJO, 2007). A figura 5 exemplifica o funcionamento desse processo.

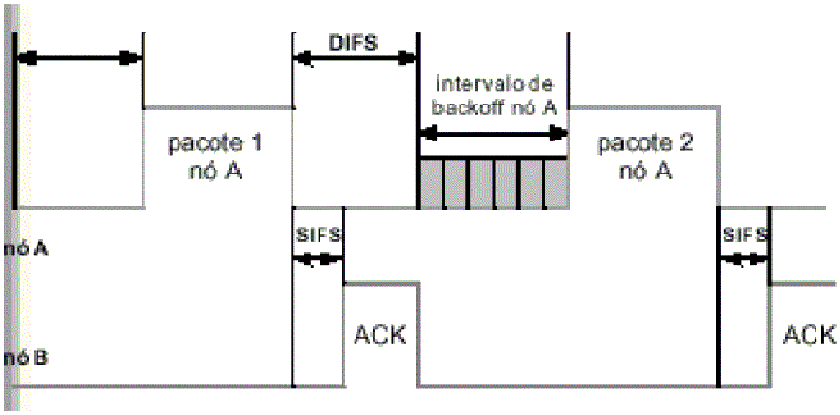

Figura 5: Estação operando com a DFC.
Fonte: http://www.garf.coppe.ufrj.br

2.1.7 Padrões de segurança em redes sem fio

O uso de redes sem fio implica em algumas características especiais no que diz respeito a segurança se forem colocadas lado a lado com redes cabeadas.

Ataques sofridos pelas redes sem fio dependem diretamente de como a rede foi implementada. Para que se tenham um padrão de segurança parecido com uma rede cabeada, há a necessidade de se incluir mecanismos de confidencialidade de informação e autenticação de elementos de rede.

Existem alguns sistemas de criptografia responsáveis por proporcionar mais privacidade e segurança de informações que trafegam pela rede. São eles: WEP, WPA e WPA2.

O WEP ou *Wired Equivalent Privacy* era o padrão inicialmente proposto para o padrão 802.11, porém apresentava alguns problemas. O conteúdo da chave de segurança devia ser configurado em todos os dispositivos que desejavam ter acesso a rede e em cada ponto de acesso de maneira estática. Logo, nem sempre essas chaves eram atualizadas. Assim, como o comprimento das chaves era pequeno, apenas 64 bits. Fazendo com que fossem facilmente burladas.

Já o WPA (*Wi-Fi Protected Access*), criado pelo grupo *Wi-Fi Alliance* faz troca dinâmica de chaves por meio de um protocolo chamado TKIP (*Temporal Key Integrity Protocol*) e utiliza o sistema de autenticação PSK (*Preshared Keys*). Dessa forma o WPA resolve os problemas apresentados pelo WEP, tem uma criptografia forte fazendo com que as chaves sejam automaticamente trocadas e autenticadas entre os elementos de pois de um período de tempo.

Por fim, o WPA2, também apresenta métodos mais eficientes de criptografia, troca dinâmica de chaves e autenticação, com a inclusão do padrão AES (*Advanced Encryption Standard*) (OLIVEIRA, 2012).

2.2 Voz sobre IP

A tecnologia VoIP é recente, foi explorada efetivamente a partir da década de 90. O VoIP possibilita que sejam efetuadas chamadas de voz sobre redes IP. Atualmente o interesse pela tecnologia de voz sobre IP vem crescendo exponencialmente, pois possibilita a convergência das redes de dados e voz em uma única infraestrutura, proporcionando uma economia significativa (OLIVEIRA, 2012).

2.2.1 Conceitos básicos

O VoIP é um tecnologia criada para transporte de voz, de maneira eficiente, em pacotes IP em uma rede de dados. Porém, não somente trata-se de transmissões de voz, mas também, de conteúdo multimídia.

O funcionamento do VoIP pode ser descrito da seguinte da seguinte maneira: A voz é transformada em um sinal elétrico analógico através de um microfone, que por sua vez é transformado em um sinal digital e codificado por um CODEC para que possa ser inserida em um pacote IP. Ao chegar em seu destino, o sinal é decodificado pelo CODEC e transformada novamente em um sinal analógico para que possa ser convertido em ondas sonoras (mecânicas), para por fim, ser compreendida (COUTO, 2010).

2.2.1.1 CODECs

O termo CODEC é uma abreviação de codificador/decodificador. São responsáveis pela conversão analógico/digital e da voz humana e da compressão e descompressão dos dados gerados. Os CODECs podem ser classificados em dois tipos: CODECs de forma de onda e paramétricos. Os CODECs baseados em forma de onda proporcional um sinal digitalizado bem próximo ao analógico original. Já os paramétricos, modelam a geração do sinal e enviam apenas parâmetros do sinal original. Este tipo, por sua, vez proporciona maiores taxas de compressão, por consequência este método é mais complexo e necessitam de mais processamento e maior capacidade de armazenamento.

Para mensurar a qualidade da chamada gerada por um CODEC, utiliza-se um parâmetro denominado MOS (*Mean Opinion Score*). Avalia a qualidade da chamada em uma escala de 1 até 5 (COUTO, 2010).

Score	Definição	Descrição
5	Excelente	Um sinal de voz perfeito gravado em um local silencioso
4	Bom	Qualidade de uma chamada telefônica de longa distância (PSTN)
3	Razoável	Requer algum esforço na escuta
2	Pobre	Fala de baixa qualidade e difícil de entender
1	Ruim	Fala não clara, quebrada

Quadro 2: Descrição da escala MOS.
Fonte: http://www.teleco.com.br/

No quadro abaixo, seguem alguns dos principais CODECs e suas características.

Método de Compressão	Bit Rate (kbit/s)	MOS Score	Delay (ms)
G.711 PCM	64	4.1	0.75
G.726 ADPCM	32	3.85	1
G.728 LD-CELP	16	3.61	3 to 5
G.729 CS-ACELP	8	3.92	10
G.729 x 2 Encodings	8	3.27	10
G.729 x 3 Encodings	8	2.68	10
G.729a CS-ACELP	8	3.7	10
G.723.1 MP-MLQ	6.3	3.9	30
G.723.1 ACELP	5.3	3.65	30

Quadro 3: Características dos CODECs.
Fonte: http://www.teleco.com.br/

2.2.2 Modelos de implementação

Pode-se construir uma rede VoIP sob vários topologias diferente. Destacam-se as topologias Ponto-a-Ponto, com *Gateway* e Híbrida.

A arquitetura Ponto-a-Ponto é constituída por dois ou mais elementos, estes podem ser PCs com *softphone* instalados ou telefones IPs. Nessa modelo, os próprios elementos fazem o tratamento da voz e as chamadas são feitas baseadas nos endereços IPs de destino.

A implementação com um *Gateway*, os telefones convencionais (PSTN) ligam para um Gateway de telefonia próximo as suas centrais. Este é responsável pela

codificação, empacotamento do sinal de voz, e em alguns casos pela digitalização da voz, que pode ser feita pelo próprio telefone. O Gateway de entrada valida o numero do remetente e solicita o numero do destinatário. Dados que são passados para o Gateway de saída, que inicia uma sessão de transmissão de pacotes IP. Quando o destinatário atende, inicia-se a transmissão de pacotes de voz sobre IP.

Em muitos casos a topologia utilizada é hibrida. Pois é necessário que seja possível a realização de chamadas entre telefones convencionais, telefones IPs e PCs com *Softphones* (ARAÚJO, 2007).

A figura 6 representa uma rede Híbrida.

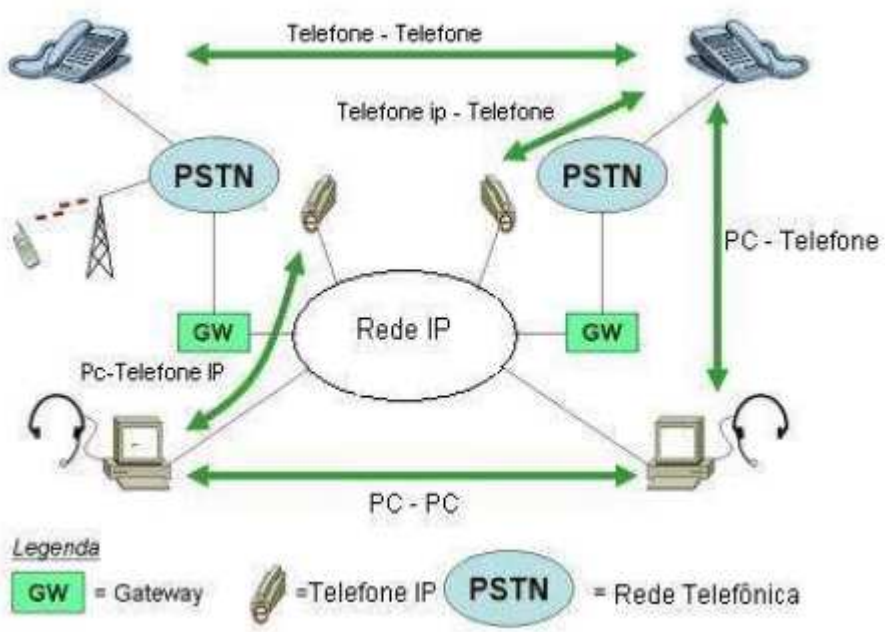

Figura 6: Rede VoIP Híbrida.
Fonte: http://monografias.cic.unb.br

2.2.3 Protocolos VoIP

O protocolo IP apenas, não é capaz de garantir a comunicação de voz entre dispositivos. Para que seja possível ter um resultado igual ou superior às redes de telefonia convencionais, é necessário que sejam implementados outros protocolos e soluções adicionais.

Os principais protocolos empregados na tecnologia VoIP são categorizados por sua finalidade da seguinte forma: protocolos de sinalização, *Gateways* e Midia. A figura 7 representa os protocolos VoIP de acordo com sua classificação.

Os principais protocolos do VoIP são: H.323, SIP, IAX e Megaco ou H.248. Além dos protocolos de voz, são utilizados, também, protocolos de transporte, como o UDP, RTP e RTCP, que atuam na camada de transporte do modelo OSI (COUTO, 2010).

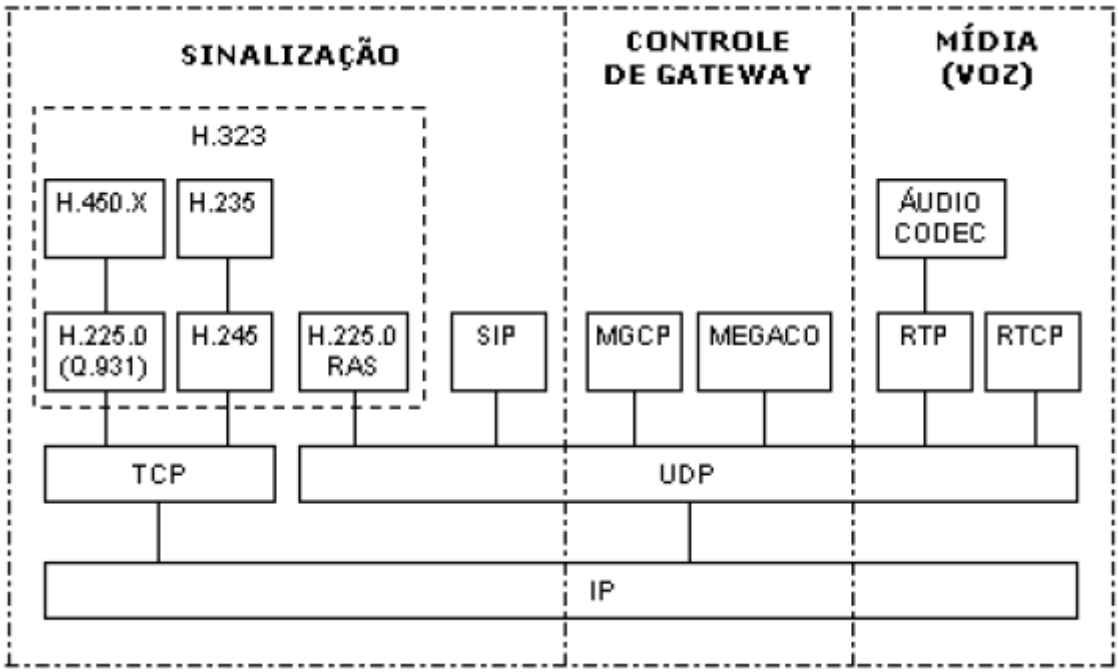

Figura 7: Protocolos VoIP.
Fonte: http://bdtd.bczm.ufrn.br

2.2.3.1 Protocolos de Midia

Protocolos utilizados para transporte de mídias, como por exemplos os protocolos RTP e RTCP. O RTP (*Real-Time Transport Protocol*) é utilizado para transporte de dados em tempo real, esses podem ser voz e imagem. O protocolo oferece transporte fim a fim destinado a aplicações que manipulam dados em tempo real. O RTP identifica o tipo dos dados que estão sendo transportados, marca os pacotes em sequência, grava o tempo da sessão e monitora a qualidade. Portanto, o RTP não possui dispositivos que garantam a entrega dos pacotes no tempo esperado ou com uma qualidade superior. Para tal finalidade é utilizado, em conjunto o protocolo RTCP (*Real-Time Transport Control Protocol*). Esse protocolo permite monitoramento da entrega dos pacotes e a qualidade de serviço de forma escalável. Esse monitoramento é feito através do envio, periódico, de pacotes de

controle para os participantes da sessão RTP. Ambos os protocolos, RTP e RTCP, são elementos centrais da maioria dos sistemas e serviços VoIP (COUTO, 2010).

2.2.3.2 Protocolos de sinalização

Protocolos de sinalização são encarregados pelo estabelecimento da conexão entre os dispositivos realizadores das chamadas, o controle dessa conexão a finalização da chamada. Após o encerramento da conexão, deve-se ser sinalizada a liberação do meio.

Alguns dos protocolos de sinalização existentes são H.323 e o SIP (*Session Initiation Protocol*). Na figura 8 são apresentados os protocolos H.323 e SIP de acordo com o modelo OSI (COUTO, 2010).

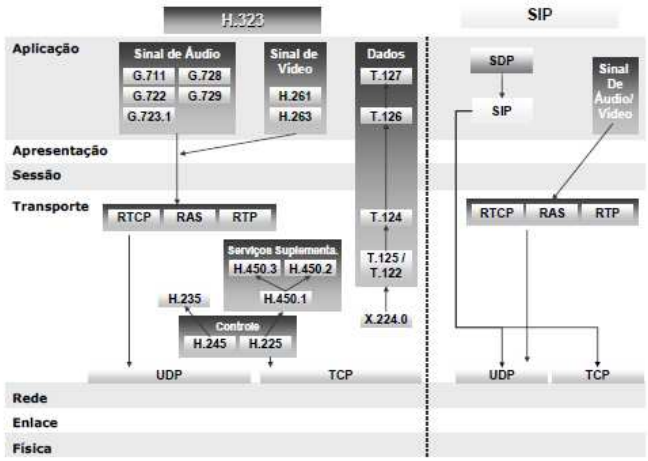

Figura 8: Protocolos SIP e H.323.
Fonte: http://bdtd.bczm.ufrn.br

2.2.3.2.1 Protocolo SIP

É um protocolo de sinalização de telefonia IP, que atua na camada de aplicação, e teve sua origem em meados de 1990 com seu principio de funcionamento parecido com o HTTP. É utilizado para estabelecer, encerrar e modificar conferencias ou chamadas VoIP. Essas características deixam o controle da aplicação para o terminal, o que não faz necessário uma central de resposta, a exemplo do H.323.

Baseado em uma arquitetura cliente/servidor, o SIP, opera sobre os protocolos UDP ou TCP, sendo mais comum o UDP. Tem por objetivo localizar e convidar dispositivos para participar das chamadas. É responsável pelo gerenciamento das chamadas, como início e término, inclusão e exclusão de participantes, podendo ser em transmissões *unicast* ou *multicast*. O SIP é utilizado em conjunto com outros protocolos, como o RTP e SDP (*Session Description Protocol*) para descrever sessões multimídia e prover serviços ao usuário. No entanto, a sinalização da comunicação é independente do tratamento do transporte de mídia.

Cada dispositivo é visto como uma entidade que requisita ou recebe respostas. Essas requisições ou respostas ocorrem até que ocorra uma mensagem final. As mensagens SIP são codificadas em formato de texto (COUTO, 2010).

2.2.3.2.2 Componentes do SIP

A arquitetura SIP é composta pelos elementos: terminais, servidor *Proxy,* servidor de registro, servidor de redirecionamento e servidor de localização.

Os terminais são programas no dispositivo final, como por exemplo um PC ou um telefono IP, que solicitam inicio de uma chamada e respondem a outras solicitações da rede.

O servidor *Proxy* funciona como um roteador. Sua função é receber uma requisição e encaminha-la para outro servidor ou terminal. Se necessário, o servidor, é capaz de resolver nomes consultando um DNS.

O servidor de registro é responsável por registrar os usuários e receber solicitações sobre a localização dos terminais.

Já o servidor de redirecionamento, responde as requisições referentes aos endereços dos terminais.

Por fim, o servidor de localização disponibiliza a localização atual de qualquer dispositivo na rede. A figura 9 ilustra a disposição dos componentes da arquitetura SIP (OLIVEIRA, 2012).

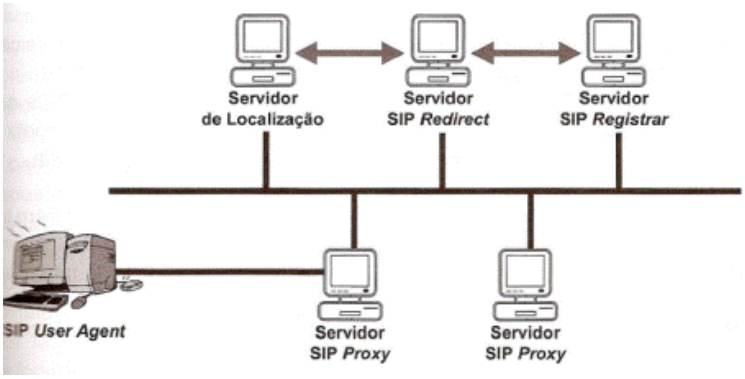

Figura 9: Componentes do SIP.
Fonte: http://www.teleco.com.br/

2.2.3.2.3 Mensagens SIP

Existem as mensagens de requisição e resposta. As mensagens de requisição são geradas pelo cliente ou por um servidor proxy. Abaixo segue o quadro 4 com os métodos de requisição.

Método	Funcionalidade
INVITE	Estabelece uma sessão
BYE	Término de uma sessão
ACK	Confirma o recebimento de um INVITE
REGISTER	Registra alocalização atual de um usuário

Quadro 4: Mensagens de requisição.
Fonte: http://monografias.cic.unb.br

As mensagens de reposta são usadas por todos os dispositivos de uma sessão SIP. São formadas por um código numérico de três dígitos separados em seis classes. O quadro 5 apresenta as mensagens de resposta (ARAUJO, 2007).

Categoria	Funcionalidade
1xx	Resposta Informativa
2xx	Resposta de Sucesso
3xx	Resposta de Redirecionamento
4xx	Resposta de Falha em Cliente
5xx	Resposta de Falha em Servidor
6xx	Resposta de Falha Global

Quadro 5: Mensagens de resposta.
Fonte: http://monografias.cic.unb.br

2.2.3.2.4 Estabelecimento de uma chamada SIP

O SIP suporta o estabelecimento de sessão *peer-to-peer* ou via *proxy*. O modo *peer-to-peer* é o mais simples para se estabelecer as chamadas, logo como não há um servidor intermediário presente, alguns serviços não vão estar disponíveis. Já a comunicação via *proxy* conta com a presença de um servidor responsável por receber e encaminhar as informações e controlar o seu fluxo. A figura 10 apresenta o processo de estabelecimento de uma sessão SIP (ARAUJO, 2007).

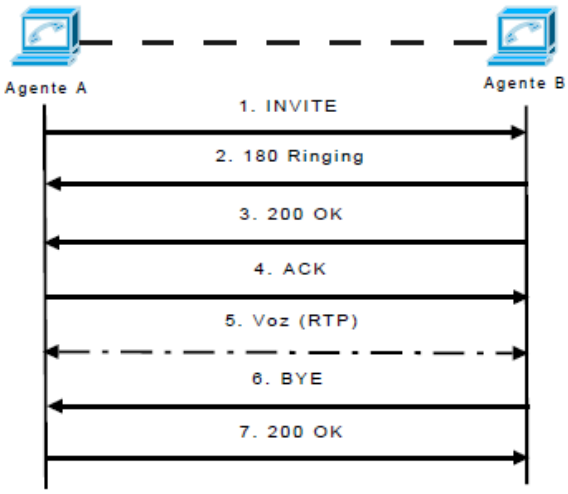

Figura 10: Estabelecimento de uma sessão SIP.
Fonte: http://monografias.cic.unb.br

2.2.3.2.5 Padrão H.323

Criado pela ITU-T, é um conjunto de recomendações destinado para voz e vídeo em uma rede de dados.

O desenvolvimento do H.323 visa a interoperabilidade com outras redes de serviços multimídia. Nesse padrão existem alguns componentes específicos quanto a arquitetura. Como por exemplo, o *gateway*, onde seu papel é proporcionar maior interoperabilidade entre redes (OLIVEIRA, 2012).

2.2.3.3 Protocolos de controle de *Gateway*

Gateways são interconexões de dispositivos em rede VoIP, que atuam como uma ponte dentre o VoIP e outra rede externa. São considerados elementos controladores que operam sobre a rede IP e se comunicam através do protocolo de controle de *Gateway*, o MGCP (*Media Gateway Control Protocol*) e o MEGACO ou H.248.

O MGCP é um protocolo mestre-escravo que usado para o estabelecimento, controle e termino das chamadas. Já o MEGACO, foi desenvolvido com a finalidade de ser uma alternativa ao MGCP. Apresenta diferenças, como um melhor suporte a conferencias (MOREAU, 2012).

2.2.4 Qualidade de serviço em VoIP

Devido ao fato de que o protocolo UDP não garante que os pacotes sejam entregues em ordem e também não prove garantias de qualidade do serviço, redes VoIP sofrem com propriedades intrínsecas da comutação por pacotes. Algumas dessas propriedades são: o atraso, *Jitter,* taxa de perda de pacotes, banda disponível e o eco.

O atraso é o tempo que o pacote leva para passar pelo meio de transmissão e chegar ao seu destino. De modo geral sistemas de tempo real tem o atraso como fator importante na determinação da qualidade, o que não é diferente em redes VoIP. Há um tempo máximo aceitável para que o som da voz enviado deve chegar ao receptor. A ITU-T recomenda que os atrasos totais do sistema não ultrapassem 150 ms para que a conversação não seja afetada.

O atraso é gerado pelos seguintes fatores: Filas dos pacotes entre roteadores ao longo do caminho, *buffer* de *jitter*, atraso na codificação e decodificação, serialização do pacote IP, atraso de propagação na rede.

O *jitter* está relacionado com a variação na taxa de atraso dos pacotes, ou seja, é a diferença entre o atraso do pacote atual e o do próximo pacote. O *jitter* é causado pelo comportamento aleatório do tempo de enfileiramento dos pacotes nos roteadores. Variação bruscas no atraso podem impactar muito na qualidade do

VoIP, fazem com que pacotes sejam processados fora de ordem. O ITU-T recomenda que o *jitter* não ultrapasse 30 ms.

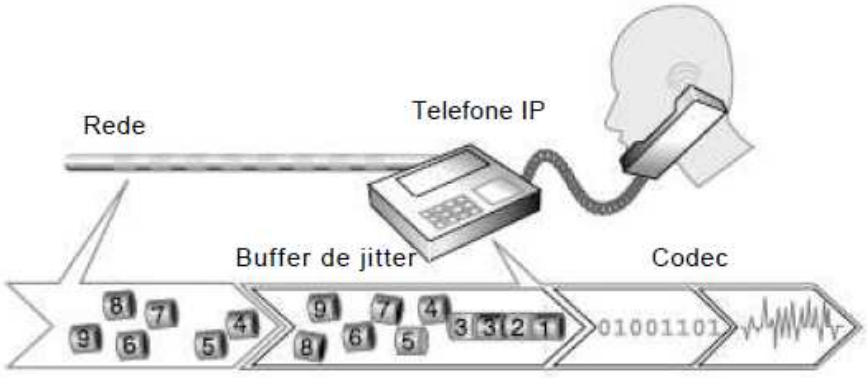

Figura 11: *Jitter*.
Fonte: http://monografias.cic.unb.br

A taxa de perda de pacotes representa a quantidade de pacotes que são enviados e não chegam ao seu destino final. A principal causa da perda de pacotes é o congestionamento nos *buffers* entre os diversos dispositivos da rede, além de aumento abruto do tráfego na rede, atrasos em excesso causados por problemas fiscos em equipamentos de transporte. A perda de pacotes máxima recomendada pelo ITU-T é de 1% (ITU-T, 2006).

A largura de banda é um fator importante na implementação de redes VoIP, principalmente na definição de classes de serviço. Sendo assim, cada aplicação na rede terá uma determinada banda alocada para o seu melhor desempenho. Largura de banda é um recurso escasso, portanto, no VoIP é necessário empregar CODECs, que juntamente com algoritmos de compressão e descompressão permitem uma economia de banda. Pois transmitir voz puramente ocuparia muito à banda da rede.

Por fim, o eco que é o sinal de voz de quem fala refletido de volta para origem, com intensidade e atraso suficientes para que seja confundido como parte da conversação. O eco pode ser causado por inconsistências de impedância nos circuitos analógicos (ARAUJO, 2007).

2.3 Asterisk

Desenvolvido em 1999 pela Digium Inc., o Asterisk, é um software que implementa um PABX de telefonia. Utilizado em diversos contextos, o Asterisk é capaz de interligar redes VoIP com as redes de telefonia convencionais.

O Asterisk é um *software* de PABX livre lançado sob a GLP 2 (*General Public Licence*) que roda, também, em Linux e em outras plataformas Unix, podendo ser ou não conectado a rede publica através de hardware específico. A Digium investe continuamente no desenvolvimento do código fonte assim como em *hardware* de telefonia compatíveis com Asterisk.

O software é programado em linguagem C, com alguns módulos em Pearl, PHP e Java. Funciona em Linux com a versão do Kernel a partir de 2.4 e não depende de hardware especifico para o funcionamento. A implementação do servidor Asterisk é simples e rápida, assim como a sua configuração. A figura abaixo ilustra a visão geral da arquitetura Asterisk (GONÇALVES, 2012).

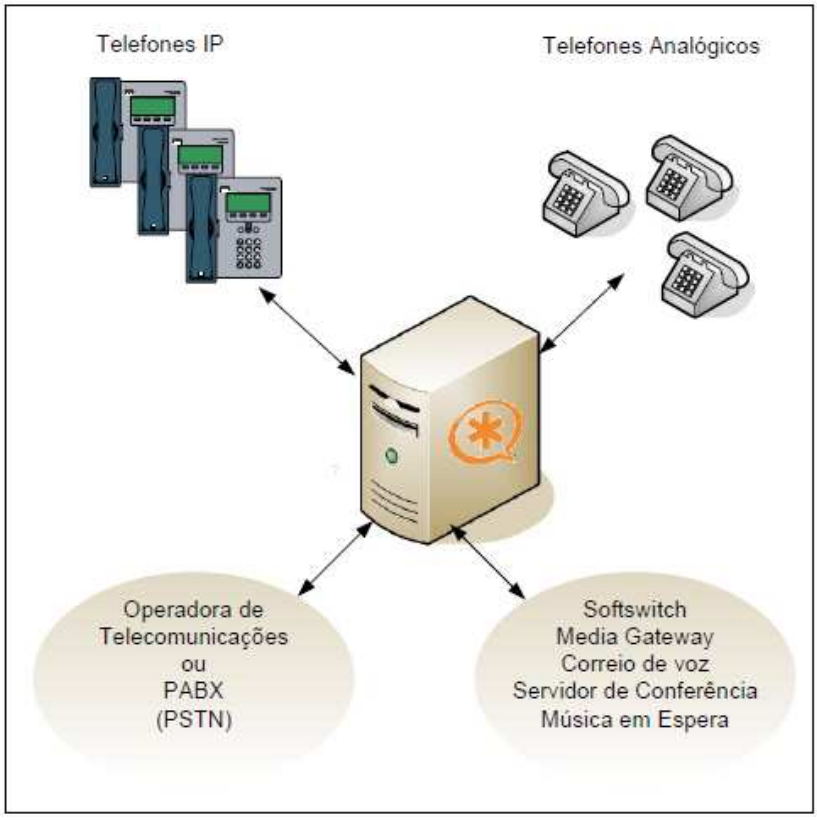

Figura 12: Visão geral da arquitetura Asterisk.
Fonte: http://www.taioque.com.br/linux/Livro Asterisk Curso Completo.pdf

2.3.1 Dimensionamento de *Hardware*

Uma maquina ideal para rodar o servidor Asterisk deve ter apenas essa função. Ou seja, o processador deve ser exclusivo para processamento das ligações realizadas. O servidor Asterisk deve ter no mínimo um processador compatível com Intel superior a um Pentium 300Mhz com 256 MB RAM. Como o sistema não requer muito espaço em disco, 100 MB são compilados.

Se o uso for apenas do VoIP, não se faz necessária a utilização de hardwares adicionais, não é necessário ter uma placa de vídeo sofisticada ou periféricos. Sendo assim, pode-se utilizar *softphones* e utilizar operadoras gratuitas ou não para prover entroncamento. Caso contrário, será necessário incorporar ao sistema hardwares para conexão com uma rede de telefonia convencional (GONÇALVES, 2012).

2.3.2 Instalação do Asterisk

O *software* Asterisk necessita da instalação de alguns outros módulos. Esses, podendo incluir bibliotecas de fabricantes diferentes. Os próprios módulos Asterisk, em algumas situações, não possuem sincronismo com o lançamento das versões. Por esse motivo é importante consultar o site oficial da comunidade Asterisk: http://forums.digium.com.

Para instalação do Asterisk, se faz necessário a instalação de algumas dependências. Pode-se instala-las em um ambiente Linux Debian através dos seguintes comandos:

```
# apt-get install bison openssl libssl-dev libusb-dev fxload liba-sound2-dev libc6-dev libnewt-dev libncurses5-dev zlib1g-dev gcc g++ make doxygen linux-headers-`uname-r` module-assistant

# m-a prepare

# ln –s /usr/src/linux-headers-`uname-r` /usr/src/linux
```

Após o download e instalação dos pré-requisitos de software deve-se reiniciar a maquina e baixar os seguintes softwares: o próprio Asterisk, Zaptel, Libpri e Asterisk-addons.

Para realizar esse processo foi executado os comandos abaixo.

```
# mkrdir /tmp/asterisk
# cd /tmp/asterisk
# wget http://downloads.digium.com/pub/asterisk/releases/asterisk-
1.4.21.tar.gz -O /tmp/asterisk/asterisk-1.4.21.tar.gz
# wget http://downloads.digium.com/pub/zaptel/releases/zaptel-
1.4.11.tar.gz  -O /tmp/asterisk/zaptel-1.4.11.tar.gz
# wget http://downloads.digium.com/pub/libpri/releases/libpri-
1.4.4.tar.gz  -O /tmp/asterisk/libpri-1.4.4.tar.gz
# wget http://downloads.digium.com/pub/ asterisk
/releases/asterisk-addons-1.4.7.tar.gz  -O
/tmp/asterisk/asterisk-addons-1.4.7.tar.gz
```

Após término do download dos módulos, deve-se descompacta-los individualmente na pasta /usr/src de acordo com os comandos abaixo:

```
# tar –xvzf /usr/src/asterisk-1.4.21.tar.gz
# tar –xvzf /usr/src/zaptel-1.4.11.tar.gz
# tar –xvzf /usr/src/libpri-1.4.4.tar.gz
# tar –xvzf /usr/src/asterisk-addons-1.4.7.tar.gz
```

Com os módulos descompactados, dá-se inicio ao processo de compilação dos mesmos. Os pacotes são compilados na da seguinte forma: Zaptal, libpri, asterisk e asterisk-addons. Abaixo segue os comandos a serem executados.

```
# cd /usr/src/zaptel-1.4.11
# ./configure
# make menuconfig
# make
# make install
# make config
```

```
# cd /usr/src/libpri-1.4.4
# make
# make install

# cd /usr/src/asterisk-1.4.21
# ./configure
# make menuconfig
# make
# make install
# make config
# make samples

# cd /usr/src/asterisk-addons-1.4.7
# ./configure
# make menuconfig
# make
# make install
```

Comandos para adicionar o módulo ztdummy na inicialização automática do sistema:

```
# modprobe ztdummy
# echo “ztdummy” >> /etc/modules
```

2.3.3 Configuração básica do Asterisk

O diretório principal do Asterisk está localizado no /etc/asterisk. Nele, encontram-se praticamente todos os arquivos de configuração, rotas, filas, rotas e outras especificações do servidor (OLIVEIRA, 2012).

2.3.3.1 Plano de discagem

O plano de discagem é considerado o coração do Asterisk, funciona como o *core* do servidor. Está contido no arquivo /etc/asterisk/extensions.conf e define como serão gerenciadas as chamadas listando instruções que o Asterisk deverá seguir. Essas instruções são acionadas através dos dígitos recebidos de um telefone ou

uma aplicação. No arquivo extensions.conf encontramos as seguintes partes: Aplicações, Contextos, Extensões e Prioridades.

Contextos têm um importante papel na organização e segurança do plano de discagem, também definem um escopo e separam diferentes partes do mesmo. Cada ligação que entra no Asterisk é processada dentro de um contexto que está ligado diretamente a um canal.

Por exemplo, tendo dois tipos de ramais, gerentes e funcionários. Os gerentes podem fazer ligações de longa distancia e os funcionários não. Quando um gerente digita “0” ouve-se o tom de discagem. Já quando um funcionário disca o “0” é recebido uma mensagem de “ligação proibida”. São criados contextos [gerentes] e [funcionários].

No entanto, dependendo do contexto escolhido, diferentes canais podem ser recebidos em diferentes telefones, pois, uma ligação é recebida dentro do contexto do canal.

Existe um contexto denominado [globals], que fica localizado no inicio do arquivo extensions.conf. É onde as variáveis são definidas, podendo ser utilizados em todo plano de discagem.

Extensões são *strings* que disparam eventos e são definidas dentro de cada contexto. A figura 13 apresenta algumas extensões.

```
exten=>8580,1,Dial(SIP/8580,20)
exten=>8580,2,voicemail(u8580)
exten=>8580,101,voicemail(b8580)
```

Figura 13: Extensões.
Fonte: http://www.taioque.com.br/linux/Livro Asterisk Curso Completo.pdf

O comando “exten=>” define qual o próximo passo para a chamada. O número 8580 são os dígitos discados. Os números 1, 2 e 101 são as prioridades, que são passos ordenados para execução das extensões, onde cada prioridade aciona uma determinada aplicação. Aplicações são partes fundamentais no servidor Asterisk, elas regulam o canal tocando sons, validando dígitos ou encerrando chamadas. No exemplo acima, discando o numero 8580 irá fazer com que toque, durante 20 segundos o ramal configurado com este número, caso ninguém atenda, será encaminhado para prioridade 2 e se estiver ocupado, encaminhado para 101

(GONÇALVES, 2012). Abaixo segue o exemplo de configuração utilizado no neste trabalho.

```
root@tarcizoserver:/etc/asterisk# cat extensions.conf
[teste]

exten => 9000,1,Dial(SIP/9000,30);
exten => 9000,2,Hangup;
exten => 9001,1,Dial(SIP/9001,30);
exten => 9001,2,Hangup;
```

A prioridade 2, *Hangup*, faz com que o usuário seja desconectado.

2.3.3.2 Configuração dos ramais utilizando SIP

A configuração dos ramais utilizando o protocolo SIP, é feita através do arquivo /etc/asterisk/sip.conf, que possui configurações dos clientes que podem ser telefones IPs ou *softphones*. O arquivo é interpretado de cima para baixo, possui a primeira parte com as configurações globais, como endereço IP e número de porta que o servidor está ligado.

As próximas seções determinam parâmetros como nome de usuário, senha e endereço IP para os clientes (GONÇALVES, 2012). O quadro 6 apresenta os parâmetros de configuração global.

Parâmetro	Descrição
allow	Permite que um determinado codec seja usado.
bindaddr	Endereço IP onde o Asterisk irá esperar pelas conexões SIP.
context	Configura o contexto padrão onde todos os clientes serão colocados.
disallow	Proíbe um determinado codec.
port	Porta que o Asterisk deve esperar por conexões de entrada SIP.
tos	Configura o tipo de serviço usado para o SIP e RTP.
maxexpirey	Tempo máximo para registro em segundos.
defaltexpirey	Tempo padrão para registro em segundos.
register	Registra o Asterisk com outro host.

Quadro 6: Configurações globais.
Fonte: http://www.taioque.com.br/linux/Livro Asterisk Curso Completo.pdf

Depois da seção global, definem-se as configurações SIP dos clientes, que são divididos como *peer*, *user* e *friend*.

O *peer* é a entidade que o servidor Asterisk envia ligações, o provedor. A entidade que faz chamadas através do Asterisk é definhada como *user*, e a que faz esses dois papeis ao mesmo tempo é denominada *friend* (GONÇALVES, 2012). O quadro 7 apresenta alguns parâmetros de configuração das entidades SIP.

Parâmetro	**Descrição**
type	Configura a classe de conexão.
host	Configura o endereço IP ou nome do host.
username	Esta opção configura o nome do usuário que o Asterisk tenta conectar quando uma chamada é recebida.
secret	Um segredo compartilhado usado para autenticar as entidades.

Quadro 7: Configurações das entidades.
Fonte: http://www.taioque.com.br/linux/Livro Asterisk Curso Completo.pdf

Abaixo segue, como exemplo, o arquivo de configuração sip.conf utilizado nesse trabalho.

```
root@tarcizoserver:/etc/asterisk# cat sip.conf
[general];
context = defalt;
bindport = 5060;
bindaddr = 0.0.0.0;
srvlookup = yes;


[9000];
type = friend;
callerid = "9000" <9000>;
username = 9000;
secret = 1234;
host = dynamic;
canreinvite = no;
context = instituto;

[9001];
type = friend;
callerid = "9001" <9001>;
username = 9001;
```

```
secret = 1234;
host = dynamic;
canreinvite = no;
context = teste;
```

3 AMBIENTE DE TESTES

Este capítulo tem o objetivo de descrever a montagem do ambiente de testes e procedimentos utilizados para execução dos mesmos, desde *softwares* utilizados até procedimentos e técnicas empregadas.

3.1 Softwares utilizados

3.1.1 Softphones

São aplicativos multimídia, que em conjunto com a tecnologia VoIP funcionam como um telefone comum. Nesse trabalho foram utilizados os *softphones* descritos abaixo.

O X-Lite que foi desenvolvido pela *CounterPath,* que é proprietário porém é distribuído gratuitamente. É derivado do *eyeBeam* e utiliza o protocolo SIP como padrão.

O software Ekiga é uma aplicação livre, de vídeo conferências e telefonia IP para o GNOME. É liberado sob licença GPL, disponível em *Windows* e Linux. A aplicação verifica a porcentagem de perda de pacotes, pacotes atrasados e fora de ordem.

3.1.2 Wireshark

Ferramenta utilizada para análise do tráfego de rede. Ela captura os pacotes e os organiza pelos protocolos. Suas funcionalidades são semelhantes as do *tcpdump* com uma interface gráfica.

3.1.3 Iperf

É uma ferramenta de medição de desempenho de rede utilizada para gerar tráfego de pacotes TCP e UDP desenvolvida em C++. Permite ao usuário definir parâmetros que auxiliam o teste de uma rede. Tem funcionalidade de cliente/servidor e pode medir o desempenho da rede unidirecionalmente ou bi-

direcionalmente. É um software de código aberto que roda em plataformas *Windows* e Linux.

3.2 Descrição e configuração do ambiente

Para realização dos testes foram montados em um ambiente *indoor*, uma topologia baseada em rede sem fio, com o objetivo de executar testes de chamadas entre clientes da rede e analisar os parâmetros de qualidade fazendo uma comparação entre os testes realizados.

O ambiente sem fio é composto por três clientes, sendo eles dois computadores munidos de placas de rede *wireless* e um *smartphone* com um *softphone* genérico instalado. Um *access point* central faz a distribuição do sinal da rede que é conectado via cabo ao servidor Asterisk e um modem ADSL com DHCP configurado. O local para realização dos testes possui três andares, o *access point* foi instalado no terceiro andar. Sendo assim, foram realizadas quatro chamadas para coleta de dados. A primeira foi realizada no mesmo andar onde se situa o AP e as demais foram realizadas nos andares abaixo em sequência. A figura 13 ilustra a disposição do ambiente de testes descrito anteriormente.

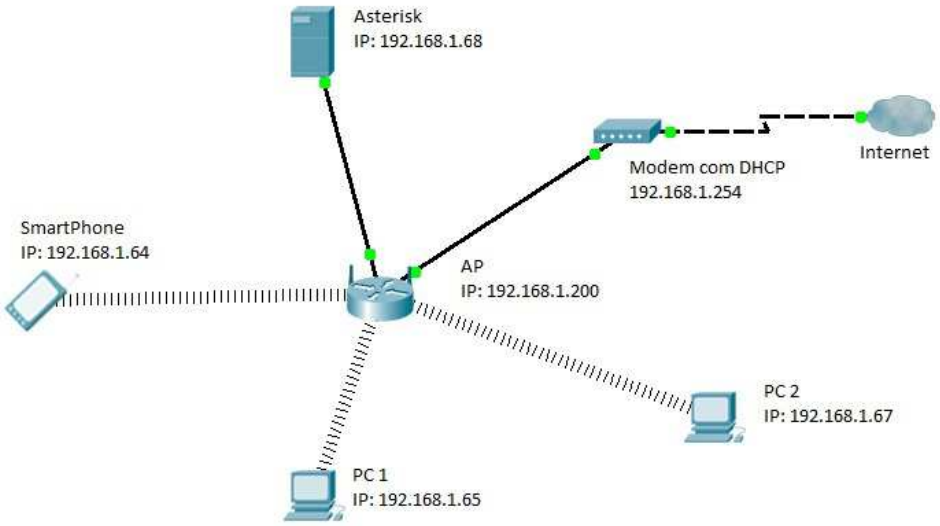

Figura 13: Disposição do ambiente *Wireless*.
Fonte: Autoria própria.

3.2.1 Configuração do Asterisk e clientes

O servidor Asterisk foi configurado de uma maneira muito simples, com o objetivo de simplesmente prover as chamadas na rede VoIP. O Asterisk possibilita inúmeras funcionalidades em suas configurações que saem do foco central do trabalho. A seguir seguem as configurações realizadas para execução dos experimentos.

O arquivo extensions.conf e sip.conf:

```
root@tarcizoserver:/etc/asterisk# cat extensions.conf
[teste]

exten => 9000,1,Dial(SIP/9000,30);
exten => 9000,2,Hangup;
exten => 9001,1,Dial(SIP/9001,30);
exten => 9001,2,Hangup;
exten => 9002,1,Dial(SIP/9002,30);
exten => 9002,2,Hangup;

root@tarcizoserver:/etc/asterisk# cat sip.conf
[general];
context = defalt;
bindport = 5060;
bindaddr = 0.0.0.0;
srvlookup = yes;

[9000];
type = friend;
callerid = "9000" <9000>;
username = 9000;
secret = 1234;
host = dynamic;
canreinvite = no;
context = instituto;

[9001];
type = friend;
callerid = "9001" <9001>;
username = 9001;
secret = 1234;
host = dynamic;
```

```
canreinvite = no;
context = teste;

[9002];
type = friend;
callerid = "9002" <9002>;
username = 9002;
secret = 1234;
host = dynamic;
canreinvite = no;
context = teste;
```

Para realização das chamadas, nos clientes foi instalado o *softphone* X-Lite com as seguintes configurações demonstradas pela figura 15:

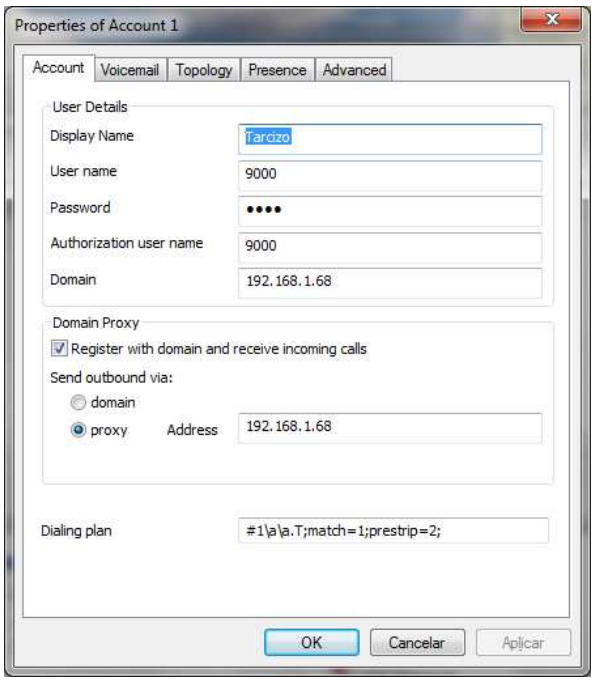

Figura 15: Configuração do cliente VoIP.
Fonte: Software X-Lite

3.3 Coleta dos dados

Para a coleta dos dados foi utilizado o *software Wireshark* instalado em um dos computadores realizadores de chamadas, onde foram filtrados os pacotes do protocolo RTP durante as ligações, a partir da sua interface de rede.

Primeiramente a coleta foi feita em uma chamada realizada pelos clientes no mesmo andar onde se situa o AP. A chamada foi realizada entre o PC1 e o *smartphone* (de acordo com a figura 16) de aproximadamente três minutos, sem adição de tráfego concorrente na rede. O *Wireshark* foi instalado no PC1 “ouvindo” a sua interface de rede sem fio. Posteriormente foram realizadas mais três novas chamadas nos demais andares do local, com o intuito de aumentar a distância e adicionar obstáculos na rede sem fio. E, um teste adicional, onde uma chamada foi realizada com a inserção de um tráfego concorrente na rede de 80 kbps, com o objetivo de analisar o seu comportamento com outra ligação em paralelo. Tráfego adicionado através do *software Iperf* com o comando iperf -s -u -i 1, para o servidor, onde o parâmetro –s indica que o funcionamento será de servidor, o –u aplica o tráfego udp e por fim, -i 1 faz com que sejam exibidos de um em um segundo as informações dos pacotes na tela. Para o cliente o seguinte comando foi utilizado: iperf -c 192.168.1.68 -u -b 80k -d -t 99999. O parâmetro c indica modo cliente, -b é utilizado para definir a largura de banda a ser utilizada, -d habilita tráfego bidirecional no circuito e -t define o tempo em segundos em que os pacotes serão enviados. As figuras 17 e 18 ilustram o processo.

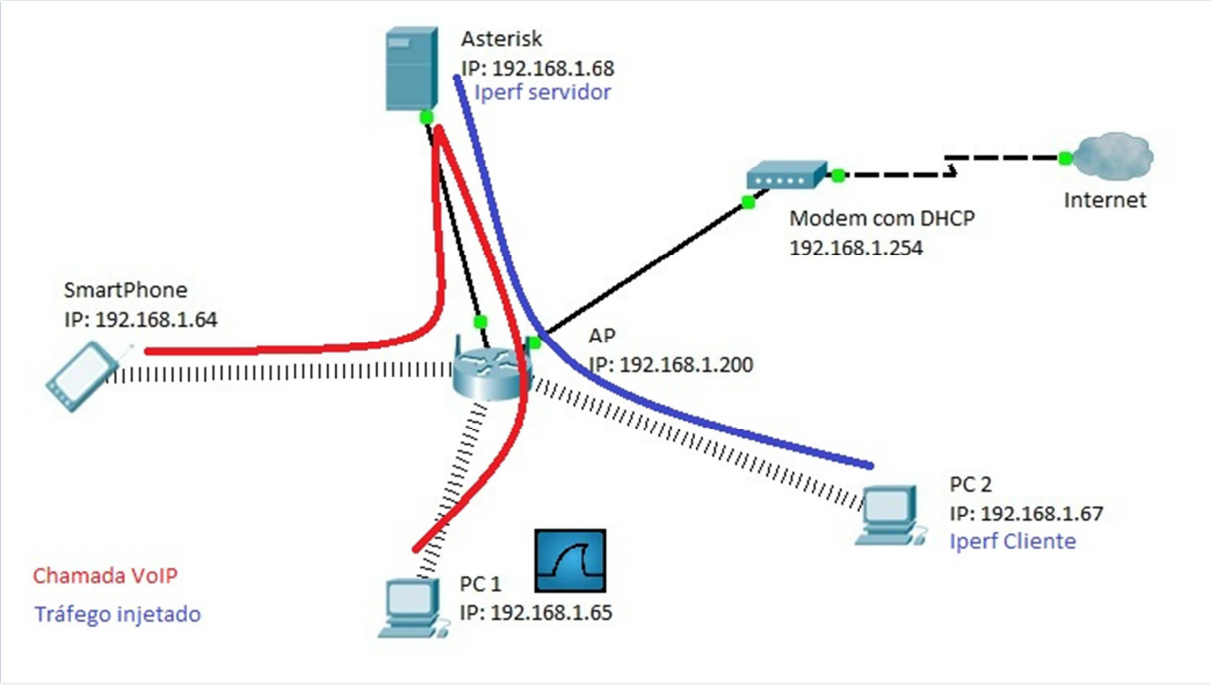

Figura 16: Topologia do ambiente de testes.
Fonte: Autoria própria.

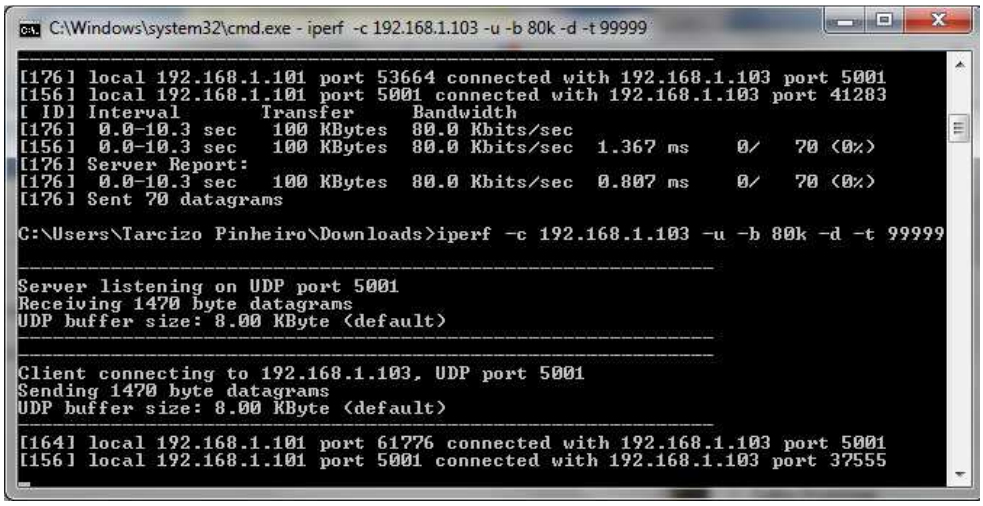

Figura 17: *Iperf* em modo cliente.
Fonte: Autoria própria.

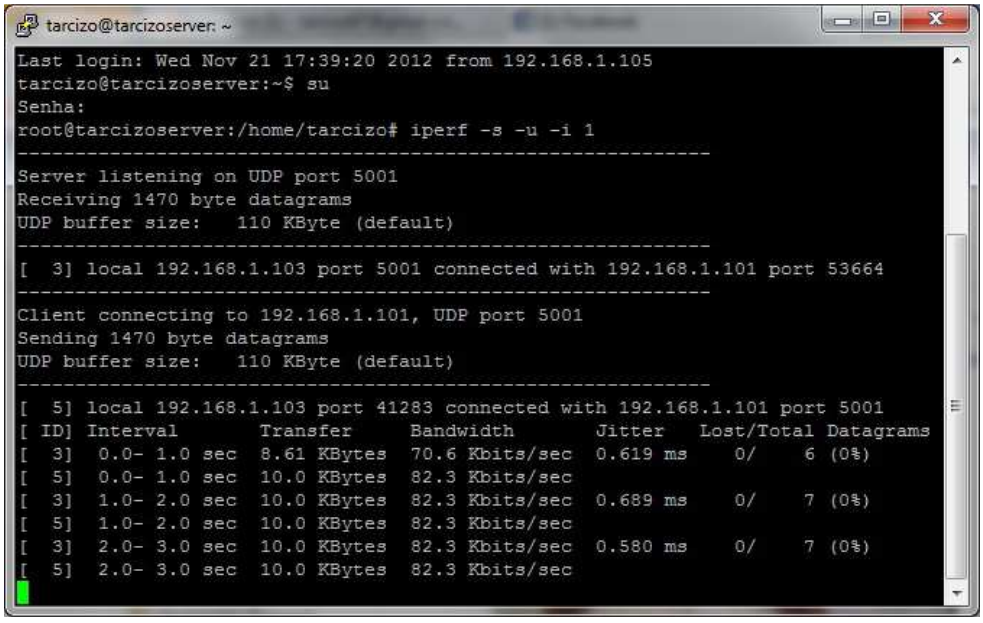

Figura 18: *Iperf* em modo servidor.
Fonte: Autoria própria.

4 RESULTADOS

O primeiro teste foi realizada com os dispositivos próximos ao AP. A ligação fluiu normalmente sem picotes e com bom áudio. As figuras 19 e 20 apresentam os gráficos da latência e *Jitter* dessa chamada. Nos gráficos estão representados os níveis recomendados pelo ITU-T que são de 150 ms para latência entre os pacotes e 30 ms para *Jitter*.

Os parâmetros coletados no primeiro teste foram: *Jitter* médio 20,48 ms, *Jitter* máximo de 28,56 ms, latência máxima entre um pacote e outro de 134,18 ms, latência media de 19,98 ms e zero pacotes perdidos.

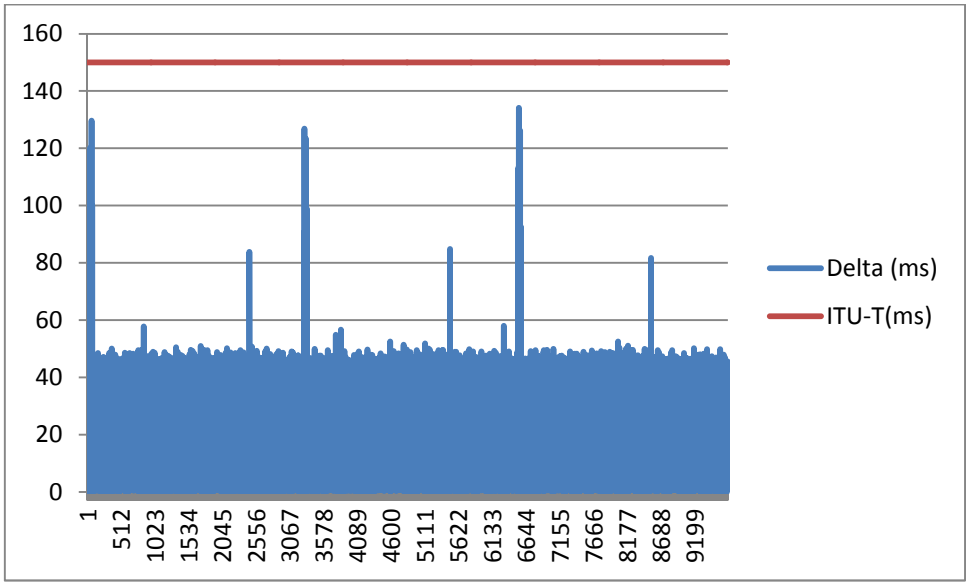

Figura 19: Gráfico da latência na primeira chamada.
Fonte: Autoria própria.

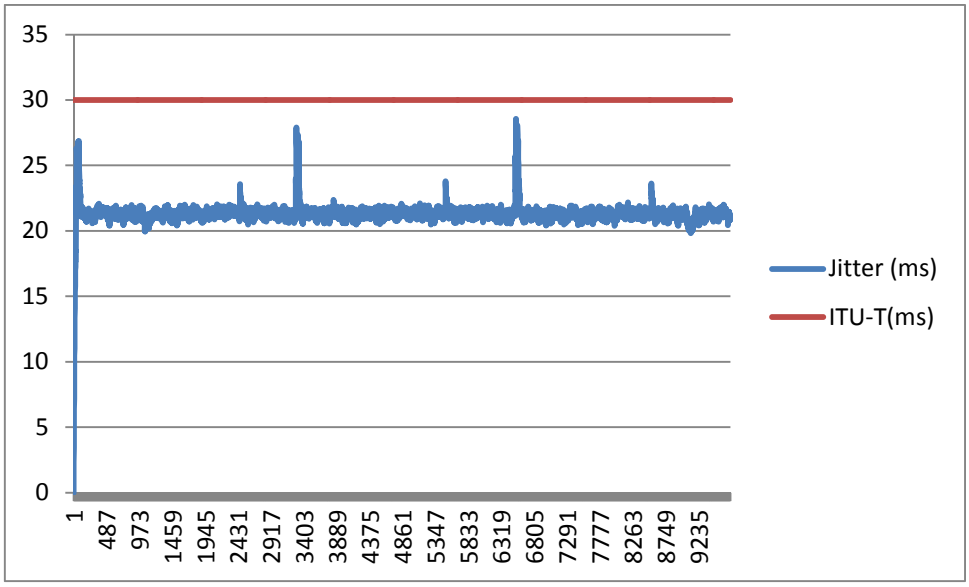

Figura 20: Gráfico do *Jitter* na primeira chamada.
Fonte: Autoria própria.

O segundo teste foi realizado no próximo andar abaixo, em outra sala. Também ocorreu sem picotes e com bom áudio. Os dados coletados foram: *Jitter* médio 21,30 ms, *Jitter* máximo de 30,99 ms, latência máxima entre um pacote e outro de 201,55 ms, latência media de 19,99 ms e zero pacotes perdidos. Pode-se observar, de acordo com as figuras 21 e 22, que houve mais valores de pico na latência e *Jitter*, alguns até ultrapassando o valor recomendado pela ITU-T.

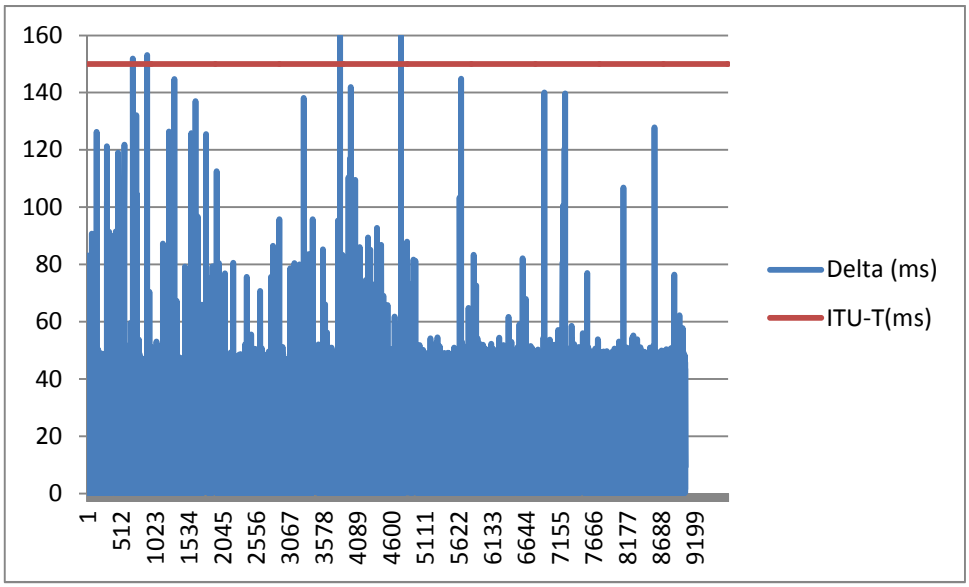

Figura 21: Gráfico da latência na segunda chamada.
Fonte: Autoria própria.

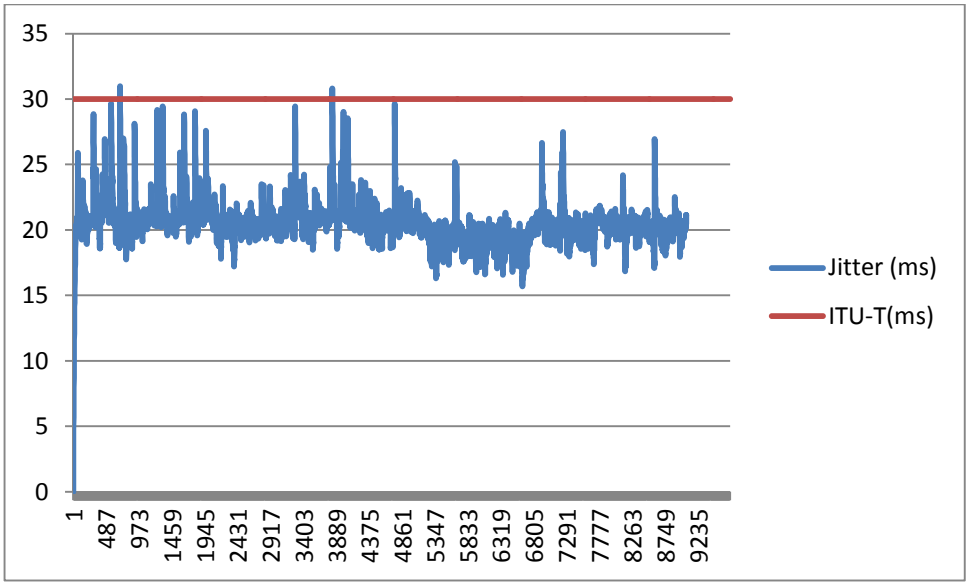

Figura 22: Gráfico do *Jitter* na segunda chamada.
Fonte: Autoria própria.

Já no terceiro teste, que foi realizado no segundo andar abaixo, o térreo, houve alguns picotes e o áudio ficou um pouco comprometido, com algum chiado. A distância entre os dispositivos e o AP não é muito grande, fica em torno de 12 metros em linha reta. Porém os obstáculos como paredes e outros objetos faz com que o sinal chegue aos dispositivos mais atenuado. Sendo assim, mais vulnerável a interferências de outros sinais externos. Os dados coletados foram: *Jitter* médio 23,92 ms, *Jitter* máximo de 564,16 ms, latência máxima entre um pacote e outro de 10787,42 ms, latência media de 25,8601 ms e 1 pacote perdido. De acordo com as figuras 23 e 24 pode-se observar que a chamada ficou boa parte do tempo com os parâmetros a cima dos níveis recomendados pela ITU-T.

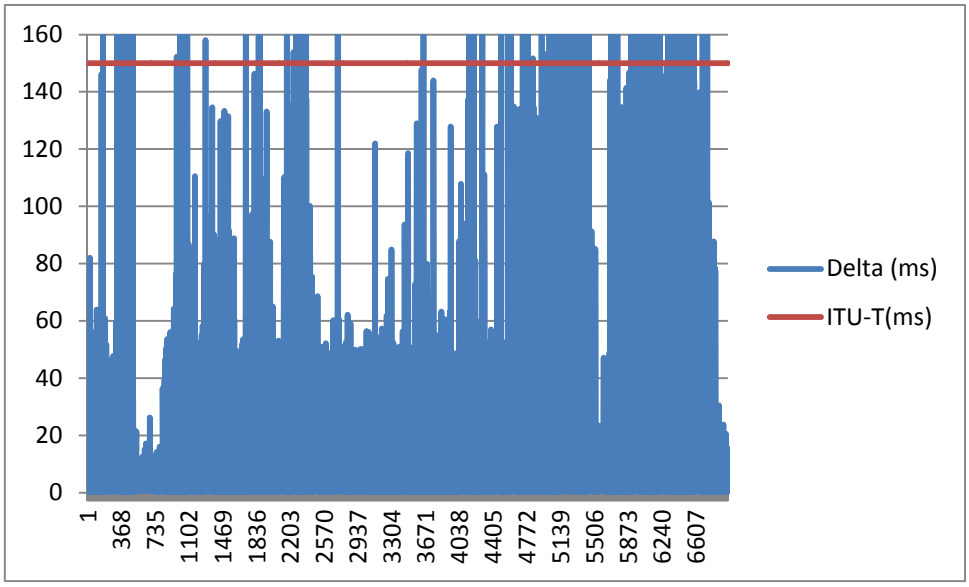

Figura 23: Gráfico da latência na terceira chamada.
Fonte: Autoria própria.

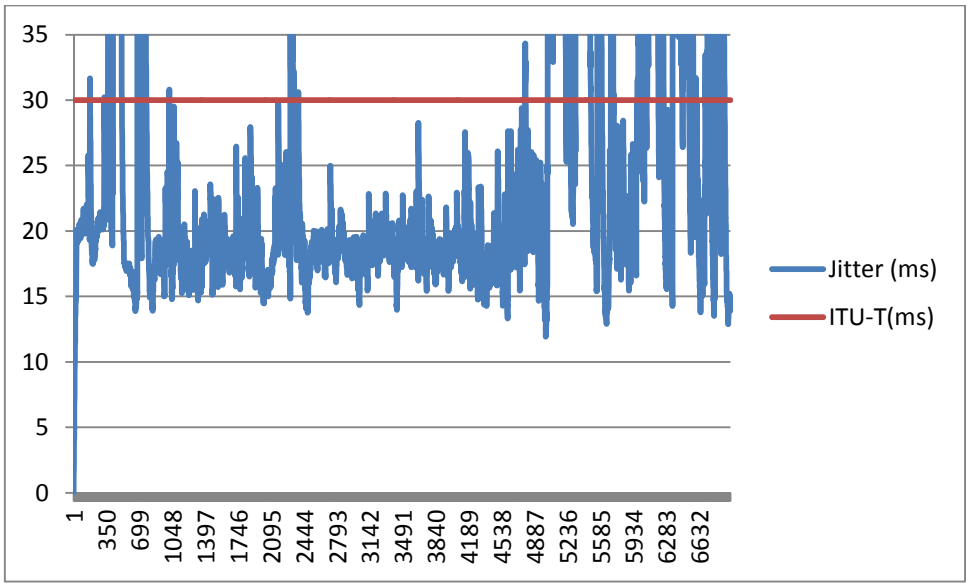

Figura 24: Gráfico do *Jitter* na terceira chamada.
Fonte: Autoria própria.

O quarto teste foi efetuado no mesmo ambiente da terceira, porém, alguns metros mais afastado. Esta ligação ficou com muitos picotes e chiado, tornado a comunicação impraticável e com duração da metade do tempo, pois a conexão VoIP caiu. Os dados coletados foram: *Jitter* médio 63,32 ms, *Jitter* máximo de 1708,50 ms, latência máxima entre um pacote e outro de 10265,35 ms, latência media de 49,40689 ms e 474 pacotes perdidos, equivalente a 12,94%. O ITU-T recomenda que a porcentagem de pacotes perdidos em uma chamada VoIP não ultrapasse 1%. De acordo com as figuras 25 e 26 pode-se observar que a chamada ficou boa parte

do tempo com os parâmetros à cima dos níveis recomendados pela ITU-T. Nota-se pelo eixo X dos gráficos que há menos amostras, pois a chamada durou aproximadamente metade do tempo das demais. Caso durasse o mesmo tempo, a chamada teria os parâmetros acima dos recomendados pela ITU-T na maior parte do tempo.

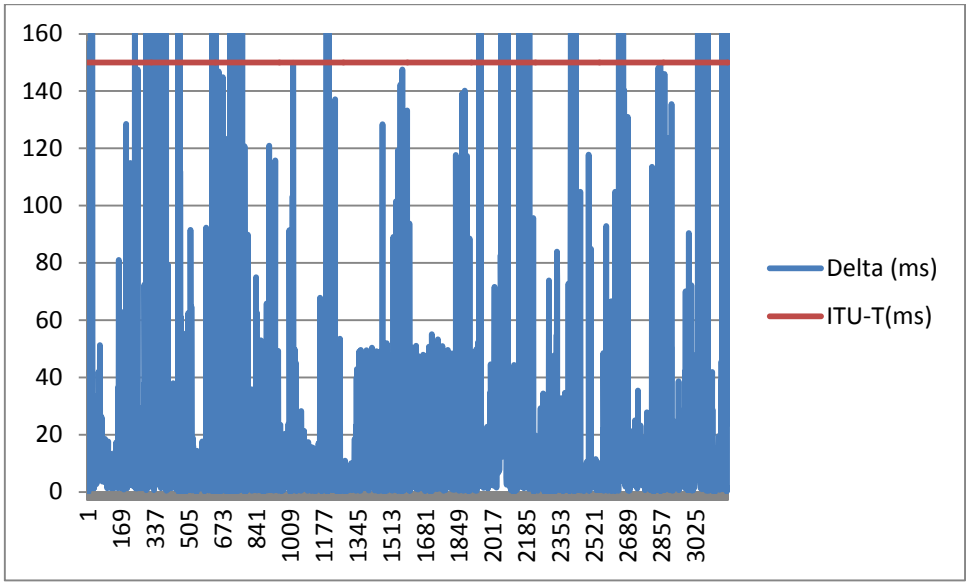

Figura 25: Gráfico da latência na quarta chamada.
Fonte: Autoria própria.

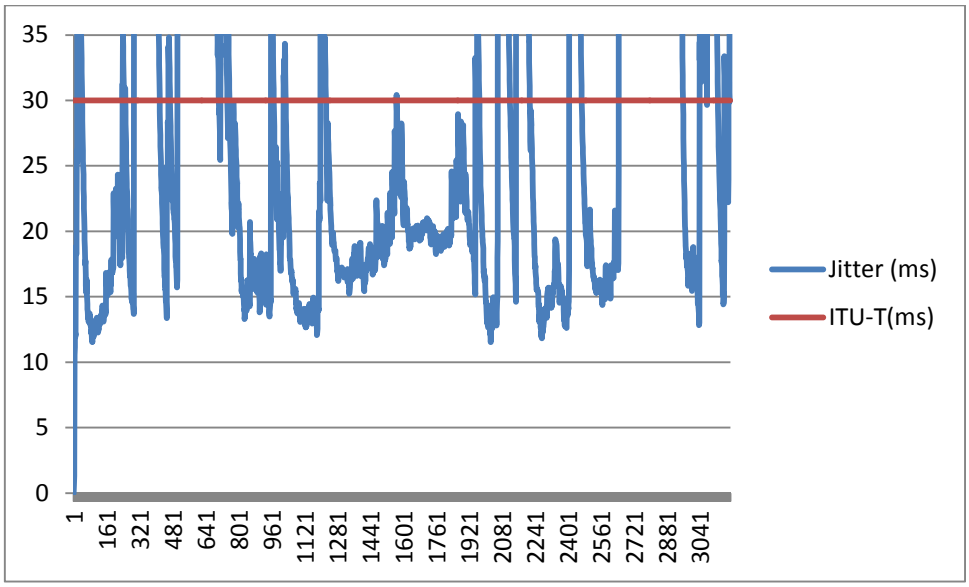

Figura 26: Gráfico do *Jitter* na quarta chamada.
Fonte: Autoria própria.

Por fim foi realizada um ultimo teste, agora, com tráfego inserido na rede, a fim de simular o efeito de uma chamada concorrente disputando o acesso ao meio. Paralelamente a ligação efetuada, foi injetado na rede um tráfego de 80 kbps (figura 27), que equivale a taxa de uma conexão VoIP. Não houve diferença significativa dos parâmetros coletados na primeira chamada, apenas outro dispositivo disputando o acesso ao meio não foi suficiente para afetar a qualidade da ligação. Fica como sugestão de trabalho futuro, a verificação do comportamento da qualidade de serviço com o aumento de chamadas através de outros dispositivos concorrendo o acesso ao meio.

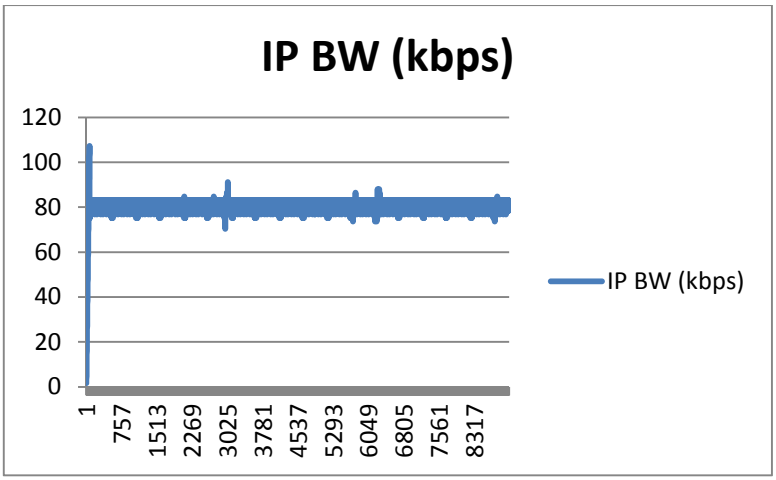

Figura 27: Gráfico da largura de banda ocupada pela chamada VoIP.
Fonte: Autoria própria.

O quadro 8 ilustra todos os dados coletados em cada uma das chamadas realizadas.

	1ª chamada	**2ª chamada**	**3ª chamada**	**4ª chamada**	**5ª chamada**
Jitter médio	20,48 ms	21,30 ms	23,92 ms	63,32 ms	20,35 ms
Jitter máximo	28,56 ms	30,99 ms	564,16 ms	1708,50 ms	27,86 ms
Latência média	19,98 ms	19,99 ms	25,86 ms	49,40 ms	19,78 ms
Latência máxima	134,18 ms	201,55 ms	10787,42 ms	10265,35 ms	132,58 ms
Pacotes Perdidos	0	0	1	474 (12,94%)	0

Quadro 8: Dados coletados.
Fonte: Autoria própria.

Comparando os resultados finais, nota-se que a latência e *Jitter* médio, não tiveram um aumento considerável entre as chamadas, porém, houve em vários momentos valores de pico durante os testes, quando distancia e obstáculos foram inseridos. Isso se deve ao fato de o sinal ficar mais vulnerável a interferências externas, pois chega ao destino cada vez mais atenuado. Não pela distancia em si, que apesar de ser aumentada em cada chamada, não chegou a valores expressivos para interferir na qualidade das ligações, e sim pela quantidade de obstáculos presentes em cada teste, como paredes e moveis.

Dentro do cenário montado, para que o desempenho das chamadas realizadas no térreo seja bom ou equivalente às realizadas nos andares mais próximos ao AP, seria necessária a adição de mais um ponto de acesso no andar intermediário, funcionando como um repetidor regenerando o sinal do primeiro AP.

5 CONSIDERAÇÕES FINAIS

Os conhecimentos teóricos obtidos nas disciplinas ao decorrer do curso, aliado aos materiais de apoio pesquisados, foram de grande importância para a análise e simulação da rede em estudo.

Com a realização dos experimentos envolvendo sistemas VoIP em redes sem fio, foi possível constatar a sua sensibilidade e o impacto causado por fatores internos e externos ao sistema. Como por exemplo, o fator distância e obstáculos físicos, que foi o foco do trabalho. Fica evidente que para a implantação de um sistema como esse, em uma escala maior, necessita-se de um planejamento e comissionamento adequados, caso contrário, o sistema pode não funcionar corretamente e comprometer toda a comunicação da rede.

O sistema VoIP sem fio se mostrou bastante flexível, fazendo com que seja possível instalar pontos telefônicos em locais com maior dificuldade de acesso, sem precisar alterar a infra estrutura local. Porém, a rede deve ser corretamente dimensionada e estudada para que não ocorram pontos onde as chamadas percam qualidade devido a interferências, obstáculos físicos e distâncias mais elevadas. Nessas situações verifica-se a importância de um *Site Survey* feito corretamente para que sejam detectados problemas de desempenhos na implantação da rede.

Durante o trabalho foi possível aprender o processo de instalação e configuração do servidor Asterisk, mesmo que de maneira simples, apenas para funcionamento básico, pois foi verificado que o PABX tem inúmeras funcionalidades que podem auxiliar a comunicação de uma empresa de diversas formas. Foi possível, também, averiguar a aplicação de *softwares* para monitoramento e medição de desempenho de rede. Ferramentas de fundamental importância para a operação e manutenção de uma rede.

REFERÊNCIAS

COMER, Douglas E. **Redes de computadores e internet**, 4ª edição, Porto Alegre: Bookman, 2007.

COUTO, Patrícia Aloise. "**TCC: Estudo da Qualidade de serviço de uma Aplicação VoIP em Ambientes Wireless com Handoff".** Natal: UFRN, 2010.

FILIPPETTI, Marco Aurélio. **CCNA 4.1 Guia Completo de Estudo**, 1ª edição, São Paulo: Editora Visual Books, 2008.

GONÇALVES, Flávio Eduardo de A. **Asterisk PBX Guia de configuração**. Disponível em: http://www.taioque.com.br/linux/Livro Asterisk Curso Completo.pdf. Acesso em: 23/10/2012.

ITU Telecommunication Standardization Sector. Disponível em: http://www.itu.int/en/ITU-T/Pages/default.aspx Acesso em : 20/10/2012

MOREAU, Richard. **Protocolo de gateway a Gateway.** Disponível em: http://www.imsaformet.com/protocolo-de-gateway-a-gateway.html. Acesso em: 23/10/2012

OLIVEIRA, Thiago Vinícios V. de**. Implementação Comunicação VOIP em Rede Sem Fio com Utilização de Telefones WLAN-VOIP**, 1ª edição, Rio de Janeiro: Editora Cência Moderna, 2012.PEDRÃO, Maudy T. Ekiga: o Skype livre. Disponível em: http://www.ubuntudicas.com.br/blog/2011/11/ekiga-o-skype-livre/. Acesso em: 19/09/2012

ARAÚJO, Thays Cristina Costa de. **“TCC: Avaliação do Impacto da Implementação de Protocolos Seguros em um Ambiente VoIP**”. Brasília: UnB, 2007.

ROESLER, Valter. **Redes de Computadores** – modelo OSI e TCP/IP. São Leopoldo: Universidade do Vale do Rio dos Sinos, 2004.

SOUZA, Lindeberg de. **Projetos e Implementação de redes: fundamentos, soluções, arquiteturas e planejamento**, 1ª edição, São Paulo: Érica, 2007.

TANENBAUM, Andrew S. **Redes de computadores**, 4ª edição, Rio de Janeiro: Editora Campus, 2003.