VoIP – Tecnologia de Voz sobre IP

Nilson José Ribeiro[1] , Luís Augusto Mattos Mendes[1]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil

Nilsinho_ribeiro@yahoo.com.br, luisaugustomendes@yahoo.com.br

Resumo: A tecnologia VoIP vem crescendo ao passar dos anos devido o grande uso da internet comunicação entre pessoas, seja para fins de negocio ou de interesse pessoal. Este artigo tem como objetivo explicar a tecnologia VoIP e dois fatores que influenciam diretamente no crescimento da tecnologia, que são a qualidade de serviço e a segurança.

Palavras-chave: VoIP, Qualidade de Serviço, Segurança, TCP/IP.

1 Introdução

Com a facilidade de acesso à *internet*, vem crescendo também diversas tecnologias que a utilizam como meio. Uma das tecnologias que está em destaque é a tecnologia VoIP, *Voice Over Internet Protocol,* com ela podemos nos comunicar via voz, como se fosse um sistema de telecomunicações tradicional, com qualquer pessoa em qualquer lugar do mundo com um custo bem mais acessível.

Neste artigo irei discutir o funcionamento da tecnologia, com os protocolos usados e em cima disso irei abordar um pouco sobre a arquitetura TCP/IP, a qual o VoIP utiliza pra transportar seu dados. Também vou abortar dois pontos de fundamental importância para que esta tecnologia tenha um crescimento ainda maior. A primeira é a qualidade de serviço oferecido, com técnicas para maior desempenho na rede, pois já que estamos falando de transmissão de voz e fundamental que esta transmissão seja bastante rápida e com o mínimo de perda de qualidade possível. A segunda será a seguraça, nesta parte vamos abordar as vulnerabilidades da tecnologia, mostrando técnicas de ataque que podem facilmente neutralizar as aplicações VoIP.

Na seção dois é apresentado o modelo TCP/IP com suas camadas e principais protocolos, na seção três conceitos sobre e VoIP e seus principais protocolos, na seção quatro técnicas de qualidade de serviço e na seção cinco segurança.

2 *Modelo TCP/IP*

Como citado anteriormente a telefonia sobre IP foi feita para funcionar em cima do modelo TCP/IP, com isso será apresentado as principais características e funcionalidades do modelo TCP/IP

"O Modelo de Referência TCP/IP, cujo nome vem de seus dois mais conhecidos protocolos TCP e IP, foi criado com o objetivo de ligar várias redes, pois houveram vários problemas quando surgiram redes de satélite e rádio que deveriam se comunicar com a ARPANET[1] "[1].

Tal modelo é composto por quatro camadas como podemos ver na Figura 1.

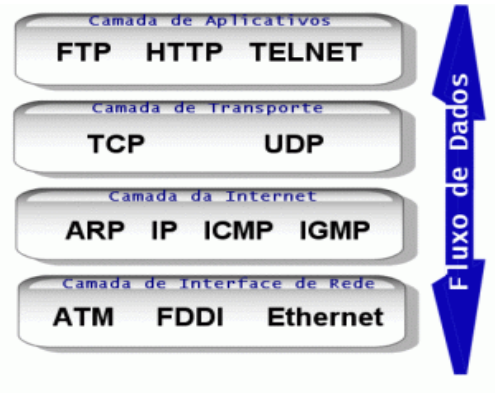

FIGURA 1 – Camadas TCP/IP[2]

2.1 *Camada de Aplicação*

A camada de aplicação contém os protocolos de alto nível como TELNET, FTP,HTTP, RTP, SMTP, SNMP e é responsável por fazer a comunicação entre os aplicativos e a camada de transporte. A comunicação com a camada de transporte é feita através da utilização de portas.

2.2 *Camada de transporte*

Está camada é responsável por receber os dados vindos da camada de aplicação e transformá-los em pacotes que posteriormente serão entregues à camada de Internet. Seu principal objetivo é oferecer um serviço confiável e eficiente a seus usuários. Dois protocolos operam nesta camada, são eles: TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol). O primeiro é um protocolo bastante confiável que permite a entrega dos pacotes de dados sem erro. Já o UDP é um protocolo menos confiável, porém é amplamente utilizando quando a entrega imediata dos dados é mais importante que sua entrega precisa.

È nesta camada que esta uma função importante para o trabalho proposto que é a qualidade de serviço e a checagem de erros fim-a-fim.

---

[1] ARPANET – *Advanced Research Projects Agency* e uma rede desenvolvida pelo Departamento de Defesa dos Estados Unidos durante a década de 70, a ARPANET foi criada para resistir a ataques nucleares com o objetivo de investigar a utilidade da comunicação de dados em alta velocidade para fins militares. Essa rede foi colocada fora de operação em 1990.

2.3 Camada Internet

A finalidade da camada de Internet é enviar pacotes da origem de qualquer rede e fazê-los chegar ao destino, independentemente do caminho e das redes que tomem para chegar lá. O protocolo específico que governa essa camada é chamado *Internet Protocol* (IP). A determinação do melhor caminho e a comutação de pacotes acontece nessa camada.

2.4 Camada de Host/Rede

É a camada responsável pela transmissão dos pacotes recebidos da camada Internet na rede física. Está camada relaciona tudo aquilo que um pacote IP necessita para realmente estabelecer um *link* físico. Isso inclui detalhes de tecnologia e detalhes encontrados nas camadas física e de enlace do modelo OSI.

2.5 Protocolo IP

O protocolo IP foi projetado visando conseguir transportar dados entre os mais diferentes tipos de redes. Sua tarefa é fornecer a melhor forma de transportar pacotes de dados da origem para o destino, independente das redes onde ambos estejam. Outra característica do IP é que se trata de um protocolo não orientado à conexão e também não é responsável por verificar se um pacote que foi enviado chegou ou não ao seu destino, ficando esta função a cargo do protocolo de transporte. O protocolo IP, sofreu algumas mudanças e foi evoluindo de acordo com o tempo. Tendo com isso várias versões, entre as quais a versão quatro, também conhecida como IPv4, e a versão seis, chamada de IPv6. Durante um bom tempo os recursos do IPv4 foram utilizados de forma satisfatória. Porém, com o inúmero crescimento de equipamentos que deveriam se conectar a Internet, surgiu um problema. O número de endereços IP logo estaria esgotado, não suportando a demanda. Com esse problema começou-se a trabalhar em uma nova versão do IP. Os principais objetivos da nova versão do IP eram:

- Possuir um número maior de endereços IP;
- Reduzir o esforço necessário para o roteamento dos pacotes IP;
- Diminuir o tamanho das tabelas de roteamento;
- Oferecer uma segurança maior em relação ao IPv4;
- Aumentar a importância da informação sobre o tipo de serviço, principalmente para os serviços de tempo real;
- Possibilitar a evolução do protocolo;
- Possibilitar a compatibilidade entre a nova versão e o IPv4.

2.6 TCP X UDP

O TCP, *Transmission Control Protocol*, trata-se de um protocolo orientado à conexão e projetado especialmente para manter a transmissão dos dados. É atualmente o protocolo mais utilizado na Internet para a transmissão de arquivos. O TCP também é responsável pelo controle de erro fim-a-fim e de fluxo, que são ligados à qualidade de serviço

O UDP, *User Datragram Protocol*, trata-se de um protocolo que não é orientado à conexão. Ele oferece uma maneira das aplicações enviarem pacotes IP brutos encapsulados sem precisar realizar uma conexão. Porém não garante a entrega dos pacotes em sua origem, ele também é ideal para aplicações em tempo-real que desejam transmitir áudio e vídeo. Como tais aplicações são sensíveis ao atraso, não faz sentido preocupar-se com a correção dos pacotes, pois tempo será gasto nessa correção, gerando assim um atraso na entrega dos pacotes. O importante para essas aplicações é o pacote chegar o mais rápido possível. Como as aplicações de voz em tempo-real são sensíveis ao atraso, torna-se claro então que o protocolo UDP é o ideal para aplicações de voz sobre IP (VoIP)

Ambos os protocolos estão situados na camada de transporte do modelo TCP/IP. Onde o TCP, por ser orientado à conexão, apresenta uma maior confiabilidade na entrega dos dados. Já o UDP é mais simples e permite que os dados sejam transmitidos com uma maior velocidade, porém sacrificando a confiabilidade.

3 VoIP

Para entender a tecnologia VoIP achei interessante conhecer um pouco da história podendo assim saber de seu surgimento e de suas evoluções.

A tecnologia VoIP surgiu em 1994 com Alan Cohen e Lior Haramaty fundando a Vocaltec, em 1995 a empresa laçou o *Internet Phone* que viria a ser o primeiro software de VoIP, claro que ele não oferecia toda a qualidade de transmissão que, por exemplo, o *Skype*[2], oferece hoje mas isso se limita basicamente por causa da largura de banda[3] que era oferecida, mas aparti deste ponto abriu-se as portas para está tecnologia que vem crescendo bastante atualmente.

VoIP é simplesmente a transmissão de tráfego de voz, que é comprimida e convertida em pacote de dados, via redes de computadores. Toda a tecnologia foi construída em cima do modelo TCP/IP de forma que para o seu uso independam do meio físico. Com essa tecnologia em mãos surgiram diversos softwares, hardwares e protocolos que possibilitam essa comunicação[3].

3.1 Protocolos VoIP

Existem protocolos na camada de aplicação que se propõe a melhorar a entrega de dados que devem ser transmitidos pelos aplicativos em tempo real. Como uma conversação telefônica acontece em tempo-real faz-se necessário à utilização de protocolos especiais que auxiliam o processo de transmissão da voz. Pode-se citar entre esses protocolos o SIP, SDP, RTP MGCP e o H.248. As subseções seguintes tratam da discussão desses protocolos.[4]

---

[2] Skype é um software que permite comunicação grátis pela internet através de conexões sobre VoIP.

[3] Largura de banda - É a quantidade de dados possível de transmissão em um circuito em um determinado tempo. Para conexões digitais, a largura de banda é usualmente expressa em bits por segundo (bps).

3.1.1 *SIP* (*Session Iniciation Protocol*),

O SIP foi criado em 1999 com o objetivo de possibilitar o tráfego de voz sobre IP, dentre suas principais funcionalidades tem-se a localização de usuários, o estabelecimento, modificação e término de chamadas. O protocolo é baseado em texto e se assemelha com o HTTP, sua arquitetura é baseada no modelo cliente-servidor onde os clientes iniciam uma chamada e o servidor as responde. Com o fato do SIP tratar-se de um protocolo cliente servidor uma chamada pode envolver diversos servidores e clientes, como é ilustrado na Figura 2.

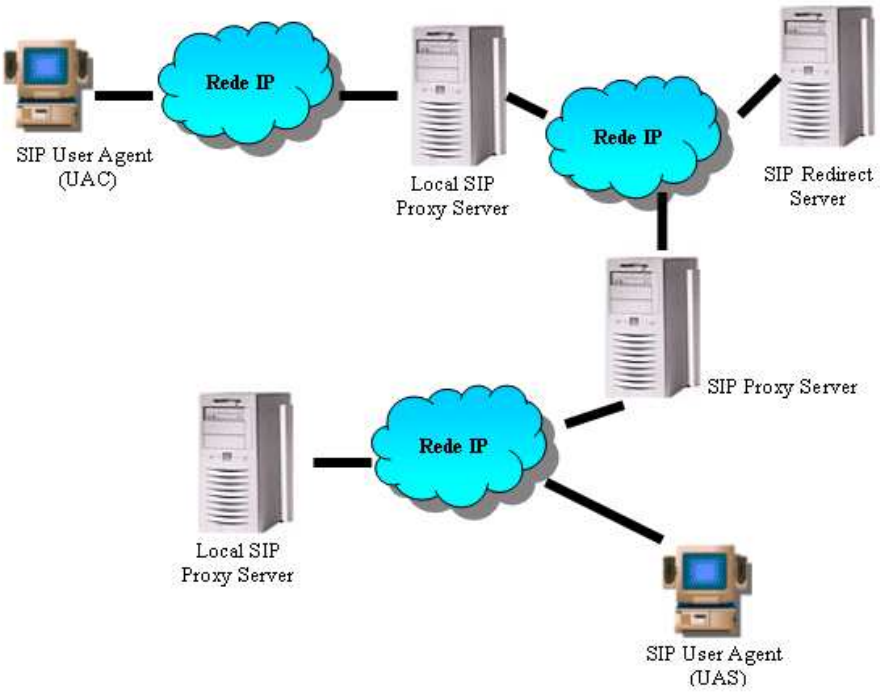

FIGURA 2 – Funcionamento do SIP[5]

A arquitetura SIP pode ser descrita com dois elementos:

- *SIP User agents*: qualquer aplicação cliente ou dispositivo que inicia uma conexão SIP. Composto de UAC (*user agent client)* e de um UAS (*user agent Server*). UAC é responsável por iniciar as chamadas enviando requisições, e o UAS é responsável por responder às chamadas, enviando respostas
- *SIP Proxy Serve*: servidor de redirecionamento de requisições e respostas. O servidor passa a realizar a sinalização como se fosse o originador da chamada, e quando a resposta lhes é enviada, ela é redirecionada para o originador real.

3.1.2 *SDP* (*Session Description Protocol*)

O SDP é utilizado para descrição de uma sessão multimídia (inicialização, convite, anúncio). Ele não tem mecanismo de transporte próprio, mas é adaptado para utilizar o de outros protocolos como o SIP.

3.1.3 RTP (*Real-time Transfer Protocol*)

O Protocolo de Transporte em Tempo Real provê o transporte fim-a-fim de aplicações, transmitido em tempo real dados como áudio, vídeo ou ambos simultaneamente. Ele suporta transferência de dados para múltiplos destinos, usando distribuição *multicast*[4] ou *unicast*[5] e também possui habilidades como: reconstrução de sincronismo, detecção de perda de datagramas, segurança, entre outras, porém o RTP não realiza reserva de recursos e não garante qualidade de serviço para serviços de Tempo real. O transporte desse tipo de dados é complementado pelo protocolo de controle RTCP.

3.1.4 RTCP (*Real-time Transfer Control Protocol*)

O Protocolo de controle de Transporte em Tempo Real é um protocolo que pode ser usado juntamente com o RTP, porém o RTP e RTCP são distintos um do outro pelo uso de diferentes números de portas. Trata-se de um protocolo opcional cuja principal função é transmitir periodicamente pacotes de controle, contendo informações estatísticas, para os participantes de uma conversação com o objetivo de monitorar a qualidade de serviço e transportar informações úteis de tais participantes. Trata-se de um protocolo bastante utilizado em aplicações de vídeo-conferência. Embora as informações retornadas pelo RTCP não informem onde determinado problema está ocorrendo, elas podem servir como ferramenta para localizar o problema. Pois as informações podem ser geradas por diferentes *gateways*[6] em uma rede. Isso ajuda a delimitar a área da rede em que o problema pode estar ocorrendo.

3.1.5 MGCP (*Media Gateway Control Protocol*)

O MGCP é relativamente novo, ele é utilizado para controlar gateways de telefonia a partir de um elemento de controle externo de chamadas de modo centralizado, chamado Controle de gateway ou agente de chamadas. O MCGP é na essência um protocolo mestre/escravo onde se espera que os gateways executem comandos mandados pelo agente de chamadas.

Uma conexão MGCP possui dois tipos básicos de dispositivos lógicos: os *endpoints* e conexões. O primeiro são interfaces físicas ou lógicas que inicializam ou terminam uma conexão VoIP, são comumente portas em um roteador e atuam como gateway ou como portas em um sistema PBX. O segundo são fluxos lógicos e temporários que tem como objetivo estabelecer, manter e terminar uma chamada VoIP. Uma vez terminada a chamada, a conexão é desfeita e os recursos alocados são liberados para serem reusados em uma nova conexão.

3.1.6 MeGaCo/H.248

[4] MULTICAST é a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções.

[5] UNICAST é um endereçamento para um pacote feito a um único destino, ou seja, em comparação com o multicast, a entrega no *unicast* é simples, ponto-a-ponto.

[6] Gateways,são dispositivos que estabelecem a conexão em redes diferentes fazem a conversão necessária, tanto em termos de hardware quanto de software.

MeGaCo/H.248 é a evolução do padrão MGCP. Ele é semelhante ao MGCP em muitas formas oferecendo várias melhorias e funcionalidades que o MGCP não oferece. O MeGaCo/H.248 propõe uma série de modificações, uma das melhores alterações é a que separa fisicamente o plano de controle, do plano de conexão. O plano de controle é responsável por trocar as sinalizações e mensagens com as outras redes e protocolos, converter as mensagens para os comandos do MeGaCo/H.248 e encaminhar na rede IP para o plano de conexão, controla também a existência das entidades lógicas no plano de conexão.

4 Qualidade de Serviço

Os atuais avanços tecnológicos na área de redes de computadores têm propiciado um aumento das taxas de transmissão, tornando possível discuti-se mais sobre qualidade de serviço, por isso a expressão qualidade de serviço (QoS) tem varias interpretações e definições, mas há um consenso que QoS é como o conjunto de características de um sistema necessário para atingir uma determinada funcionalidade. Assim a qualidade de serviço deve ser fim-a-fim, o tráfego tem que ser tratado na rede local de origem, nas conexões de longa distância e roteadores intermediários, finalmente, na rede local destino. *QoS* é fundamental para diversos tipos de aplicações, sobretudo as multimídias, pois é desejável que haja um sincronismo entre as diversas mídias. Por exemplo, numa videoconferência o som deve estar sincronizado com a imagem, ou seja, deve haver sincronia entre as palavras e os movimentos dos lábios das pessoas. Como pode ser visto no exemplo anterior, as definições de *QoS* tem um aspecto subjetivo, podendo variar de aplicação para aplicação. Dentre estes aspectos existem parâmetros que devem ser controlados visando a obtenção da qualidade de serviço, mas estes não são localizados num único equipamento ou componente da rede, estando assim encontrado desde o inicio da rede no *host* de origem até o *host* de destino.

4.1 Parâmetros para a QoS

Como foi citado anteriormente é necessário o controle de alguns parâmetros para a utilização do QoS. Os principais parâmetros são:[6]

- Vazão
- Latência ou Atraso
- Jitter

4.1.1 Vazão

A vazão é na sua essência, a taxa de transferência de dados entre dois nós da rede. Está taxa é diretamente influenciado pela largura da banda e pela quantidade de fluxos compartilhado. A vazão é o parâmetro básico para a utilização de QoS.

4.1.2 Latência ou Atraso

Este parâmetro é de fundamental importância para a qualidade de serviço em definição é dado pelo tempo gasto para os dados trafegarem da origem até o destino. Aplicações como vídeo e áudio apresentam tempo de latência alto. A latência é também designada como atraso.

Alguns dos principais fatores que influenciam na latência de uma rede são:

- atraso de propagação
- velocidade de transmissão
- processamento nos equipamentos.

4.1.3 Jitter

O jitter é um parâmetro bastante usado em aplicações de tempo real, pois ele trata que as informações sejam processadas em um tempo definido. Este parâmetro é a variação no atraso fim-a-fim, ou seja, ele trata a variação da latência. Alguns fatores que podem causar estas variações são:

· tempos de processamento diferentes nos equipamentos intermediários (roteadores, *switches*, etc.);

· tempos de retenção diferentes impostos pelas redes públicas (*Frame Relay*, ATM, X.25, IP) e outros fatores ligados à operação da rede.

4.2 Técnicas de controle de fluxo ou congestionamento

Congestionamento ocorre quando o número de pacotes que estão sendo transmitidos aproxima-se da capacidade máxima.

O controle de congestionamento é feito através de técnicas de enfileiramento de dados com a intenção de minimizar os congestionamentos de dados. Este controle é realizado de forma a garantir que a rede seja capaz de transportar o tráfego oferecido.[6]

4.2.1 FIFO – FIRST IN FIRST OUT

O FIFO é bastante usado em conexões seriais, a técnica do *first in first out* é baseado no armazenamento dos pacotes, estes pacotes são armazenados pela ordem que chegam, ou seja, o primeiro a chegar é o primeiro a sair. Por não ter um tratamento mais rígido dos pacotes de dados ele não serve para a utilização de aplicações sensíveis ao tempo.

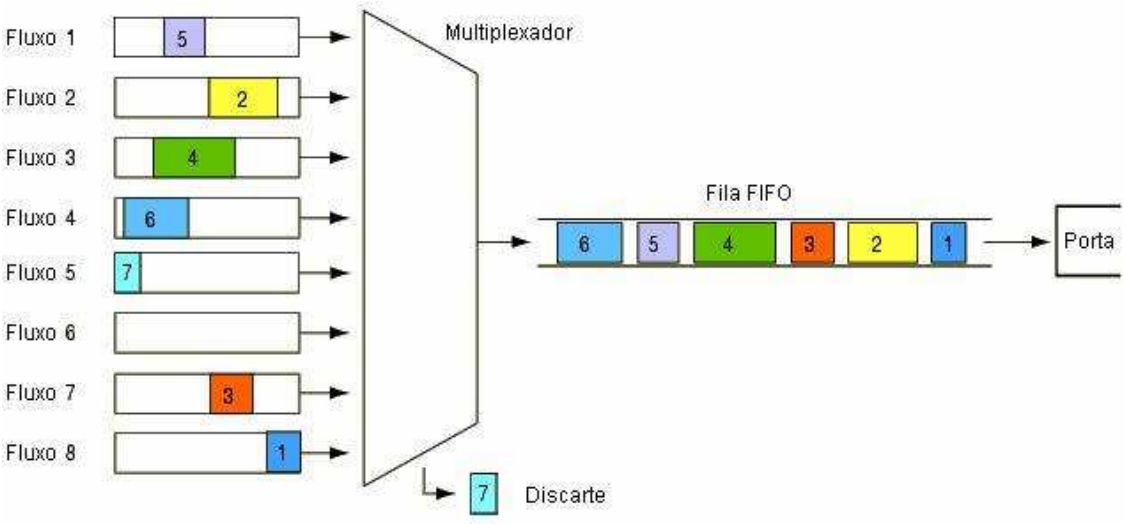

FIGURA 3 – Funcionamento FIFO[7]

4.2.2 FQ - Enfileiramento F*air Queueing*

No *Fair Queueing*, ou enfileiramento justo, as mensagens são organizadas por sessões, para cada sessão e reservado um canal. A ordem na fila é feita através do ultimo bit, com isso a alocação fica mais justa. Quando uma sessão estiver cheia, os próximos pacotes são descartados, independentes das demais sessões

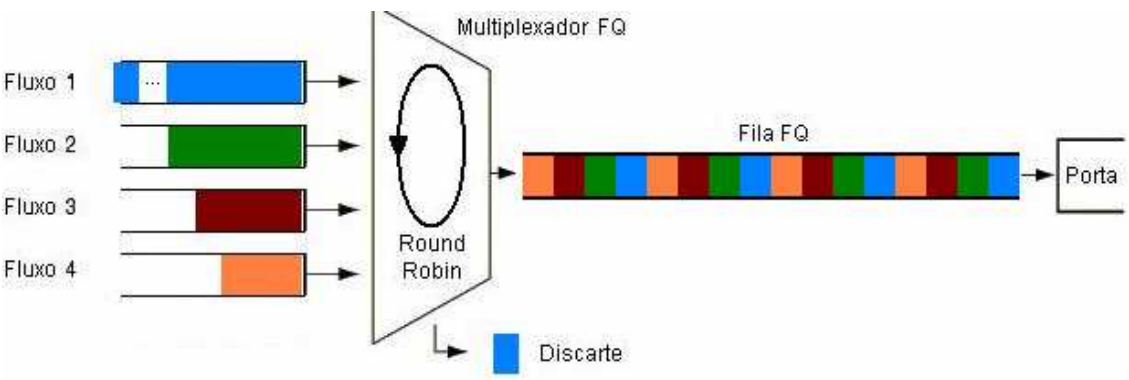

FIGURA 4 – Funcionamento FQ[8]

4.2.3 PQ - Enfileiramento *Priority Queueing*

No enfileiramento prioritário os pacotes de dados são classificados em quatro níveis de prioridade, sendo eles alta, média, normal e baixa.

Os pacotes classificados como prioritário tem total preferência. Por isso este método é bastante perigoso podendo aumentar bastante o jitter nas aplicações de menor prioridade se os de maiores prioridades tomarem toda a banda.

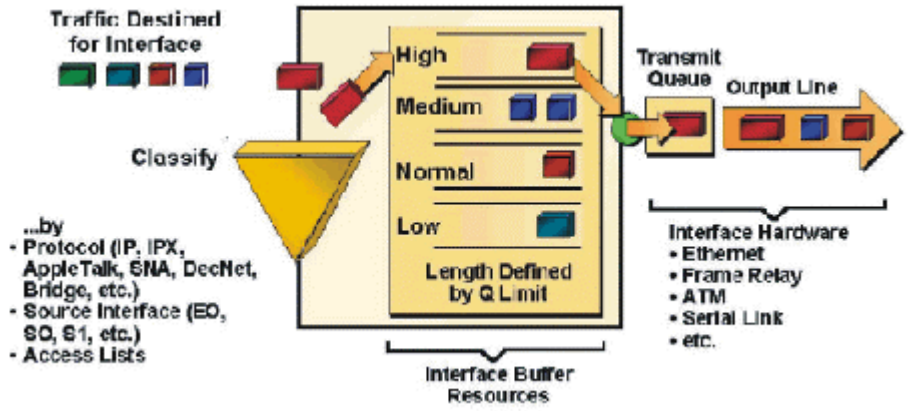

FIGURA 5 – Funcionamento PQ[8]

4.2.4 CQ - Enfileiramento *Custom Queueing*

Este algoritmo permite especificar uma porcentagem da banda para um aplicação e deixando o restante da banda para compartilhado com as demais aplicações. O *custom queueing* funciona semelhante ao *fair queueing*

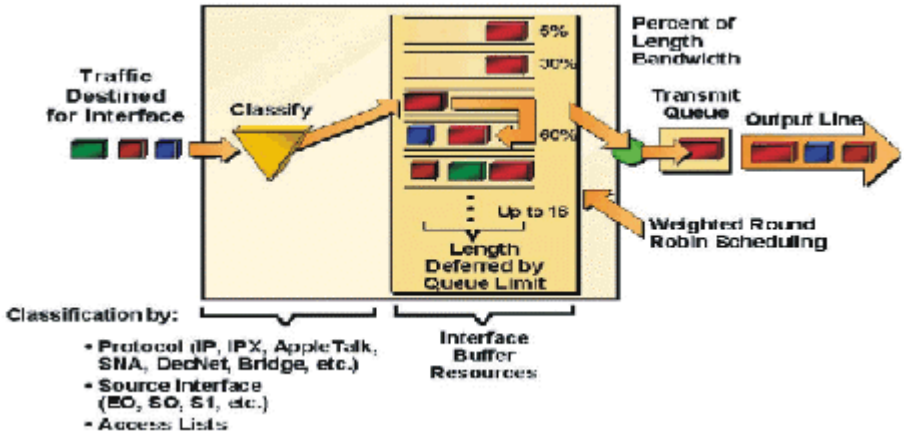

FIGURA 5 – Funcionamento CQ[8]

4.3 Alternativas técnicas de QoS

Existem varias técnicas para se obter um bom resultada de QoS, que são as seguintes: [11]

- IntServ
- DiffServ
- MPLS

4.3.1 IntServ

O IntServ também conhecido com serviço integrado, foi desenvolvido para estabelecer QoS em comunicações fim-a-fim, esta técnica tenta garantir a qualidade que foi estabelecida na configuração original. Mas o que ocorre é que diversas conexões virtuais são estabelecidas entre cada roteador que a conexão utiliza. Logo para estabelecer uma conexão IntServ, a

aplicação do usuário de origem terá que verificar se o roteador tem recursos que a aplicação necessita, e este processo deverá ser feito pelos roteadores até chegar ao usuário destino. Se todos tiverem recurso disponíveis para oferecer será realizada a conexão. Para isso é necessário que IntServ verifique dois aspectos essenciais:

- Como as solicitações feitas pelas aplicações
- Como os elementos da rede devem garantir reservas de recursos para garantir a qualidade de serviço

Mesmo sendo uma idéia interessante, o IntServ não é funcional pois é pouco provável que todos os roteadores tenham os requisitos de conexão exigida pela aplicação.

4.3.2 DiffServ

A técnica do DiffServ ou Serviços Diferenciados é bastante usada para conexões com grande volume de dados, nesta técnica duas entidades principais são definidas: o roteador de borda e o roteador de núcleo, em ambas entidades há fila distinta para cada classe. O roteador de borda tem a responsabilidade de policiar e atribuir uma classe agregada para os pacotes transmitidos. Já o toteador de núcleo não diferencia fluxos individuais e manipula os pacotes de acordo com as classe estabelecida pelos roteadores de borda.

4.3.3 MPLS – Multiprotocol Label Switching

O MPLS inicialmente foi desenvolvido pela Cisco Systems, com o nome de *tag switching*. A idéia principal do projeto era acelerar o encaminhamento dos pacotes com especificações pré-definidas. Ao conectarem-se em uma rede MPLS, os pacotes recebem uma identificação que permite que os roteadores MPLS associem o pacote a uma rota já pré-definida. Apesar de ter sido desenvolvido visando redes com camada IP e de enlace ATM, o mecanismo de encaminhamento dos pacotes no MPLS pode ser utilizado para quaisquer outras combinações de protocolos de rede e de enlace, o que explica o nome de *Multiprotocol Label Switching*.

O *Multiprotocol Label Swuitching* é uma solução voltada para a área de engenharia de trafego de pacotes que garante um QoS bastante eficaz, pois tem uma simplificação na função de roteamento nos roteadores diminuindo assim a sua latência.

5 Segurança

Tratando-se de tecnologias que envolvem transferência de dados pela *internet* tem-se que dar uma atenção para a área de segurança, pois estas estão propensas a quebra de sigilo. Logo que a tecnologia VoIP tem a *internet* como seu meio de transferência é impossível garantir uma total segurança sobre o fluxo de dados, incluindo ligações telefônicas. À medida que novas tecnologias, como o VoIP, surgem também novos protocolos de segurança. De forma geral, todos os sistemas VoIP já estão preparados para criptografia, pois pela própria forma de transmissão por pacotes IP tem-se uma facilidade de transformar estes pacotes de

dados em pacote de dados codificado.Como o VoIP torna-se popular, a segurança continua a ser apontada como uma chave para o avanço desta tecnologia.[9]

5.1 Técnicas de Ameaça à Tecnologia

Nesta seção será discutido as técnicas de ameaça a tecnologia VoIP, com a varredura de rede bastante usada por *hackers* para capturar informações e a de ataque à dispositivos, usada para impossibilitar que uma comunicação seja feita.

5.1.1 Varredura de Rede

Esta categoria de ataque visa a captura de comunicações VoIP. Os ataques mais comuns nesta categoria são:

- Varredura ICMP ping
- Varredura TCP ping

5.1.1.1 Varredura ICMP ping

Para começarmos a entender está técnica é importante sabermos o que é o protocolo ICMP, bem o protocolo citado é um protocolo integrante do protocolo IP, o *Internet Control Message Protocol* é utilizado para enviar relatorios de erros, a maioria dos computadores que utiliza o protocolo IP aceita as mensagens ICMP. Do ponto de vista de especialistas em segurança, a liberação sem nenhum critério do tráfego de mensagens ICMP é considerada como uma ameaça para a segurança. Agora que entendemos como funciona o protocolo ICMP vamos para a técnica de varredura.

Esta técnica identificar quais *hosts* que estão ativos na rede, através de diversas ferramentas como o FPING, NMAP, SUPERSCAN. Através desta ferramenta é possível disparar solicitações ICMP para múltiplos host, elas também podem identificar o *Ethernet Media Access Control* (MAC) o que nos diz qual o fabricante associado a cada dispositivo. Dessa forma já fazemos uma identificação prévia dos dispositivos VoIP.

Com isso entramos em um dilema, pois os pacotes ICMP são bastante importantes para o tratamento de problemas em redes, seja para medidas de desempenho ou de diagnóstico dos dispositivos da rede. Entre tanto torna a rede vulnerável a ataques teste tipo, uma solução seria bloquear os dispositivos VoIP para pacotes ICMP.

5.1.1.2 Varredura TCP Ping

Como nos avanços de segurança o método te ataque também evolui rapidamente, com o mesmo objetivo da varredura da técnica anterior o TCP *Ping Scans*. Esta técnica utiliza-se do envio de pacotes TCP, para portas que comumente são utilizadas, após o envio de pacote TCP, o atacante receberá outro pacote TCP informado se o aplicativo esta rodando ou não. O envio de pacotes TCP é mais eficaz quando existe algum *firewall* que monitore as

conexões e que bloqueie alguns tipos de pacotes a estabelecerem uma nova conexão. Alguns dispositivos inteligentes de segurança de redes como sistemas de prevenção de invasão podem ajudar a detectar e bloquear *TCP ping*. Outros dispositivos podem identificar certo volume desse tipo de pacote, e podem colocar o host em uma lista negra.

5.1.2 Ataques contra Disponibilidade da rede

Esta categoria de ataque visa o travamento dos dispositivos da ou do sistema operacional. Os ataques mais comuns nesta categoria são:

- Fragmentação de Pacotes
- *QoS Modification Attck*

5.1.2.1 Fragmentação de Pacotes

Com a utilização de fragmentação de pacotes é possível deixar dispositivos VoIP inutilizados, pois com esta fragmentação o aumento de consumo de recursos ficam alem do suportado. Existem diversas formas de fragmentar pacotes, só que a mais usada e através de exploits, que são aplicações responsáveis por fragmentar os pacotes

5.1.2.2 QoS Modification Attck

QoS Modification Attck consiste em modificar campos do cabeçalho de protocolos de forma a causar degradação dos serviços. Com esta modificação o *switch* irá interpretá-los com sendo pacotes de voz , assim eles terão as mesmas prioridades dos pacotes utilizados pela aplicação VoIP. Dependendo do volume de pacotes modificados, aplicação travará pois não haverá recursos para suportar.

6 Considerações Finais

Com este artigo mostra-se um apanhado geral da tecnologia VoIP e explicando o seu funcionamento. Após esta introdução na tecnologia foram descritas as especificações do TCP/IP, onde o VoIP utiliza-se para transmitir os dados, com suas camadas e propriedades. Foram citadas também os principais protocolos utilizados pelo VoIP como o SIP, RTP, H248 e outros.

Mostrou algumas técnicas de inibição de congestionamento, entretanto não foram citas todas, pois a maioria é similar ou derivada das apresentadas neste artigo e mostramos como que com estas alternativas técnicas apresentadas possibilitam um melhor gerenciamento do tráfego dos dados fornecendo uma qualidade de serviço desejada para cada aplicação específica.

Também cita-se as principais ameaças a Tecnologia VoIP, mostrando suas vulnerabilidades e algumas ferramentas que possibilitam fazer estes ataques.

Após o estudo deste artigo podemos considerar que, por exemplo, os benefícios que esta tecnologia nos oferece como: a redução de custo crê que esta seja a principal e mais marcante característica da tecnologia, a simplificação, pois reuni em uma mesma infra-estrutura várias formas de comunicação e com isso tornando o meio de transmissão unificado.E algumas desvantagens que são principalmente a grande preocupação que se teve ter com a qualidade de serviço e que esta tecnologia ai se encontra bastante vulneráveis a diversos tipos de ataques.

6. Bibliografia

[1] TANENBAUM, Andrew S. **Redes de Computadores.** Tradução por Insight Serviços de Informática. 3. Ed. Rio de Janeiro: Campus, 1997. Tradução de: Computer Networks.

[2] Desconhecido, Tudo sobre TCP/IP,Baboo. Mensagem disponível em: http://www.baboo.com.br/absolutenm/templates/content.asp?articleid=4522&zoneid=24&resumo= . Acesso em 17 maio 2008.

[3] Bernal, Paulo Sergio Milano. **Voz Sobre Protocolo IP : a Nova Realidade da Telefonia**. Ed Érica, 2007

[4]DOMINGUES, Miriam Lúcia Campos Serra. **Protocolos de Dados para Conferências Multimídia**. 2000. Dissertação de Mestrado (Ciências da Computação) – Universidade Federal do Rio Grande do Sul, Porto Alegre.

[5] Desconhecido,Tutorial Banda larga VoIP. Disponível em: http://www.teleco.com.br/tutoriais/tutorialtelip2/pagina_3.asp. Acesso em 20 maio 2008.

[6] SILVA, Dinailton José da. **Análise de Qualidade de Serviço em Redes**. 2004. (Dissertação de Mestrado em Ciência da Computação) – Universidade Estadual de Campinas.

[7] Desconhecido, Técnicas de controle de fluxos. Disponível em: http://www-ceb.bo.infn.it/docum/nt970id/fifo_ceb.html. Acesso em 10 abril 2008

[8] Desconhecido, Qualidade de serviço em VoIP. Disponível em: http://www.cliconnect.com/br/Artigos/QualidadeServico01.html

[9] Endler,Collier. **Hacking Exposed VoIP: Voice over IP Security Secrets and Solutions**. New York, McGraw-Hill, 2006

SANTOS, Rafael Moraes. Telefonia IP: Estudo dos Porocolos SIP e H.323. CEFET Centro Federal de Educação Tecnológica de Goiás, 2006

COMER, D. E. **Internetworking with TCP/IP: Volume I – Principles, Protocols and Architecture**, 4ª edição, Prentice-Hall, 2000, Upper Saddle River, NJ.

JESZENSKY, Paul Jean Etienne. **Sistemas Telefônicos**. São Paulo, Manole, 2004.