UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

HUGO LEONARDO CROCETTI

O IMPACTO DO *QOS* NAS COMUNICAÇÕES *VOIP*

MONOGRAFIA

CURITIBA
2012

HUGO LEONARDO CROCETTI

O IMPACTO DO *QOS* NAS COMUNICAÇÕES *VOIP*

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Me. Fabiano Scriptore de Carvalho

CURITIBA

2012

AGRADECIMENTOS

Agradeço primeiramente a toda minha família, minha namorada Adriane e aos amigos que me apoiaram neste aprendizado.

Ao meu orientador Prof. Fabiano Scriptore de Carvalho que esteve comigo por estes longos três meses de batalha e cedeu o laboratório para que fosse possível desenvolver este trabalho.

Aos meus colegas de sala.

RESUMO

CROCETTI, Hugo Leonardo. **O impacto do *QoS* nas comunicações *Voip***. 2012. 70 folhas. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Este trabalho teve como tema principal a análise e verificação de tráfego de dados e topologias com implementação de políticas de *QoS. Foram realizados* testes de estresse para comparar o impacto entre topologias, com e sem políticas de *QoS*. Para a realização da pesquisa, foi utilizado um ambiente real de rede com switches, roteadores, servidores e computadores pessoais. Foram implementadas diversas topologias incluindo um servidor *Voip,* para suporte aos *softphones*. Foi possível analisar o impacto do trágego na comunicação *Voip,* quando não há políticas de *QoS*. O *software Wireshark* foi utilizado durante os testes para captura e análise do tráfego gerado pelos servidores, clientes e s*oftphones*. Foram utilizados os conceitos estudados durante as aulas do curso *CCNA Exploration.* A estrutura de rede *LAN* foi configurada utilizando o conceito de *VLANs,* quebrando o domínio de *broadcast.*

Palavras-chave: Tráfego, *Voip, QoS, Softphones, Wireshark, Iperf, Jperf.*

ABSTRACT

CROCETTI, Hugo Leonardo. **The impact of QoS in VoIP communications.** 2012. 70 pages. Monograph (Specialization in Configuring and Managing Servers and Networking Equipment) - Federal Technological University of Paraná. Curitiba, 2012.

This work had as main theme of the analysis and verification of data traffic and topologies to implement QoS policies stress tests were performed to compare the impact of topologies with and without QoS policies for the research was used an environment with real network switches, routers, servers and personal computers. We have implemented various topologies including a VoIP server to support softphones. It was possible to analyze the impact of communication trágego Voip, when no QoS policies Wireshark software was used during testing to capture and analyze the traffic generated by the servers, clients and softphones. We used the concepts studied in class CCNA Exploration Course. The structure of the LAN network was configured using the concept of VLANs, breaking the broadcast domain.

Keywords: Traffic, VoIP, QoS, Softphones, Wireshark, Iperf, Jperf.

LISTA DE ILUSTRAÇÕES

LISTA DE ILUSTRAÇÕES (CONT.)

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA

A tecnologia evoluiu rapidamente nas últimas décadas, tornando possível e acessível à compra de computadores em larga escala em países emergentes. O que acabou servindo de estímulo afim de que toda a infraestrutura necessária para o uso destes equipamentos evoluísse também.

No mundo corporativo, a competitividade no uso da tecnologia através de compra de equipamentos de ponta e com o uso de banda de comunicação provido pelas modernas redes de telecomunicações, tornou-se imprescindível para a sobrevivência.

Neste trabalho será apresentada uma análise de trafego *Voice over IP (Voip)* utilizando *Quality of Service (QoS)*.

1.2 DELIMITAÇÃO DA PESQUISA

Será realizado um estudo envolvendo alguns cenários topológicos de uma rede comutada por pacotes, e os impactos nesta quando utilizamos *Voip* com e sem a utilização de *QoS*.

Nos primeiros capítulos serão apresentados conceitos sobre redes de computadores, incluindo modelos de camada *OSI, TCP/IP* e equipamentos de rede.

A seguir serão expostas as tecnologias de redes locais (*LANs*), de redes geograficamente distribuídas (*WANs)* e a qualidade de serviço que possibilitará a priorização do tráfego de voz na rede.

Serão apresentadas as ferramentas que auxiliarão na administração de redes comutadas por pacote, os quais serão importantes para determinar a importância do *QoS*.

Serão apresentados os resultados de experimentos realizados em laboratório, utilizando-se equipamentos reais. Houve situações onde não houve uso do recurso de qualidade de serviço e o outras que não.

1.3 PROBLEMA

A tecnologia revolucionou todos os segmentos da nossa sociedade moderna e como consequência houve um grande crescimento na quantidade de usuários utilizando computadores, como ferramenta para desenvolver e manter negócios a nível global.

As redes evoluíram paralelamente trazendo um leque de possibilidades de convergência e inúmeras aplicações que estão diretamente ligadas à produtividade e geração de receita para empreendedores e desenvolvedores de novas tecnologias.

A tecnologia *Voip* veio de encontro com essa nova era digital por meio do uso de uma estrutura já existente de comunicação entre grandes corporações.

A proposta de realizar a gestão de equipamentos com qualidade de serviço para que seja garantida uma comunicação de voz com qualidade, implica nos equipamentos envolvidos analisarem os pacotes e priorizarem os de voz.

1.4 OBJETIVOS

A seguir, serão apresentados os objetivos gerais e específicos, onde será exposto o que se pretende atingir com este projeto de pesquisa.

1.4.1 Objetivo Geral

Realizar um estudo de caso de uma topologia de comutação de pacotes, utilizando *Voip* e verificar o impacto da implementação da qualidade de serviço na comunicação.

1.4.2 Objetivos Específicos

- Realizar a configuração física da topologia;
- Implementar a configuração lógica da rede;
- Realizar o mapeamento de endereçamento *IP*;
- Implementar os protocolos de roteamento entre sistemas autônomos;
- Analisar os softwares existentes para implementação da topologia;
- Verificar como os dados trafegam na rede;
- Analisar o impacto de tráfego de pacotes na comunicação de voz sobre *IP;*
- Configurar o *QoS* em Switches e Roteadores;
- Analisar os cenários com o uso de *QoS* nas comunicações de *Voip*.

1.5 JUSTIFICATIVA

A relevância deste projeto está em verificar qual o impacto da não implementação do *QoS* em um ambiente de rede onde exista a utilização da tecnologia *Voip*.

O enfoque será dado na maneira que será realizado a gestão de equipamentos com qualidade de serviço para que garanta uma comunicação de voz com qualidade.

Considerando que o tema será elaborado utilizando equipamentos reais em laboratório prático, este trabalho servirá de ponto de partida para analistas de suporte de empresas de pequeno e médio porte, que venham a se deparar com o paradigma da implementação da tecnologia *Voip* em suas redes de comunicações.

1.6 PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento desta monografia, foram utilizadas referencias bibliográficas sobre os elementos que se fizeram necessários, abordando às tecnologias envolvidas e equipamentos de rede.

O referido trabalho enfoca nas tecnologias LAN, WAN e como a qualidade de serviço exerce o papel fundamental na priorização de pacotes de voz evitando que eles sejam descartados.

Ao final foram analisados e apresentados os resultados de alguns cenários onde não existe a gestão de equipamentos com qualidade de serviço em contraste com cenários onde há gestão da qualidade de serviço.

1.7 FUNDAMENTAÇÃO TEÓRICA

Esta contribuição para os administradores de rede e gerentes de tecnologia da informação, no que diz respeito a conceitos, tecnologias e equipamentos foi extraído da revisão e leitura das seguintes obras: COLCHER (2005), COMER (2007), FILIPPETTI (2009), ODOM (2008), STALLINGS (2005) e TANENBAUM (2011).

Estas bibliografias auxiliaram no desenvolvimento dos objetivos específicos relacionados à tecnologia e utilização da tecnologia *Voip*. No que diz respeito a parte prática do trabalho, foram realizados ensaios laboratoriais nas instalações da UTFPR – Laboratório de Redes, onde foram realizadas diversas simulações de cenários hipotéticos em equipamentos reais. Onde foram coletados dados que possibilitaram demonstrar e fundamentar as conclusões mais precisas da implementação *Voip* utilizando *QoS* nas redes de comunicações.

1.8 ESTRUTURA

Esta monografia é estruturada em 4 capítulos, os quais visam satisfazer os objetivos propostos. No capítulo 1, capítulo introdutório a seguinte estrutura é formulada tendo início com: i) tema de pesquisa; ii) apresentação do problema; iii) objetivos; iv) justificativa; v) procedimentos metodológicos; vi) fundamentação teoria; vii) estrutura.

Para desenvolvimento do tema proposto foram desenvolvidos os capítulos 2, 3 e 4 que enfocam na teoria e prática desta pesquisa. No capítulo 2 é apresentado um breve resumo dos modelos de camadas *OSI* e *TCP/IP,* equipamentos e tecnologias *LAN* e *WAN*, protocolos de roteamento, qualidade de serviço e ferramentas para administração de rede. A parte de

maior interesse para profissionais da área concentra-se no capítulo 3, onde é apresentado os procedimentos e os testes realizados nos equipamentos, envolvendo a utilização de *Voip* em ambientes que possuem *QoS* ou não.

No capítulo 4 é apresentada a conclusão da monografia e suas considerações, descrevendo os resultados, aplicabilidade do *QoS* e os impactos da não utilização em ambientes que utilizam *Voip*.

1.9 CRONOGRAMA

ETAPA	Mês Ano 2012					
	Maio	Junho	Julho	Agosto	Setembro	Outubro
Elaboração do Pré-Projeto						
Entrega do Pré-Projeto de pesquisa						
Pesquisas Bibliográficas						
Pesquisas de tecnologias envolvidas						
Testes de Laboratório						
Redação da Monografia						
Correção e complementação						
Defesa da Monografia						

Figura 1. Cronograma.
Fonte: Autoria própria.

2 REFERENCIAL TEÓRICO

2.1 REDES DE COMPUTADORES

Na década de 1970, quando as primeiras redes de dados surgiram, apenas os computadores de um mesmo fabricante podiam trocar informações entre si. Não era possível a integração de dois ou mais computadores autônomos em que as produtoras fossem diferentes.

Apenas em 1974 a *IBM* (*International Business Machines*) publicou o seu modelo de redes, Arquitetura de Redes de Sistemas (*Systems Network Architecture*, ou *SNA*). Após essa divulgação, os fabricantes das mais variadas marcas passaram a utilizar o *SNA* para que fosse possível a interconexão entre seus produtos e os da *IBM*. Aos poucos essa solução mostrou-se negativa visto que com o passar do tempo os maiores fabricantes de computadores poderiam dominar o mercado de redes. (ODOM, 2008).

A fim de resolver este problema na década de 1980, criou-se um grupo de trabalho que iria criar um modelo de redes padronizado e aberto. E em 1983 foi apresentado pela *ISO* (*International Standards Organization*) o modelo de referência *OSI* (*Open Systems Interconnection*), que seria o primeiro passo em direção à padronização internacional de interconexão de sistemas abertos. (TANENBAUM, 2011).

Conforme Wendell Odom (2008, p.16) expõem que:

> Uma segunda, e menos formal, tentativa de se criar um modelo de redes padronizado e público emergiu de um contrato do Departamento de Defesa dos EUA. Pesquisadores de várias universidades se ofereceram para ajudar a desenvolver os protocolos criados pelo trabalho original do departamento. Esses esforços resultaram em um modelo de redes concorrente, chamado *TCP/IP*.

2.1.1 O Modelo de Referência OSI

O modelo *OSI* é um modelo de referência, que consiste em sete camadas. De acordo com (TANENBAUM, 2011): "... o modelo *OSI* propriamente dito não é uma arquitetura de rede, pois não especifica os serviços e os protocolos exatos que devem ser usados em cada camada. Ele apenas informa o que cada camada deve fazer." A seguir na figura 2 é ilustrado o Modelo de Referência *OSI*:

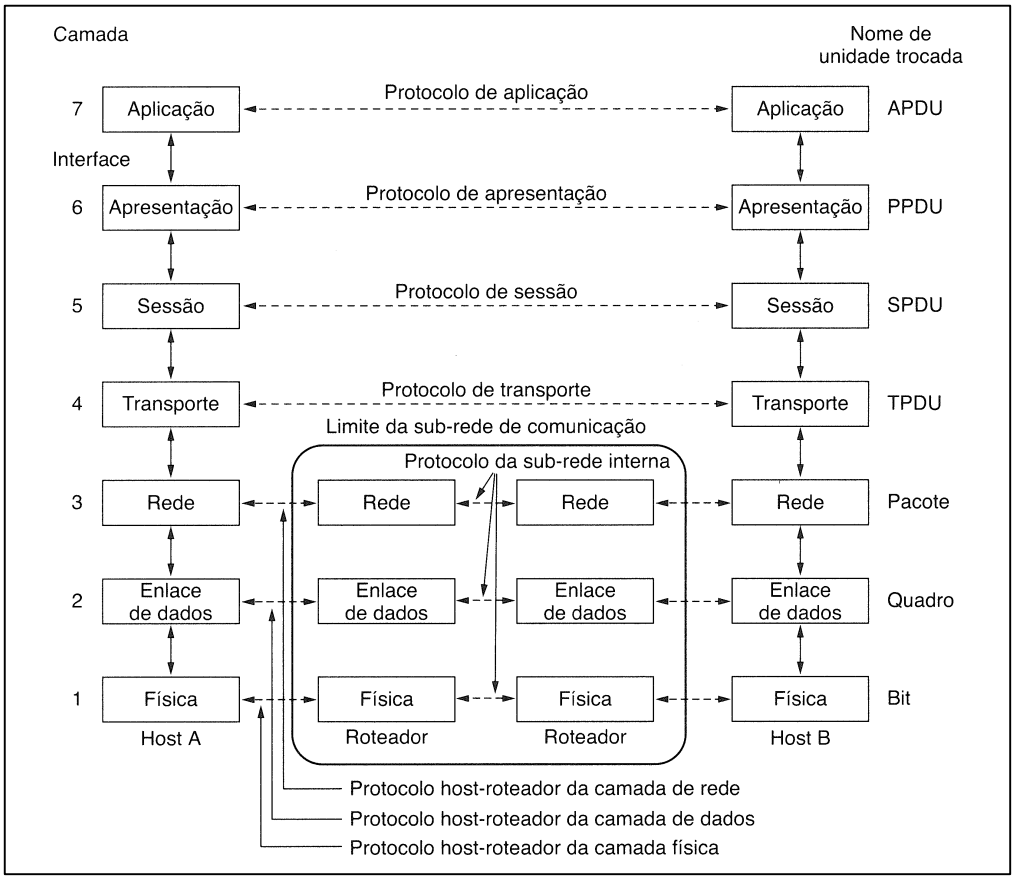


Figura 2. O modelo de referencia *OSI*.
Fonte: TANENBAUM, 2011.

A seguir será exposta cada uma das sete camadas do modelo *OSI*. Iniciaremos pela camada superior.

2.1.1.1 Camada de Aplicação

Nesta camada que ocorre a interface de contato entre micro-usuário. Também é nela onde encontramos uma série de protocolos comumente necessários para transferências de arquivos, correio eletrônico e transmissão de noticias pela rede. (TANENBAUM, 2011).

2.1.1.2 Camada de Apresentação

A função desta camada está relacionada com à sintaxe e à semântica das informações transmitidas. Ela torna possível a comunicação entre computadores com diferentes representações de dados. (TANENBAUM, 2011).

2.1.1.3 Camada de Sessão

Segundo (FELIPPETTI, 2009): "Ela é responsável pelo estabelecimento, gerenciamento e finalização de sessões entre a entidade transmissora e a entidade receptora. Ela basicamente mantém os dados de diferentes aplicações separados uns dos outros.".

Um dos diversos serviços oferecidos é o controle de diálogo (quem deve transmitir ao longo do tempo), gerenciamento e sincronização das transmissões caso ocorra uma falha. (TANENBAUM, 2011).

2.1.1.4 Camada de Transporte

A camada de transporte existe para garantir que haja uma comunicação fim-a-fim confiável. Isso é possível através dos serviços definidos nesta camada, as quais citamos duas importantes funções: *Multiplexação* (A palavra provém do inglês *multiplexing*, que significa transmitir diversas informações simultaneamente usando-se o mesmo meio ou canal.) e Controle de Fluxo. Pois como veremos á seguir nenhum protocolo de nível de rede fornece serviços confiáveis. Nestes protocolos também não há mecanismos que garantam uma entrega dos pacotes em sua sequência lógica. (FELIPPETTI, 2009).

2.1.1.5 Camada de Rede

A função desta camada é de controlar os pacotes que transitam por ela, de forma a superar qualquer problema relacionado à heterogeneidade das redes a serem interconectadas.

Os pacotes são roteados através de tabelas que podem ser estáticas ou dinâmicas. Também residem nesta camada, os mecanismos que gerenciam o possível congestionamento de pacotes. Na medida em que estes concorrem ao mesmo tempo a um caminho comum. (TANENBAUM, 2011).

Segundo Felippetti (2009, p.47): "Roteadores ou *"routers"*- também chamados de dispositivos de camada 3 (*layer 3 devices*) - são definidos nessa camada e provêm todos os serviços relacionados ao processo de roteamento.".

Existem dois tipos de pacotes definidos nesta camada: pacotes de dados (*data packets*) e pacotes de atualização (*router update packets*). (FELIPPETTI, 2009).

2.1.1.6 Camada de Enlace de Dados

O principal objetivo dessa camada é efetuar um controle de erros de forma que para sua camada superior eles não sejam detectáveis. E para que esta tarefa seja possível os dados enviados pelo transmissor são divididos, em quadros de dados contendo centenas ou milhares de bytes, e remetidos sequencialmente.

Existe também nesta camada o controle de fluxo, que evita que o transmissor envie ao receptor mais dados que esse tem condições de processar. (TANENBAUM, 2011).

Existem três tipos de tratamentos de controle de erros: simples detecção, detecção seguida de correção (efetuada pela retransmissão da informação corrompida) e correção efetuada automaticamente a partir do código. (COLCHER [et. al], 2005).

Conforme Felippetti (2009, p.49): "A camada de Enlace formata a mensagem em quadros e adiciona um cabeçalho customizado contendo o endereço de hardware (*MAC Address*) das máquinas transmissora e destinatária.". Na camada de enlace diferente da camada de rede o endereço físico de cada máquina importa.

2.1.1.7 Camada Física

A camada física é base de todas as camadas, ela trata sobre a transmissão de bits por um canal de comunicação. (TANENBAUM, 2011)

Segundo Colcher [et. al] (2005, p.57): “A função do nível físico é permitir o envio de uma cadeia de bits por um meio físico sem se preocupar com o seu significado ou com a forma como esses bits são agrupados.”.

2.1.2 O Modelo de Referência TCP/IP

Segundo Tanembaum (2011, p.28): “A ARPANET era uma rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos (*DoD*).”.

Com a evolução das redes de comunicação, divergindo da interconexão exclusiva de linhas telefônicas, houve uma procura por outra arquitetura de referência que resolvesse o problema de interligação das novas tecnologias com os protocolos existentes. Pouco tempo depois a resolução de heterogeneidade dessas diferentes redes foi alcançada pela criação do Modelo de Referência *TCP/IP*. (TANENBAUM, 2011).

O Modelo de Referência *TCP/IP*, ficou organizado em quatro camadas: Aplicação, Transporte, Inter-rede e *Host*/Rede. Abaixo, a figura 3 expõe lado a lado os dois modelos discutidos até este ponto.

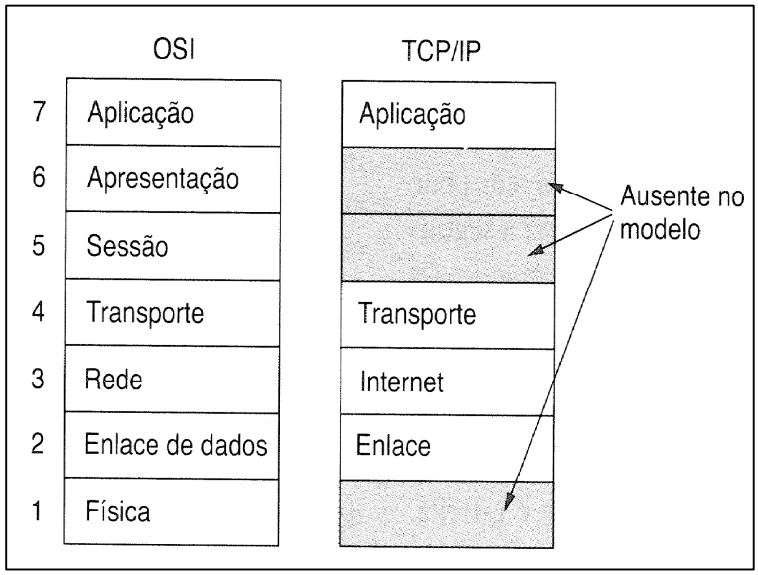


Figura 3. Os modelos de referência *TCP\IP* e *OSI*.
Fonte: TANENBAUM, 2011.

O Modelo de Referência *TCP/IP*, ficou organizado em quatro camadas: Aplicação, Transporte, Inter-rede e *Host*/Rede. A seguir serão descritas cada uma das quatro camadas do modelo *TCP/IP*. Iniciaremos pela camada superior.

2.1.2.1 Camada de Aplicação

Nesta camada estão todos os protocolos de nível mais alto. A seguir são expostos alguns bem difundidos na arquitetura *TCP/IP*:

TELNET (Telephone Network) – A principal função é a emulação de terminais.

FTP/TFTP (File Transfer Protocol/Trivial FTP) – Utilizado na transferência de arquivos entre duas máquinas. O *TFTP* apenas se diferencia do *FTP* por não possuir pesquisa em diretórios.

NFS (Network File System) – Especializado em compartilhamento de arquivos, permitindo o intercambio de dados entre tipos de sistemas heterogêneos.

SMNP (Simple Mail Transfer Protocol) – Este protocolo coleta e manipula informações de rede.

DNS (Domain Name Service) – Responsável pela resolução de nomes para endereços *IP*. (TANENBAUM, 2011).

2.1.2.2 Camada de Transporte

A principal funcionalidade desta camada é tornar transparente a camada superior as interações da rede que existem para que seja possível a conversação entre hosts de origem e destino.

Nesta camada foram definidos dois protocolos fim a fim:

O primeiro, *TCP (Transmission Control Protocol)* – Protocolo de controle de transmissão, o qual é segundo Tanembaum (2011, p.29): "..um protocolo orientado a conexões confiável que permite a entrega sem erros de um fluxo de bytes originário de uma determinada máquina em qualquer computador da internet.".

E o segundo, *UDP (User Datagram Protocol)* – Protocolo de datagramas de utilizador, o qual diferente do TCP ele não é orientado a conexão e também não confiável.

Normalmente o *TCP* é utilizado quando há necessidade de transporte de dados confiável e o *UDP* quando há necessidade de um transporte rápido. (FELIPPETTI, 2009).

2.1.2.3 Camada de Inter-Rede

A camada de inter-rede é responsável pela integração de toda a arquitetura em uma interface de rede unificada, para as camadas superiores. Pois ela permite que os pacotes sejam roteados e cheguem ao seu destino, compatibilizando os diferentes tipos de protocolos. (TANENBAUM, 2011).

Há muita semelhança entre a camada inter-rede do modelo *TCP/IP* e a camada de rede do modelo *OSI*. Nesta camada quatro protocolos coexistem: *IP* (*Internet Protocol*), *ICMP* (*Internet Control Message Protocol*), *ARP* (*Address Resolution Protocol*) e *RARP* (*Reverse Address Resolution Protocol*). O mais importante destes é o protocolo IP, visto que os demais existem apenas para suportá-lo. (FELIPPETTI, 2009).

O funcionamento dessa camada inicia-se pelo recebimento de pacotes da camada de transporte, que informa o endereço de destino. Logo em seguida o pacote é encapsulado em um datagrama *IP* e o algoritmo de encaminhamento determina se ele poderá ser entregue na mesma rede ou se ele deverá ser direcionado a um roteador. (COLCHER [et. al], 2005).

2.1.2.4 Camada de Host/Rede

É a camada inferior do modelo *TCP/IP*, nela não há restrição alguma no que diz respeito a interconexões de tecnologias das mais variadas origens em formar a inter-rede. Há apenas um ponto a ser observado: que estas tenham uma interface que compatibilize a sua tecnologia particular ao protocolo *IP*. (COLCHER [et. al], 2005).

Nesta camada são definidos, segundo Felippetti (2009, p.141): "..os protocolos de acesso ao meio (como *Ethernet, Token Ring, LocalTalk e FDDI*), os padrões de conectores

físicos (como *RJ-45, V.35, AUI* etc.), os padrões de sinalização elétrica (*como IEEE 802.2, IEEE 802.3, IEEE802.5* etc.) e as topologias..".

2.1.3 Equipamentos de Rede

Uma rede de computadores é composta por diversos equipamentos, que juntos compõem uma infraestrutura. A seguir serão vistos os principais elementos que estão presentes na grande maioria das redes de computadores. Historicamente existiram diversos padrões *LAN* (*Local area network* – Rede de área local), tais como citados por Felippetti no tópico anterior. Porém ao longo do tempo foram deixados para trás, e apenas a família de padrões os quais o termo *ETHERNET* (Tecnologia de interconexão para redes locais) refere-se continuou, tornando-se o padrão mais difundido no mundo á fora. (ODOM, 2008).

Veremos a seguir os principais equipamentos utilizados para interconectar redes locais (*LAN)* e rede de longa distância (*WAN)*.

2.1.3.1 Hubs Ethernet

Figura 4. Hub Cisco 1538 Series.
Fonte: SYSTEMS INC, Cisco. 2012.

O *Hub* é essencialmente um repetidor que possuí múltiplas portas e a função de fornecer um ponto de conexão centralizado a *LAN*. Ele é considerado um equipamento de camada um, visto que não realiza a interpretação de bits mais apenas a análise dos sinais elétricos. O funcionamento dele consiste em realizar a limpeza do sinal elétrico e sua renovação, permitindo que maiores distâncias sejam alcançadas. Porém ele não divide cada

porta em um *domínio de colisão* (é a definição de uma área lógica que frames, vindos de dispositivos diversos poderão colidir), motivo pelo qual não é possível transmitir dados simultaneamente através de mais de um transmissor por vez. (ODOM, 2008).

2.1.3.2 Switches LAN

Figura 5. Switch Cisco Catalyst Modelo 2960.
Fonte: SYSTEMS INC,Cisco. 2012.

Os switches são equipamentos que operam na camada dois (enlace), ou seja, operam analisando os quadros que passam por eles para determinar a porta requerida para envio dos dados. As vantagens em utilizá-los em relação a *hubs* são: cada porta do *switch* é um domínio de colisão próprio e diversos dispositivos podem transferir dados simultaneamente sem que ocorram colisões. Um dos métodos empregados pelos switches é o *buffering* (consiste em armazenar os frames temporariamente em memória) que evita colisões quando mais de um dispositivo quer enviar dados na mesma porta. Normalmente são mais rápidos do que os *Hubs*, pois as portas não compartilham largura de banda entre si como ocorre no hub. (ODOM, 2008).

2.1.3.2.1 Lans virtuais

O conceito de *Virtual Lan* (*VLAN*) está relacionado à divisão de domínio de broadcast (segmento lógico onde todos os dispositivos interconectados podem trocar

informações, através do recebimento e envio de quadros de um dispositivo, que será recebido por todos os outros) ao realizarmos a divisão de parte das interfaces de um *switch* em um domínio de broadcast e a as demais em outro estamos criando *VLANs* diferentes. O uso dessa implementação permite que seja reduzido a sobrecarga causada pelo aumento excessivo de *hosts* numa mesma *LAN*, melhora a segurança visto que separa grupos com características específicas logicamente através de um mesmo switch. (ODOM, 2008).

Quando um projeto de rede engloba mais do que apenas um pequeno grupo de computadores, e ultrapassa a quantidade de portas disponíveis em um *switch*, acaba por segmentar esse grande grupo em duas *LANs* diferentes. No intuito de resolver esse problema, os *switches* utilizam o *Trunking de VLAN*. Que permite que um switch seja capaz de enviar frames de diversas *VLANs*, através de um única conexão física. Estendendo as *VLANs* através de mais de um switch e aumentando o número potencial de dispositivos que podem ser interconectados. (TANEMBAUM, 2011).

Na figura abaixo é exposto um exemplo de rede com duas *VLANs* utilizando um *switch*:

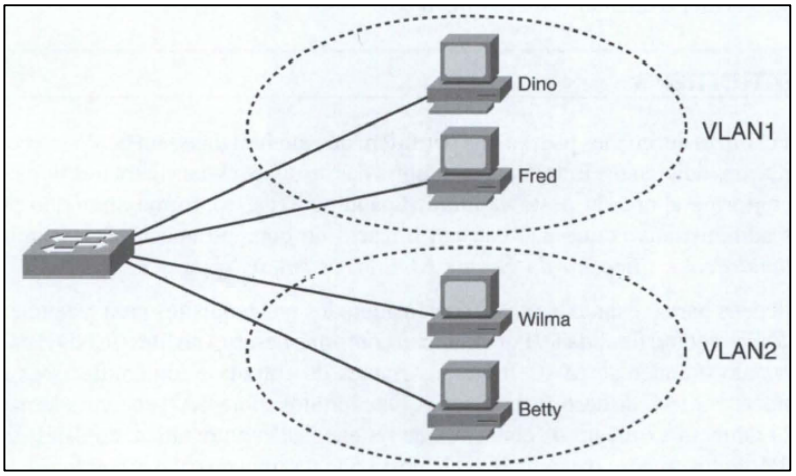


Figura 6. Rede com duas *VLANs* em um *Switch*.
Fonte: ODOM, 2008.

2.1.3.3 Roteador

F

Figura 7. Roteador Cisco Integrated Services Modelo 2811.
Fonte: SYSTEMS INC,Cisco. 2012.

O roteador tem o papel de interconectar duas ou mais redes de computadores, dispersas fisicamente, ele atua na comutação de protocolos, por este motivo ele pertence à camada três. A capacidade de encaminhar pacotes entre dois dispositivos que estão em redes separadas é possível ao roteador por ele obter os seguintes dados: endereços das redes conectadas a roteadores vizinhos e identificar as melhores rotas para se chegar a uma rede destino. O roteador armazena as informações de como alcançar cada rede aprendida numa tabela de roteamento. A qual pode ser preenchida através de um administrador de rede ou com troca de informações entre roteadores vizinhos. (FELIPPETTI, 2009).

A tabela de roteamento é fundamental aos roteadores, visto que um pacote endereçado a uma rede diferente das que estiverem diretamente conectadas deverá possuir seu destino armazenado na tabela. No caso de não existir essa correspondência o roteador irá descartar o pacote, visto que ele não envia mensagem de broadcast para identificação de rota. (ODOM, 2008).

2.1.3.4 Telefones IP

Figura 8. Telefone Cisco *Unified IP Phone* Modelo 7941G.
Fonte: SYSTEMS INC,Cisco. 2012.

O telefone *IP* é ligado na rede *LAN*. É por meio dela que ele envia pacotes *Voip* para outros telefones *IP* que podem estar na mesma rede ou em redes dispersas fisicamente. Também é possível o envio de pacotes *VOIP* para portas de comunicação que tenham conexão com rede de telefonia tradicional (*PSTN – Public Switched Telephone Network*), desse forma torna-se possível ligar para qualquer telefone do mundo. (ODOM, 2008).

2.1.4 Tecnologias LANs

O termo LAN, segundo Odom (2008, p.31): "..refere-se a um conjunto de padrões das Camadas 1 e 2 elaborado para trabalhar em conjunto com o propósito de implementar redes geograficamente pequenas.".

O *Institute of Electrical and Eletronics Engineers* (*IEEE)* é o responsável pelo processo de padronização das LANs. Como pode ser visto a seguir, os principais padrões de tecnologias para interconexão de redes locais, suas diferenças de velocidade no que diz respeito a tráfego de dados e comprimento máximo permitido pelos cabos.

2.1.4.1 Ethernet

O *IEEE* definiu inicialmente em meados de 1980, dois padrões: 10BASE5 e 10BASE2. E com eles também o algoritmo de detecção de portadora para múltiplo acesso com detecção de colisão *Carrier Sense Multiple Access with Collision Detection* (*CSMA/CD)*, eles atingiam a velocidade máxima de 10 Mbps (megabits por segundo). Os conceitos definidos para estes dois padrões mais tarde foram utilizados em todas as *LANs* modernas.

Segundo Odom (2008, p.37) exemplifica três principais conceitos, que são:

> - As *LANs Ethernet* originais criavam um barramento elétrico ao qual todos os dispositivos se conectavam.
> - Pelo fato de que colisões ocorriam nesse barramento, a *Ethernet* definiu o algoritmo *CSMA/CD*, o qual definia uma forma tanto de evitar as colisões quanto de agir quando elas acontecessem.
> - Os repetidores estendiam o tamanho das *LANs* ao limpar o sinal elétrico e repeti-lo - uma função de Camada 1 - mas sem interpretar o significado do sinal elétrico.

O *IEEE* definiu um novo padrão em meados de 1990 o 10BASE-T, que veio a resolver diversos problemas dos seus antecessores. Foi possível a utilização de cabeamento telefônico já existente o *Unshielded Twisted Pair (UTP)* no lugar do caro e difícil de instalar o cabo coaxial. Outra melhoria foi o conceito de ligar cada dispositivo a um ponto central. Ou seja, foi introduzida a utilização de h*ubs* e *switches* para que fosse possível a interconexão desse padrão. (ODOM, 2008).

2.1.4.2 Fast Ethernet

Ele foi aprovado sob o nome de 802.3u pelo IEEE, em meados de 1995. Tecnicamente não é um novo padrão, mais sim um adendo ao padrão ethernet, seu antecessor. A quantidade de pares de fios necessários para seu funcionamento é da ordem de dois, sendo que um par é responsável pelo envio de informações em uma direção e outro na direção contrária. (TANENBAUM, 2011).

No funcionamento *Full-Duplex*, não necessário verificar o meio antes de transmitir dados, pois esta disputa é impossível, visto que é o único transmissor possível na linha. Já no funcionamento do *Half-Duplex*, os computadores estarão interligados através de um *Hub* que obrigatoriamente deverá utilizar o protocolo *CSMA/CD*. (TANENBAUM, 2011).

Os tipos de fios aceitos para transportar os sinais utilizando esse padrão, estão expostos na figura 8, logo abaixo:

Nome	Cabo	Tam. máx. de segmento	Vantagens
100Base-T4	Par trançado	100 m	Utiliza UTP da categoria 3
100Base-TX	Par trançado	100 m	Full-duplex a 100 Mbps (UTP da categoria 5)
100Base-FX	Fibra óptica	2000 m	Full-duplex a 100 Mbps; grandes distâncias

Figura 9. O cabeamento *Fast Ethernet*.
Fonte: TANENBAUM, 2011.

O *Fast Ethernet* oferece uma velocidade de dez vezes maior que seu antecessor, ou seja, 100 Mbps. Além de flexibilidade para redes ethernet existente, através do uso de placas de rede 10/100 Mbps, com recurso chamado de detecção automática (*Auto Sense*).

2.1.4.3 Gigabit Ethernet

É um padrão *ethernet* também conhecido por 802.3z, que foi ratificado pelo comitê *IEEE* em meados de 1998. Diferentemente de seus antecessores, as configurações de *gigabit ethernet* são ponto a ponto, e não multiponto. Outra característica importante é que ele admite dois modos de operação: *Full-Duplex* (onde é possível enviar e receber dados ao mesmo tempo, pois cada operação é realizada em um canal dedicado) e *Half-Duplex* (onde é possível apenas enviar ou receber dados, visto que existe apenas um canal). (TANENBAUM, 2011).

Os tipos de cabeamentos possíveis para a ethernet gigabit são: fios de cobre e de fibra. Logo abaixo na figura 9, ambos são expostos com mais detalhes:

Nome	Cabo	Tam. máx. de segmento	Vantagens
1000Base-SX	Fibra óptica	550 m	Fibra de multimodo (50, 62,5 micra)
1000Base-LX	Fibra óptica	5000 m	Modo único (10) ou multimodo (50, 62,5)
1000Base-CX	2 pares de STP	25 m	Par trançado blindado
1000Base-T	4 pares de UTP	100 m	UTP padrão da categoria 5

Figura 10. O cabeamento da *Gigabit Ethernet*.
Fonte: TANENBAUM, 2011.

O *Ethernet Gigabit* oferece uma velocidade de dez vezes mais que seu antecessor, ou seja, 1000 Mbps. Ele admite controle de fluxo, através do uso de quadros *PAUSE*. E também mantêm a flexibilidade para uso em redes *Ethernet* e *Fast Ethernet* existentes.

2.1.5 TECNOLOGIAS WANs

O termo *Wide Area Network* (*WAN)*, segundo Comer (2007, p.200) é:

> O aspecto chave que separa as tecnologias de WAN das tecnologias de LAN é a escalabilidade – uma WAN deve ser capaz de crescer o quanto for necessário para conectar muitos sites espalhados por distâncias geograficamente grandes, com muitos computadores em cada um.

Uma tecnologia *WAN* também deve ser capaz de proporcionar desempenho razoável aos computadores interconectados de forma que seja possível a troca de informações simultaneamente entre eles. (COMER, 2007).

2.1.5.1 PROTOCOLO PPP

O *Point-to-Point Protocol* (*PPP*) tem a tarefa de transportar pacotes de camada de rede através de um enlace da camada de enlace. Além dessa tarefa ainda podemos citas muitas outras funções segundo Odom (2008, p.317):

> • Definição de um cabeçalho e um *trailer* que permite a entrega de um quadro de dados através do enlace.
> • Suporte a enlaces síncronos e assíncronos.
> • Um campo tipo de protocolo no cabeçalho, permitindo que vários protocolos de camada 3 passem através do mesmo enlace.
> • Ferramentas de autenticação embutidas: *PAP* (*Password Authentication Protocol*) e *CHAP* (*Challenge Handshake Authentication Protocol*).
> • Protocolos de controle para cada protocolo de camada mais alta que executa sobre o *PPP,* permitindo uma integração mais fácil e suporte a estes protocolos.

Diferente do seu antecessor *High-level Data Link Control* (*HDLC*), o protocolo *PPP* incluí em seu frame um campo tipo de protocolo, que identifica o protocolo tornando possível a interligação de roteadores de diferentes fabricantes. (ODOM, 2008).

Na figura 11 são expostos alguns conceitos relacionados a circuitos *WAN*, e logo em seguida explicados alguns termos-chave.

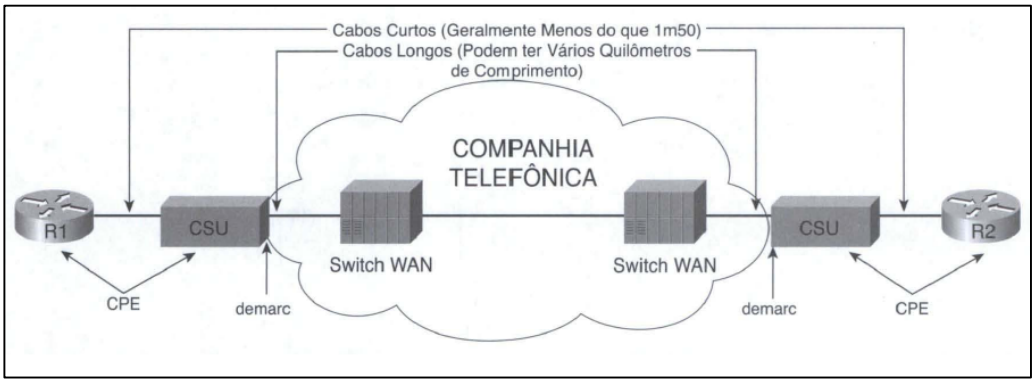


Figura 11. Linha alugada ponto-a-ponto: componentes e terminologia.
Fonte: ODOM, 2008.

O termo *Customer Premises Equipment* (*CPE*) é uma referencia a dispositivos que ficam no lado do cliente. Normalmente o roteador existente no *CPE* liga-se a um dispositivo chamado de unidade de serviço de canal / unidade de serviço de dados *Channel Service Unit / Data Service Unit (CSU/DSU*). Ainda conectado a *CSU/DSU* está um cabo da companhia prestadora de serviços. O ponto que divide as responsabilidades da operadora e cliente é identificado pelo *Demarc* em referencia a "ponto de demarcação". (ODOM, 2008).

2.1.5.2 Frame Relay

Além da conectividade *WAN* de linhas alugadas (ponto-a-ponto), existe outra opção que pode ser categorizada como comutação de pacote. Na sua antecessora, rede ponto-a-ponto, era possível através de um enlace interligar apenas dois sites. Já no protocolo Frame Relay, através do serviço de comutação de pacotes, através de um único link é possível centralizar a comunicação de diversos roteadores. Desta forma ele acaba sendo muito mais econômico no que diz respeito ao crescimento da rede e favorecendo a comunicação direta entre todos os sites que estiverem conectados. (ODOM, 2008).

No ponto-a-ponto a operadora examina os quadros enviados pelo roteador, utilizando a comutação de pacotes segundo Odom (2008, p.64):

> O *Frame Relay* define o seu próprio cabeçalho e rodapé *data-link*. Cada cabeçalho *Frame Relay* armazena um campo de endereço chamado de identificador de conexão *datalink* (*datalink connection identifier*, ou *DLCI*). O *switch WAN* encaminha o frame baseado no *DLCI*, enviando o frame através da rede do provedor até que ele chegue ao roteador do site remoto, no outro lado da nuvem do *Frame Relay*.

Na figura 12 são expostos alguns conceitos relacionados a redes *Frame Relay*:

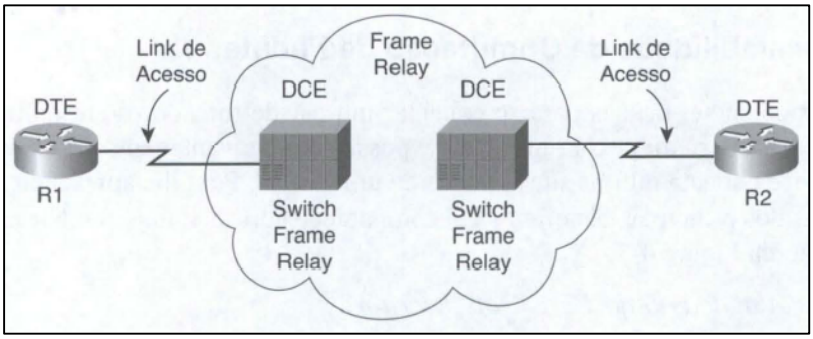


Figura 12. Componentes do *Frame Relay*.
Fonte: ODOM, 2008.

O *Frame Relay* é uma rede multiacesso (onde mais de dois dispositivos podem ser conectados). É possível observamos na figura 11 que os links de acesso (são linhas alugadas tais como no *PPP*) ligam os roteadores a um *switch Frame Relay*.

2.1.5.3 MPLS

MultiProtocol Label Switching (MPLS) é uma tecnologia que está sendo empregada em larga escala pelas provedoras de serviço de *Internet*. Seu funcionamento baseia-se na inclusão de um rótulo, ao invés de um endereço de destino para mover os pacotes dentro da sua rede. Essa técnica reduz muito o tempo de encaminhamento de pacotes, visto que o rótulo é usado como índice numa tabela interna, que direciona a interface de saída correta. (TANENBAUM, 2011).

Conforme a definição de Tanenbaum (2011, p.295):

> O cabeçalho *MPLS* genérico tem 4 *bytes* de extensão e quatro campos. O mais importante é o campo *Rótulo*, que mantém o índice. O campo *QoS* indica a classe do serviço. O campo *S* relaciona-se ao empilhamento de vários rótulos. O campo *TTL* indica quantas vezes o pacote pode ser encaminhado.

Na figura 13 é exposto o formato do quadro incluindo os cabeçalhos *PPP, MPLS, IP e TCP*. Também no detalhe o cabeçalho genérico de *MPLS:*

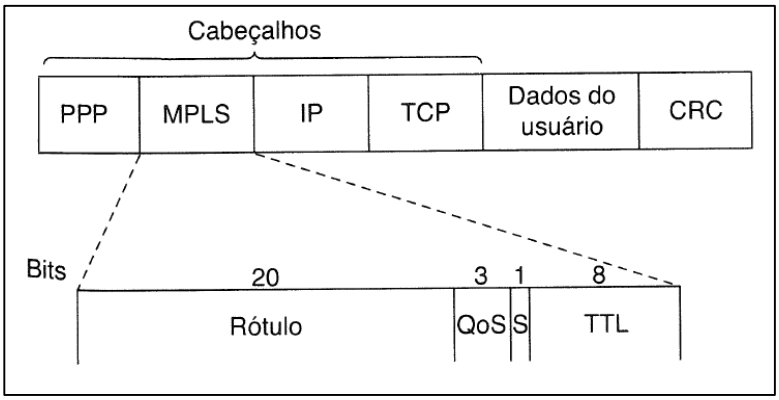


Figura 13. Transmitindo um segmento *TCP* usando *IP, MPLS e PPP*.
Fonte: TANENBAUM, 2011.

O protocolo *MPLS* é dito multiprotocolo pelo fato do seu cabeçalho não fazer parte do pacote de camada de rede e também do quadro da camada de enlace de dados. Permitindo que ele encaminhe tanto pacotes *IP*, quanto pacotes que não sejam *IP*. Os rótulos são adicionados aos pacotes quando estes alcançam um roteador de borda de rótulo, chamado de *Labell Edge Router (LER)*, através desse rótulo que o pacote será encaminhado dentro da rede *MPLS*. (TANENBAUM, 2011).

Na figura 14 é exposto o processo descrito acima:

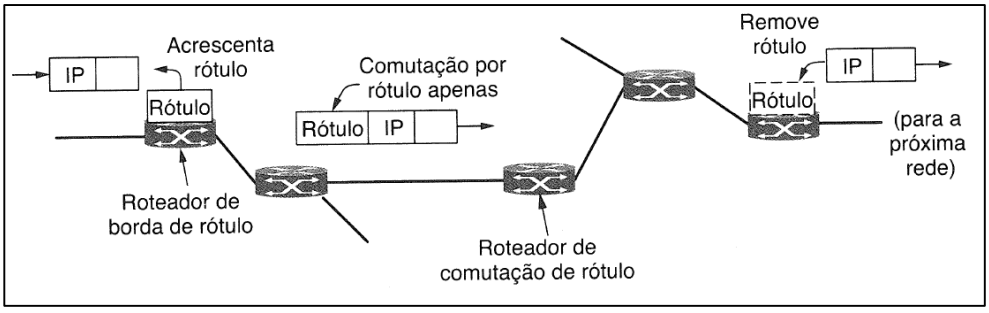


Figura 14. Encaminhamento de um pacote *IP* por uma rede *MPLS*.
Fonte: TANENBAUM, 2011.

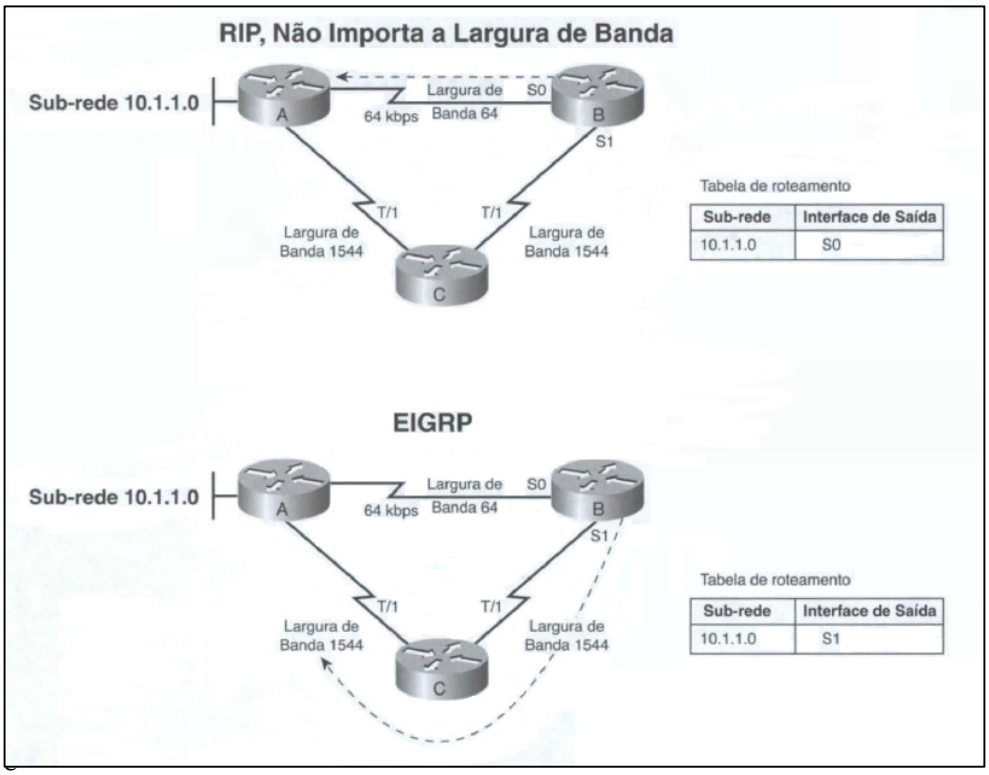
2.2 PROTOCOLOS DE ROTEAMENTO

2.2.1 RIPv2

Trata-se de um protocolo de roteamento enquadrado na categoria *Interior Gateway Protocol (IGP)* ele assim como os demais protocolos de roteamento *IP* auxilia o roteador a preencher a tabela de roteamento. Seu funcionamento consiste em anúncios de rotas contidas em sua tabela de roteamento para seus roteadores vizinhos. (ODOM, 2011).

O *Ripv2* utiliza como meio de decisão de melhor rota a quantidade de saltos (*hops)* que um pacote executa ao chegar ao seu destino. Ele ignora qualquer outra informação como, por exemplo, a largura de banda e foca-se na rota onde a quantidade de saltos seja menor. Outra vantagem do *Ripv2* é que ele suporta *Variable Length Subnet Masking (VLSM)* e a envia nas suas atualizações de roteamento, além de suportar a sumarização manual de rotas. (ODOM, 2011).

Na figura 15 observamos a diferença de métrica entre *Ripv2* e *Ospf*.



ura 15. Comparação dos efeitos das métricas de *RIP* e *EIGRP*.
Fonte: ODOM, 2011.

2.2.2 EIGRP

O protocolo de roteamento *Enhanced Interior Gateway Routing Protocol (EIGRP)* ele possui entre outros atributos uma convergência rápida além de consumir menos recursos do roteador. Este protocolo é proprietário, ou seja, só poderá ser empregado entre roteadores cisco. (ODOM, 2008).

Seu funcionamento consiste em envio de mensagens *Hello* para seus roteadores vizinhos, na sequencia ele realiza algumas verificações para determinar se os roteadores devem ou não tornar-se vizinhos. Em seguida há trocas de topologias completas entre os roteadores vizinhos, e depois apenas quando ocorrer alguma mudança na topologia da rede. (ODOM, 2008).

O *EIGRP* suporta balanceamento de carga com custos desiguais, possui características de enviar as suas atualizações de roteamento através de *Multicast* não *Broadcast* como alguns outros protocolos. Também possui autenticação para checar se o roteador vizinho possui o mesmo número de *AS* (Sistema Autônomo) configurado. (ODOM, 2008).

2.2.3 OSPF

O protocolo de roteamento *Open Shortest Path First (OSPF)* é padronizado pelo *Internet Enginerring Task Force (IETF)* de acesso público, ou seja, não pertence a nenhum fabricante proprietário sendo que sua utilização é empregada na maioria das redes heterogêneas. (FELIPPETTI, 2009).

O Seu funcionamento consiste em troca de mensagens com seus roteadores vizinhos, troca de informações de banco de dados de rotas e cálculos de rotas baseados no algoritmo de Dijkstra. (ODOM, 2008).

O protocolo *OSPF* é um protocolo enquadrado na categoria *Interior Gateway Protocol (IGP)* visto que é utilizado dentro de uma mesma rede, por este motivo leva o nome de protocolo gateway interior. O *OSPF* dá suporte ao roteamento com base no tipo de serviço,

roteando o tráfego em tempo real de uma maneira e o restante do tráfego de outra. (TANEMBAUM, 2011).

2.3 QUALIDADE DE SERVIÇO

Na medida em que as redes privadas tornaram-se populares a quantidade de tráfego entre elas e a *World Wide Web (WEB)* aumentou consideravelmente. O aumento de volume de dados rapidamente tornou imperativo a criação e desenvolvimento de métodos sensíveis e eficazes para gerenciar o tráfego e controlar o inevitável congestionamento. (STALLINGS, 2005).

Qualidade de serviço (Quality of Service – *QoS*) foi a solução para este tráfego de dados crescente. Na medida em que é realizado a priorização na rede, garantindo que os dados mais importantes devam receber uma maior preferência em relação aos dados menos relevantes. Se o tráfego estiver muito intenso, estes pacotes sem muita importância poderão ser descartados. (TANENBAUM, 2011).

Na figura 16 são expostas algumas aplicações e o grau de sensibilidade ao atraso pelo grau de importância:

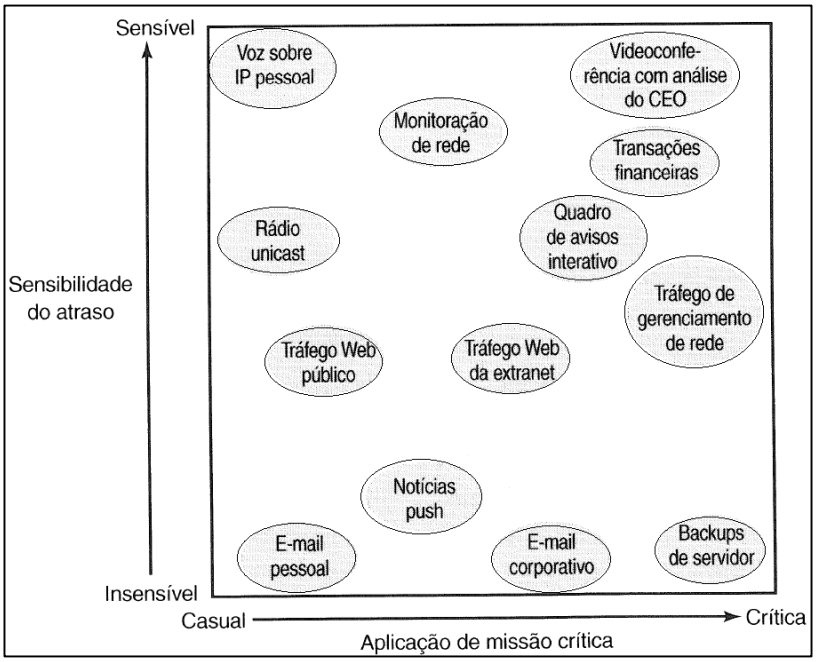


Figura 16. Comparação entre a sensibilidade de atraso da aplicação e aplicação crítica de uma empresa.
Fonte: STALLINGS, 2005.

Segundo Tanenbaum (2011, p.253):

> Quatro aspectos devem ser resolvidos para garantir a qualidade do serviço: 1- Que aplicações da rede são necessárias; 2- Como regular o tráfego que entra na rede; 3- Como reservar recursos nos roteadores para garantir o desempenho; 4- Se a rede pode aceitar mais tráfego com segurança.

2.3.1 Serviços Integrados

Resultado dos esforços do Internet Engineering Task Force (*IETF*) que ficou conhecida também como *Integrated Services (INTSERV)*, que deu vida à criação de uma arquitetura para streaming de multimídia. (TANENBAUM, 2011).

Segundo Colcher (2005, p.127): "A solicitação de serviços na arquitetura *IntServ* normalmente emprega procedimentos dinâmicos e que dependem de protocolos de sinalização específicos, sendo o *Resource reSerVation Protocol* (*RSVP)* o principal deles.".

O *RSVP* é responsável por fazer reservas, monitorar e gerenciar a largura de banda. Permitindo que vários transmissores enviem os dados para vários grupos receptores. Uma limitação a essa arquitetura é a sua pouca escalabilidade, tornando-a inadequada a redes de *backbone*. (COLCHER [et. al], 2005).

2.3.2 Serviços Diferenciados

Segundo Stallings (2005, p.171): "A arquitetura de serviços diferenciados (ou *Differentiated Services - DS*) foi criada para oferecer uma ferramenta simples, fácil de implementar e de baixa sobrecarga, para dar suporte a uma série de serviços de rede que são diferenciados com base no desempenho.".

O *DS* não é classificado quanto ao fluxo de informações requeridas e sim, no tráfego, onde cada pacote é classificado para estar num número limitado de classes de tráfego. Esta arquitetura possibilita uma redução no número de estados que devem ser mantidos nos roteadores da rede. (COLCHER [et. al], 2005).

Normalmente os serviços de *DS* são fornecidos por uma portadora de serviços de telecomunicação. Toda portadora forma um domínio administrativo, e define internamente um conjunto de classes de serviço com regras e assinatura para cada pacote que ingressar no seu domínio. Porém como cabe a cada operadora definir suas classes de serviços foi definido pela *EITF* algumas classes independentes da rede:

- A mais simples delas é a classe de encaminhamento expresso, que define internamente duas classes de serviços: regular e expressa. Cabendo ao host realizar esta marcação no pacote ou o primeiro roteador de ingresso.

- Outra mais elaborada chamada de encaminhamento garantido, que especifica que haverá quatro classes de prioridade. Além de três classes de descarte. Totalizando a relação destes dois fatores acabamos por ficar com doze classes de serviço. (TANENBAUM, 2011).

Na figura 17 verificamos uma forma possível no esquema de encaminhamento garantido:

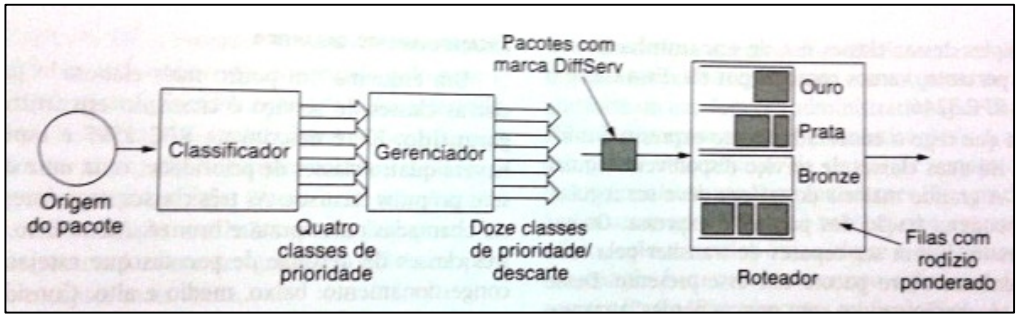


Figura 17. Uma implementação possível do fluxo de dados para encaminhamento garantido.
Fonte: TANENBAUM, 2011.

2.4 FERRAMENTAS PARA ADMINISTRAÇÃO DE REDE

As ferramentas que serão apresentadas a seguir: *Ccna Tftp Server, Wireshark* e *Iperf*. Auxiliam o administrador de redes, nas tarefas de atualização e *backup* de *IOS* dos equipamentos cisco, testes e análises do ambiente de rede de uma maneira controlada. Através do uso dessas ferramentas é possível realizar estratégias de forma a melhorar a eficiência da rede pelo administrador e obter um ambiente mais seguro em caso de desastres.

2.4.1 *Ccna Tftp Server*

O *Software Ccna Tftp Server* é um servidor que auxilia a upload e download de arquivos numa rede. Foi utilizado principalmente para transferência de backup contendo as configurações dos roteadores e switches. Sua aplicabilidade incide na disponibilidade de uma rede 24 x 7, servindo como uma ferramenta que irá amenizar um impacto de um desastre. É uma das ferramentas mais utilizadas em ambientes de produção. Pois existindo backups de configuração dos equipamentos atualizados em pouco tempo é possível restaurar as configurações.

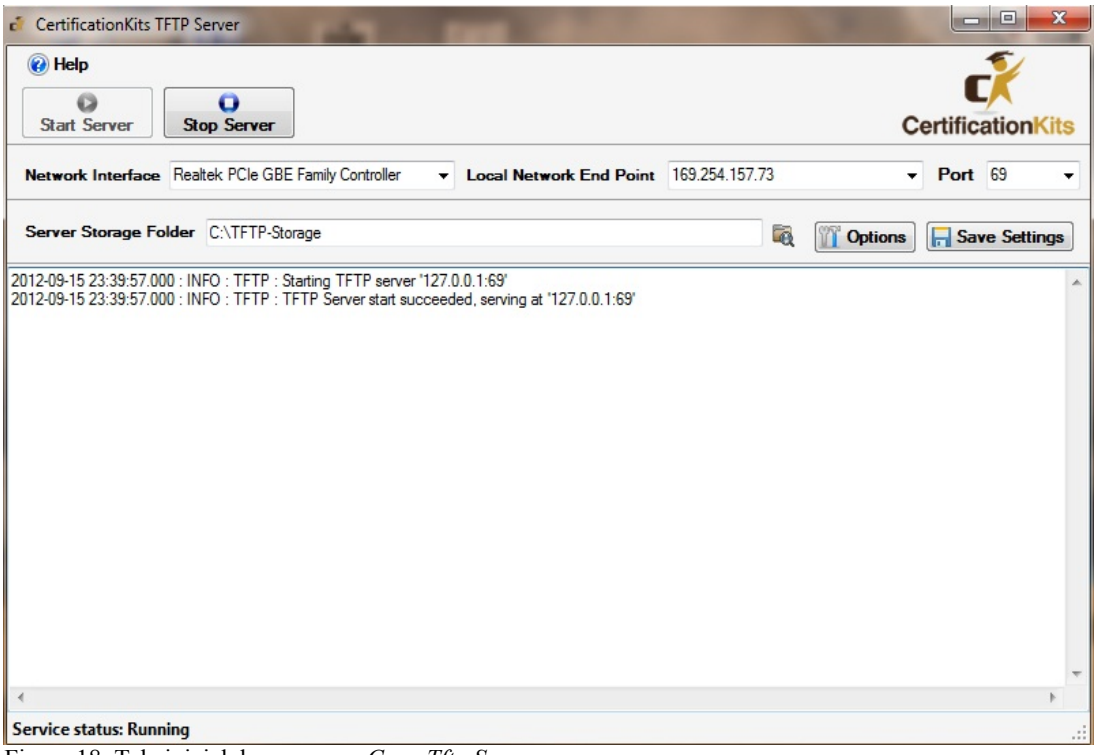


Figura 18. Tela inicial do programa *Ccna Tftp Server*.
Fonte: Autoria própria.

2.4.2 Wireshark

O *Wireshark* é um *sniffer* (analisador de protocolo) que permite capturar o tráfego de rede. Ele proporciona através de um ambiente gráfico uma poderosa ferramenta de análise de protocolos. Sendo possível analisar todo o tipo de comunicação de entrada e saída do computador no qual ele esteja rodando. É um dos mais populares do seu gênero, pois está disponível para diversas plataformas e não requer nenhuma configuração específica. Ele está disponível gratuitamente como *open source* (termo "código aberto" foi criado pela *OSI* e refere-se a software livre), e é lançado sob a versão *General Public License 2 (GNU)*.

Na figura 19 logo abaixo observamos a tela principal do programa Wireshark:

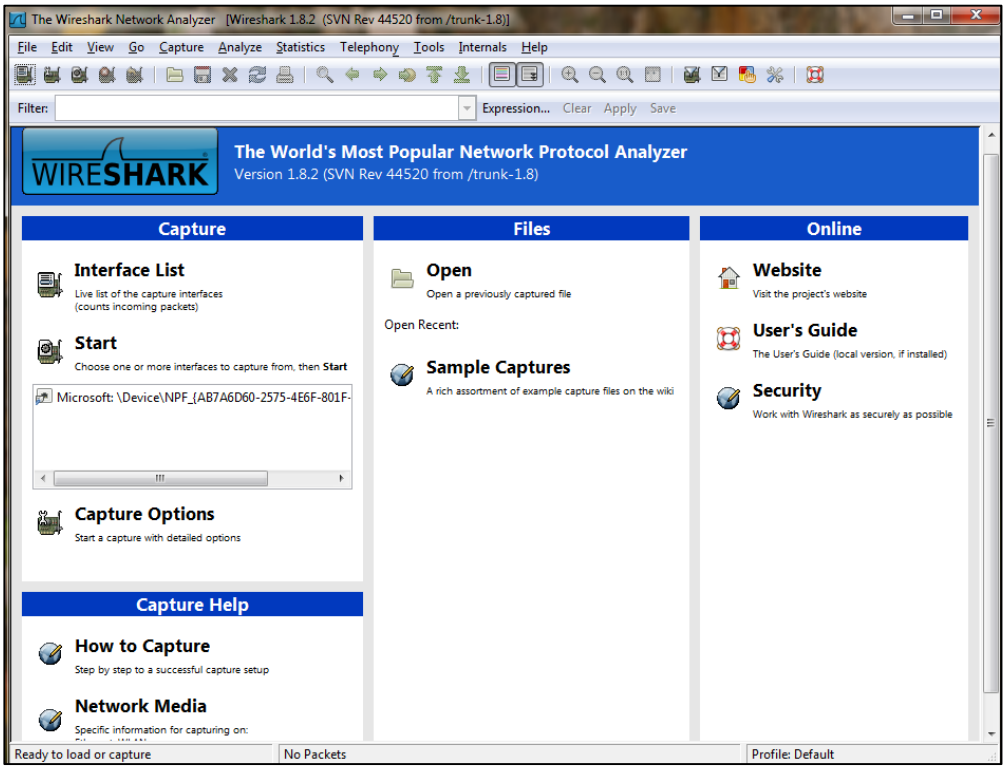


Figura 19. Tela inicial do programa *Wireshark.*
Fonte: Autoria própria.

2.4.3 IPERF

É uma ferramenta multi-plataforma que pode ser executado em qualquer rede. Ele pode ser usado para comparação de equipamentos de rede com e sem fio de uma maneira imparcial. Permitindo que seja medida a largura de banda e a qualidade de uma conexão de rede. Ele possibilita customizar a quantidade de conexões simultâneas e o tamanho dos pacotes a serem disparados. O funcionamento consiste em uma rede formada por dois hosts executando o *Iperf* sendo um deles o cliente o qual irá gerar o tráfego e o outro o servidor o qual recebe as conexões e os pacotes.

Abaixo na figura 20 logo abaixo verificamos a tela onde é executado o programa *Iperf* no papel de servidor:

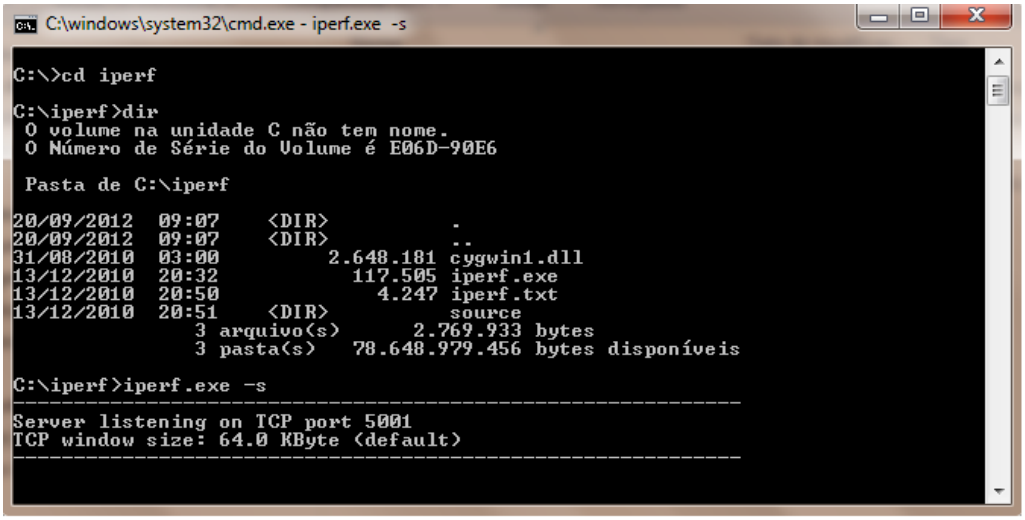


Figura 20. Programa *Iperf* executando a tarefa de servidor.
Fonte: Autoria própria.

Abaixo é explicado o significado dos principais comandos no IPERF:

-c Inicia o Iperf como Cliente *(client)*

-s Inicia o Iperf como Servidor *(server)*

-p Especifica a porta a ser utilizada

-P Especifica o número de conexões paralelas

-d Realiza o teste bidirecional simultaneamente *(dualtest)*

-i Exibe o status a cada "x" segundos

-f Especifica o formato das informações: *Kbits, Mbits, KBytes, MBytes*

-t Especifica o tempo de transmissão (*default* 10 segundos)

2.4.4 JPERF

É o já conhecido *Iperf* com uma roupagem gráfica utilizando *JAVA*. Ele dispõe exatamente das mesmas funcionalidades do seu antecessor. Ele agrega comandos mais intuitivos e fáceis de utilizar além de exibir as estatísticas de forma gráfica. O funcionamento consiste em uma rede formada por dois hosts que possua instalado o *Java Runtime Environment* que é utilizado para executar o *jperf*. Em um dos lados da rede um dos micros

fará o papel de cliente o qual irá gerar o tráfego e do outro lado o segundo que irá ser o servidor o qual recebe as conexões e os pacotes.

A sintaxe de linguagem é exatamente a mesma já apresentada para o *Iperf*. Abaixo na figura 21 é observada a tela onde é executado *Jperf* para o lado servidor:

Figura 21. Programa *Jperf* executando a tarefa de servidor.
Fonte: Autoria própria.

3 PROCEDIMENTOS EXPERIMENTAIS

Os testes ocorreram em equipamentos reais, no laboratório de redes da UTFPR Bloco V. Os equipamentos utilizados foram os seguintes:

- 11 switchs cisco modelo 2960;
- 02 switchs cisco camada 3, modelo Cisco Catalyst 8500;
- 01 switch cisco camada 3, modelo 2948G;
- 03 roteadores cisco, modelo 2811;
- 02 computadores utilizando o sistema operacional BackTrack;
- 04 computadores utilizando o sistema operacional Ubuntu;
- 02 computador utilizando o sistema operacional Windows XP Professional.

A configuração lógica da rede foi organizada da seguinte maneira:

- Separou-se a rede em 03 Vlans:

10 Vlan Dados

20 Vlan Voz

30 Vlan Gerência

- Foi escolhido para utilização nos switches o endereço 200.1.1.0 com máscara de sub-rede /28, para que não houvesse desperdício de *IP´s* de uma máscara /24. Abaixo segue as tabelas de cálculo dos endereços de rede, broadcast, máscara e *IP´s* válidos para cada uma das sub-redes:

0	Hosts
0	Rede

Quadro 1. Identificação por cores dos elementos lógicos dos próximos quadros.
Fonte: Autoria própria.

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	
				200.	1.	1.	0	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	15	Broadcast
200.	1.	1.	1 ~	200.	1.	1.	14	IP´s Válidos

Quadro 2. Cálculo das sub-redes – Parte 1.
Fonte: Autoria própria.

0	0	0	1	0	0	0	0	
				200.	1.	1.	16	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	31	Broadcast
200.	1.	1.	17 ~	200.	1.	1.	30	IP´s Válidos
0	0	1	0	0	0	0	0	
				200.	1.	1.	32	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	47	Broadcast
200.	1.	1.	33 ~	200.	1.	1.	46	IP´s Válidos
0	0	1	1	0	0	0	0	
				200.	1.	1.	48	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	63	Broadcast
200.	1.	1.	49~	200.	1.	1.	62	IP´s Válidos
0	1	0	0	0	0	0	0	
				200.	1.	1.	64	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	79	Broadcast
200.	1.	1.	65 ~	200.	1.	1.	78	IP´s Válidos
0	1	0	1	0	0	0	0	
				200.	1.	1.	80	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	95	Broadcast
200.	1.	1.	81 ~	200.	1.	1.	94	IP´s Válidos
0	1	1	0	0	0	0	0	
				200.	1.	1.	96	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	111	Broadcast
200.	1.	1.	97 ~	200.	1.	1.	110	IP´s Válidos
0	1	1	1	0	0	0	0	
				200.	1.	1.	112	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	127	Broadcast
200.	1.	1.	113 ~	200.	1.	1.	126	IP´s Válidos

Quadro 3. Cálculo das sub-redes – Parte 2.
Fonte: Autoria própria.

1	0	0	0	0	0	0	0	
				200.	1.	1.	128	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	143	Broadcast
200.	1.	1.	129 ~	200.	1.	1.	142	IP´s Válidos
1	0	0	1	0	0	0	0	
				200.	1.	1.	144	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	159	Broadcast
200.	1.	1.	145 ~	200.	1.	1.	158	IP´s Válidos
1	0	1	0	0	0	0	0	
				200.	1.	1.	160	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	175	Broadcast
200.	1.	1.	161 ~	200.	1.	1.	174	IP´s Válidos
1	0	1	1	0	0	0	0	
				200.	1.	1.	176	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	191	Broadcast
200.	1.	1.	177 ~	200.	1.	1.	190	IP´s Válidos
1	1	0	0	0	0	0	0	
				200.	1.	1.	192	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	207	Broadcast
200.	1.	1.	193 ~	200.	1.	1.	206	IP´s Válidos
1	1	0	1	0	0	0	0	
				200.	1.	1.	208	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	223	Broadcast
200.	1.	1.	209 ~	200.	1.	1.	222	IP´s Válidos
1	1	1	0	0	0	0	0	
				200.	1.	1.	224	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	239	Broadcast
200.	1.	1.	225 ~	200.	1.	1.	238	IP´s Válidos
1	1	1	1	0	0	0	0	
				200.	1.	1.	240	Rede
				255.	255.	255.	240	Mácara
				200.	1.	1.	255	Broadcast
200.	1.	1.	241 ~	200.	1.	1.	254	IP´s Válidos

Quadro 4. Cálculo das sub-redes – Parte 3.
Fonte: Autoria própria.

- Foi escolhido para utilização nos roteadores os endereços 200.1.10.0 e 200.1.20.0 ambos com máscara de sub-rede /30, para que não houvesse desperdício de *IP´s* caso fosse utilizado uma máscara /32. Abaixo segue as tabelas de cálculo dos endereços de rede, broadcast, máscara e *IP´s* válidos para cada uma das sub-redes:

0	0	0	0	0	0	0	0	
				200.	1.	10.	0	Rede
				255.	255.	255.	252	Mácara
				200.	1.	10.	3	Broadcast
200.	1.	10.	1 ~	200.	1.	10.	2	IP´s Válidos
0	0	0	0	0	0	0	0	
				200.	1.	20.	0	Rede
				255.	255.	255.	252	Mácara
				200.	1.	20.	3	Broadcast
200.	1.	20.	1 ~	200.	1.	20.	2	IP´s Válidos

u
lo das sub-redes – Parte 4.
Fonte: Autoria própria.

3.1 EXPERIMENTO Nº 1:

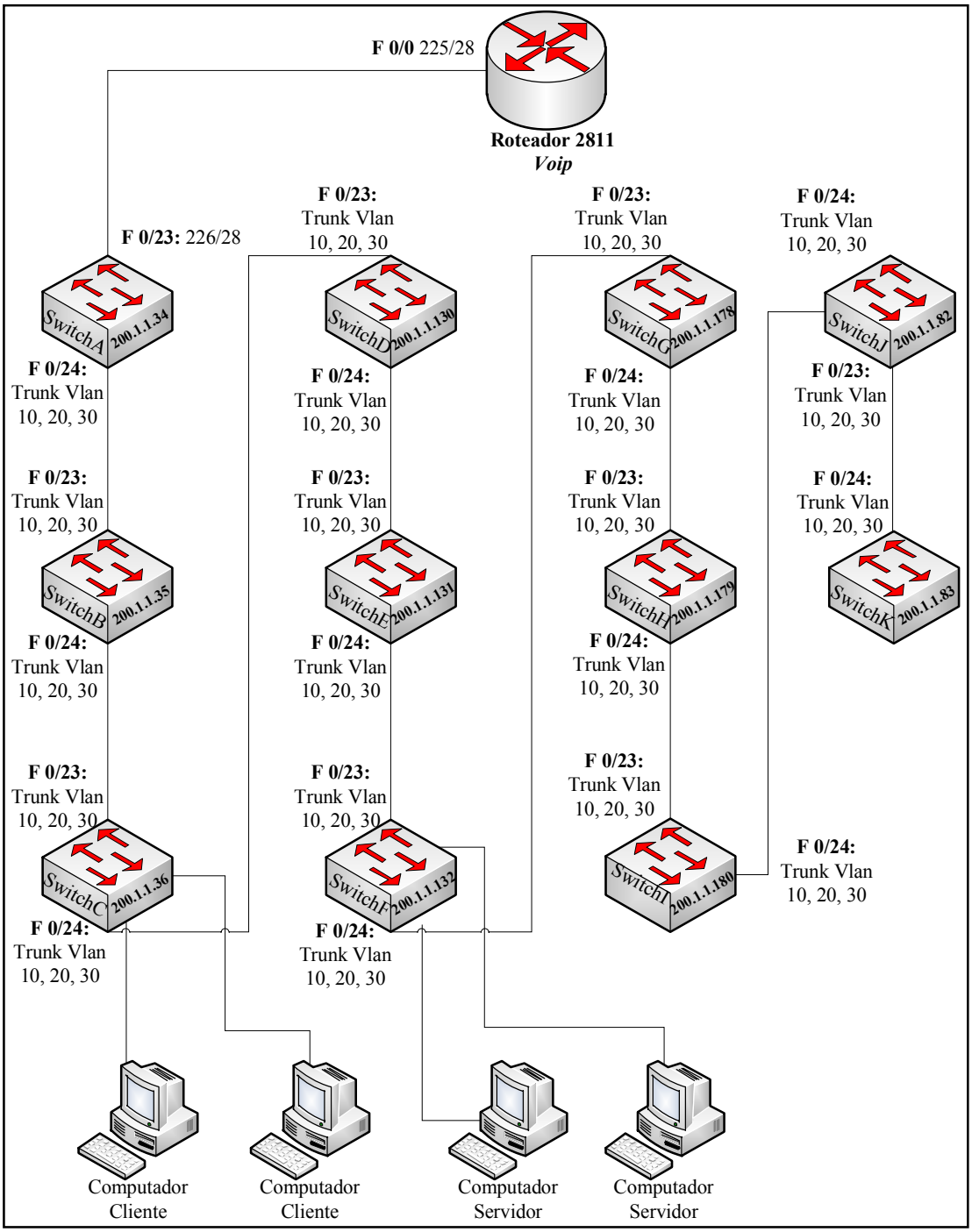


Figura 22. Toplogia do cenário nº 1.
Fonte: Autoria própria.

A figura 22 representa o cenário topológico número 1, o qual possuiu em sua estrutura física um total de onze switches ligados através de cascata e mais um roteador.

3.1.1 Procedimentos realizados nos equipamentos:

- Foi configurado em cada um dos switches 03 *VLANs*: Dados (10), Voz (20) e Gerência (30). Também foi adicionado a cada um dos *switches* um *IP* de gerência conforme ilustra a figura 22. Na figura 23 logo abaixo, os comandos executados na console dos *switches* para criação de *VLANs* e atribuição delas em portas específicas:

```
SwitchC >enable
SwitchC #conf term
SwitchC (config)#vlan 10
SwitchC (config-vlan)#name dados
SwitchC (config-vlan)#exit
SwitchC (config)#vlan 20
SwitchC (config-vlan)#name voz
SwitchC (config-vlan)#exit
SwitchC (config)#vlan 30
SwitchC (config-vlan)#name gerencia
SwitchC (config-vlan)#exit
SwitchC (config)#interface range fastEthernet 0/3-7
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 10
SwitchC (config-if-range)#exit
SwitchC (config)#interface range fastEthernet 0/8-11
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 20
SwitchC (config-if-range)#exit
SwitchC (config)#interface range fastEthernet 0/12-15
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 30
SwitchC (config-if-range)#exit
```

Figura 23. Console do SwitchC.
Fonte: Autoria própria.

- Foram deixados os switches executando o protocolo *STP* (*Spanning Tree Protocol)* o qual exerce um papel importante de evitar que ocorram *loops* na Camada de

Enlace para a execução de um dos testes. Esta opção já vem pré-configurada nos switches Cisco.

- Num outro momento foi desabilitado em todos os equipamentos o *STP* para que fosse possível realizar uma análise do impacto de um *loop* na rede. Na figura 24 logo abaixo, exibe os comandos executados na console do SwitchF:

```
SwitchF >enable
SwitchF #conf term
SwitchF (config)#no spanning-tree vlan 10 root primary
SwitchF (config)#no spanning-tree vlan 20 root primary
SwitchF (config)#no spanning-tree vlan 30 root primary
SwitchF (config)#no spanning-tree vlan 1 root primary
```

Figura 24. Console do SwitchF.
Fonte: Autoria própria.

- Foram utilizados para a execução dos testes 04 (quatro) computadores dotados do sistema operacional Ubuntu. Nestes foi utilizado os seguintes programas: *Iperf* e *Jperf*. Através destes *softwares* foi possível gerar tráfego *TCP*, análise de largura de banda e atraso de pacotes. Onde cada extremidade exercia separadamente dois a dois os papéis de cliente e servidor. Na figura 25 logo abaixo, exibe os comandos executados para a realização dos testes:

Micros Servidores:

iperf –s –i 5 –p 4001 –f m (Voz)

iperf –s –i 5 –p 4005 –f m (Dados)

Micros Clientes:

iperf –c 200.1.1.50 –i 5 –p 4001 –f m –P 1 –t 3600 (Voz - Uma conexão)

iperf –c 200.1.1.50 –i 5 –p 4005 –f m –P 10 –t 3600 (Dados - Dez conexões simultâneas)

Figura 25. Linha de comandos executadas nos programas *Iperf* e *Jperf*.
Fonte: Autoria própria.

- Foram configurados nos *switches* o *QoS*, de maneira que fosse dado prioridade para comunicação de voz. Na figura 26 logo abaixo, exibe os comandos executados na console do SwitchC:

```
SwitchC >enable
SwitchC #conf term
SwitchC (config)#mls qos
SwitchC (config)#interface range fastEthernet 0/3-7
SwitchC (config-if-range)#mls qos
SwitchC (config-if-range)#mls qos cos 1
SwitchC (config-if-range)#exit
SwitchC (config)#interface range fastEthernet 0/8-11
SwitchC (config-if-range)#mls qos
SwitchC (config-if-range)#mls qos cos 5
SwitchC (config-if-range)#exit
SwitchC (config)#interface gigabitEthernet 0/1
SwitchC (config-if)#switchport mode trunk
SwitchC (config-if)#switchport trunk allowed vlan all
SwitchC (config-if)#mls qos
SwitchC (config-if)#mls qos trust cos
SwitchC (config-if)#exit
SwitchC (config)#interface gigabitEthernet 0/2
SwitchC (config-if)#switchport mode trunk
SwitchC (config-if)#switchport trunk allowed vlan all
SwitchC (config-if)#mls qos
SwitchC (config-if)#mls qos trust cos
SwitchC (config-if)#exit
```

Figura 26. Console do SwitchC.
Fonte: Autoria própria.

- Foi realizado nos switches onde estavam conectados os computadores servidores, o espelhamento de portas. Esta ação foi necessária para que fosse possível realizar uma depuração e o monitoramento do tráfego que ocorriam nas mesmas. Utilizamos para tanto o programa *Wireshark* que é um *software sniffer* que analisa de forma eficiente os protocolos e

demais informações sobre o tráfego. Na figura 27 logo abaixo, exibe os comandos executados nos *switches* para espelhar portas nas duas *VLANs* (Dados e Voz):

```
SwitchF >enable
SwitchF #conf term
SwitchF (config)#no monitor session 1
SwitchF (config)#monitor session 1 source interface fastEthernet 0/3 rx
(porta ligada no computador que roda o Wireshark)
SwitchF (config)#monitor session 1 destination interface fastEthernet 0/4
(porta que está conectada ao computador servidor do iperf dados)
SwitchF (config)#monitor session 2 source interface fastEthernet 0/8 rx
(porta ligada no computador que roda o Wireshark)
SwitchF (config)#monitor session 2 destination interface fastEthernet 0/9
(porta que está conectada ao computador servidor do iperf voz)
```

Figura 27. Console do SwitchF.
Fonte: Autoria própria.

3.1.2 Testes realizados nos equipamentos:

- Testes de tráfego entre os switches C e F, utilizando as Vlans da seguinte maneira: Foi utilizado o *software Iperf* para gerar tráfego. Foi gerado na *VLAN* Dados um fluxo com dez conexões simultâneas. Já em relação à *VLAN* de Voz foi gerando apenas um fluxo de dados. Os resultados obtidos através do programa *Jperf* e por meio do comando *Ping* (*Packet Internet Grouper* - Procurador de Pacotes da Internet) na console dos computadores serão expostos logo a seguir pelas figuras: 28 e 29 no diz respeito a *Vlan* Dados e figuras 32 e 33 no que diz respeito à *Vlan* Voz.

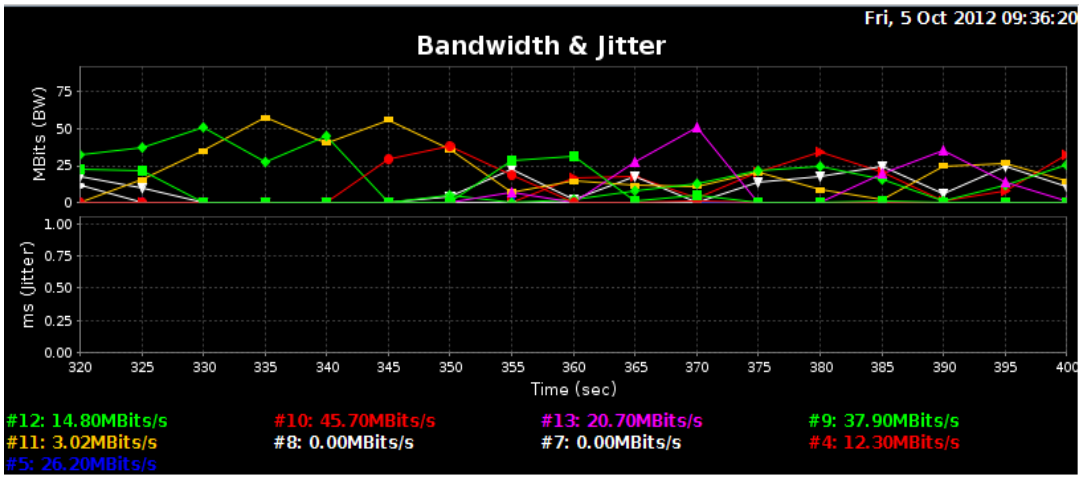


Figura 28. Programa Jperf executando a tarefa de servidor.
Fonte: Autoria própria.

A figura 28 apresenta os resultados da *VLAN* Dados. Este teste representa um cenário sem a utilização de qualquer regra de QoS. Onde podemos observar que cada linha representaria um ramo de telefones *Voip* que estariam concorrendo entre si pela banda disponível (*Best-Effort* – Melhor esforço). É possível observar que em determinado momento as linhas identificadas por #7 e #8 não enviam dados ficando com taxas de transmissão em 0.00MBits/s.

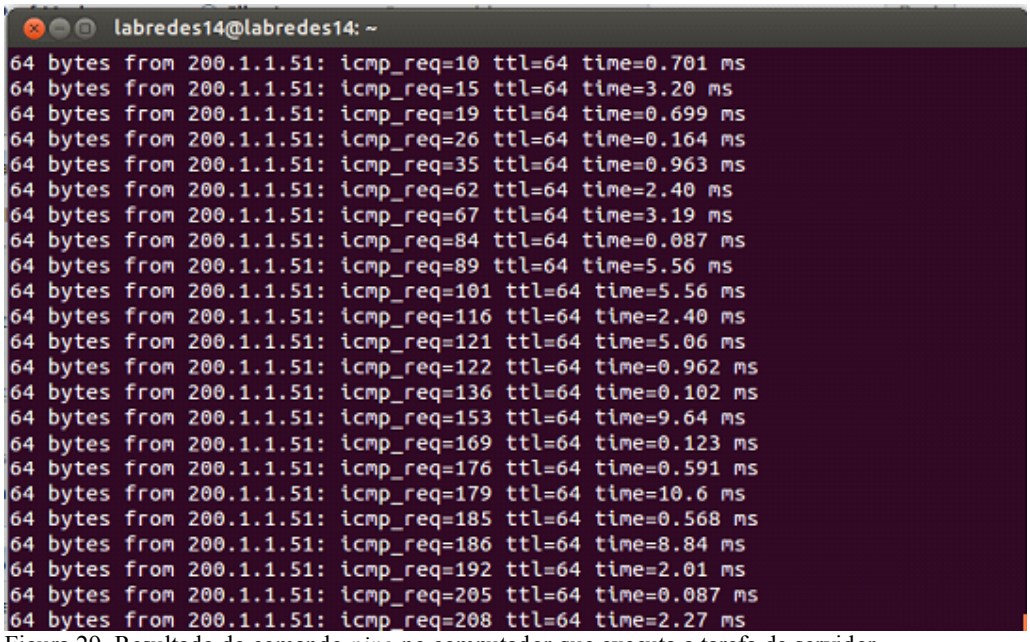


Figura 29. Resultado do comando *ping* no computador que executa a tarefa de servidor.
Fonte: Autoria própria.

A figura 29 apresenta os resultados do comando *ping,* através dele é possível obter as seguintes informações: quantidade de pacotes perdidos, ping (tempo de ida e volta de um pacote) e *Jitter* (variação estatística do atraso dos pacotes ao longo do tempo). Foi observado que a variação do tempo de ida e volta dos pacotes (*Jitter*) não é constante assim como ocorre na figura 28, cada conexão fica concorrendo pela banda disponível, o resultado é uma variação da ordem de 270% entre cada uma das instâncias. Este teste representa da mesma maneira que o da figura 28, um cenário sem a utilização de qualquer regra de QoS.

Ao utilizarmos as redes de comunicação para tráfego de voz (*VOIP)* este é especialmente suscetível ao comportamento da rede, ou seja, dependendo da perda de pacotes, atraso e o *Jitter* poderá haver degradação significativa a ponto de ser inaceitável para o usuário médio. O *VOIP* tipicamente tolera atrasos de até 150 ms antes que haja degradação na comunicação. (SYSTEMS INC, 2012).

Abaixo na figura 30 é exposta a recomendação da *ITU* (*International Telecommunication Union* - União Internacional de Telecomunicações) G.114, a qual define três faixas de atraso:

Range in Milliseconds	Description
0-150	Acceptable for most user applications.
150-400	Acceptable provided that administrators are aware of the transmission time and the impact it has on the transmission quality of user applications.
Above 400	Unacceptable for general network planning purposes. However, it is recognized that in some exceptional cases this limit is exceeded.

Figura 30: Recomendação G.114 da ITU.
Fonte: SYSTEMS INC, Cisco. 2012

O emprego de *QoS* em uma rede normalmente é necessário para garantir o desempenho de aplicações específicas. A qualidade de serviço incide justamente na capacidade de prestar serviços previsíveis, mensuráveis e às vezes garantidos por gerenciar parâmetros largura de banda, atraso, *Jitter* e perda em uma rede. (SYSTEMS INC, 2012).

Abaixo na figura 31 é exibido as 11 classes de tráfego que podem ser considerados críticos para a maioria das redes coorporativas:

Application	Layer 3 Classification			Layer 2 CoS/MPLS EXP	
	IPP	PHB	DSCP		
IP Routing	6	CS6	48	6	
Voice	5	EF	46	5	
Interactive Video	4	AF41	34	4	
Streaming-Video	4	CS4	32	4	
Locally-Defined Mission-Critical Data (see note below)	3	—	25	3	
Call-Signaling (see note below)	3	AF31/CS3	26/24	3	
Transactional Data	2	AF21	18	2	
Network Management	2	CS2	16	2	
Bulk Data	1	AF11	10	1	
Scavenger	1	CS1	8	1	
Best Effort	0	0	0	0	

Figura 31: Cisco *QoS* linha de base / *Marketing* Técnico (interino) Classificação e Recomendações Marcação
Fonte: SYSTEMS INC, Cisco. 2012.

A seguir na figura 32 e 33 apresentam-se os resultados da *VLAN* Voz. Os testes realizados para estes elementos, foram com o emprego de *QoS*. Utilizamos nesta *VLAN* a classe de serviço (*COS - Class of Service*) de número 5 (cinco) conforme recomendação de marcação contida na figura 31.

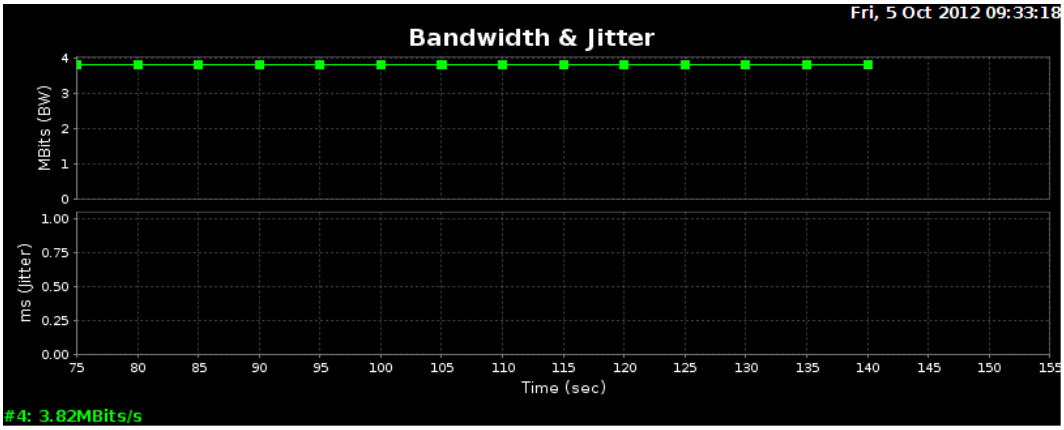


Figura 32. Programa Jperf executando a tarefa de servidor.
Fonte: Autoria própria.

Na figura 32 pode-se observar que a linha identificada por #4 mantêm-se constante ao longo do tempo, com taxa de transmissão de 3,83*MBytis/s*. A figura 33 também diferencia-se dos resultados iniciais que não fazia uso do *QoS*. Ao analisar os resultados do comando *ping* observamos que a variação do tempo de ida e volta dos pacotes (*Jitter*) é mais constante, variando apenas cerca de 9%.

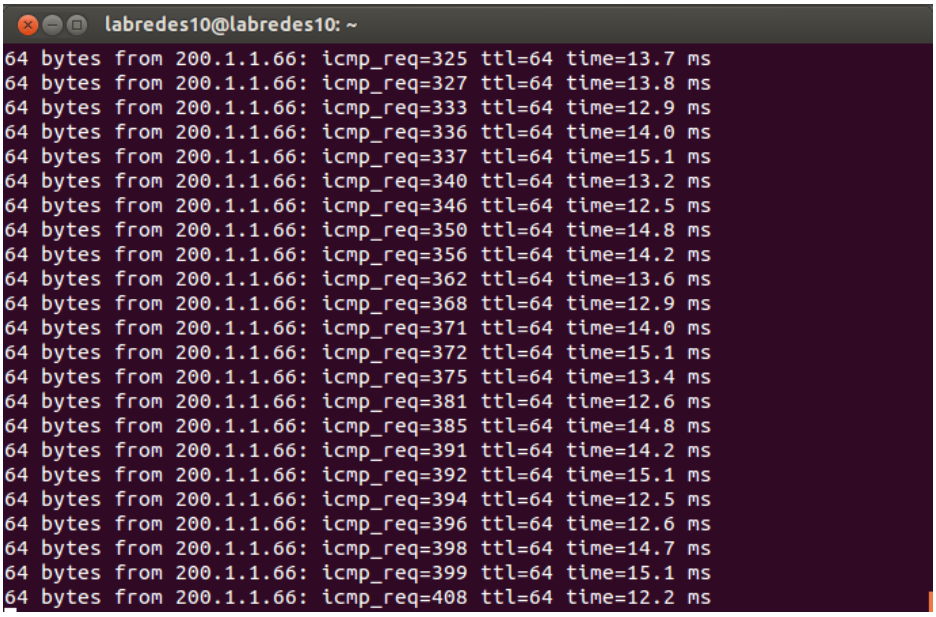


Figura 33. Resultado do comando ping no computador que executa a tarefa de servidor.
Fonte: Autoria própria.

Na figura 34 pode-se observar que os requisitos para obter uma comunicação *Voip* aceitável são basicamente 3 (três): O *Jitter* deve ser no máximo 30ms ou menor, a latência da rede deve ser no máximo 150ms ou menor e a perda de pacotes deve ser menos de 1%.

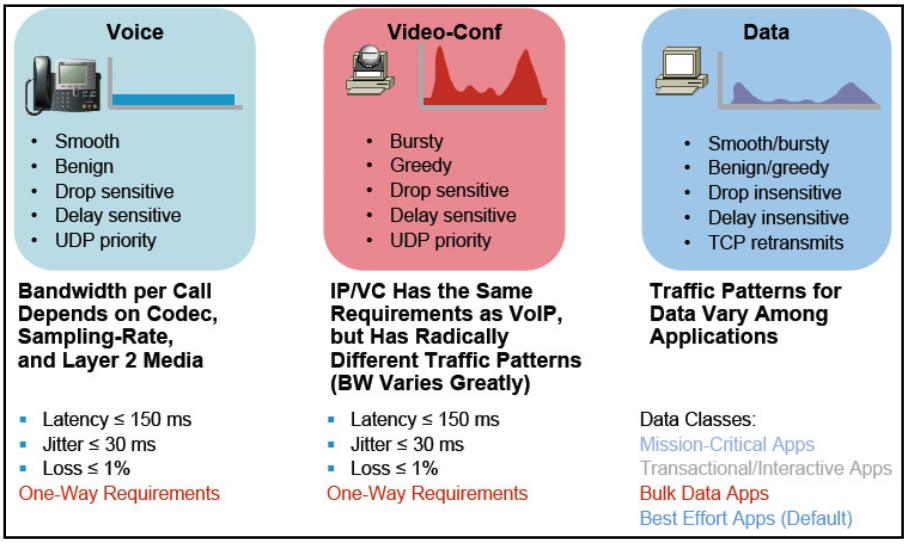


Figura 34. Perfil de Tráfego x Requisitos de *QoS*.
Fonte: BIANCHINI, Alessandro C. 2012.

Nas próximas figuras podem ser observados os resultados obtidos pelo *software Wireshark* que capturou o tráfego em cada uma das portas onde estavam ligados os computadores servidores para cada *Vlan*. Através da análise destes dados será possível verificar se houve ou não perda de pacotes em cada *Vlan* separadamente.

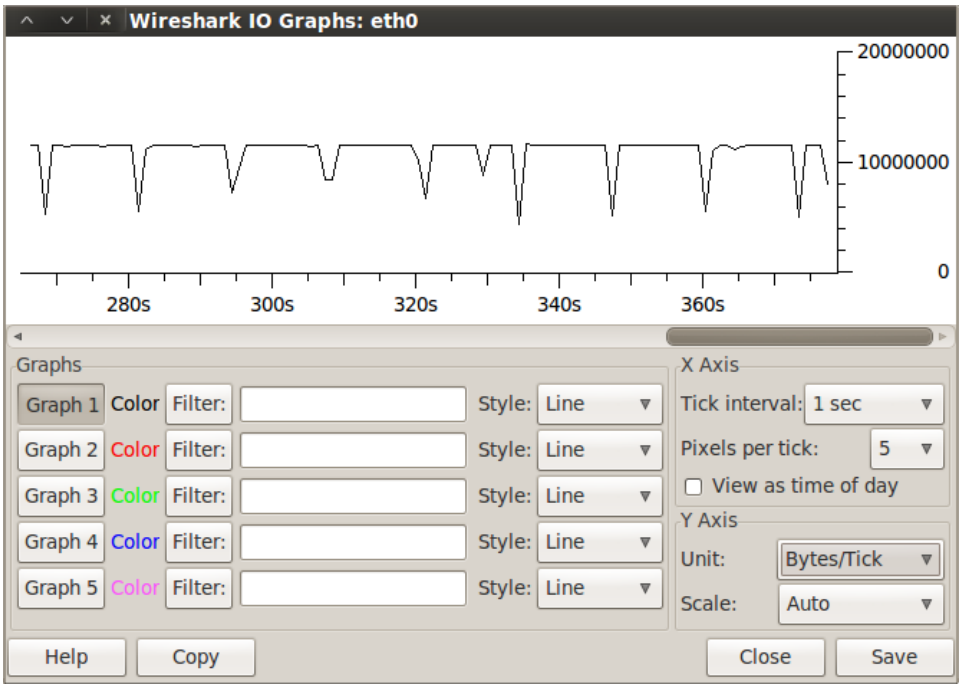


Figura 35. Análise da variação do tráfego de rede pelo tempo.(dados)
Fonte: Autoria própria.

Na figura 35 pode-se observar em forma de gráfico os dados recebidos pelo lado do servidor *Jperf,* para a *Vlan* de Dados, que como já visto não possuí nenhum tipo de *QoS* implementado além de estar recebendo dados de 10 fluxos simultâneos do outro computador cliente:

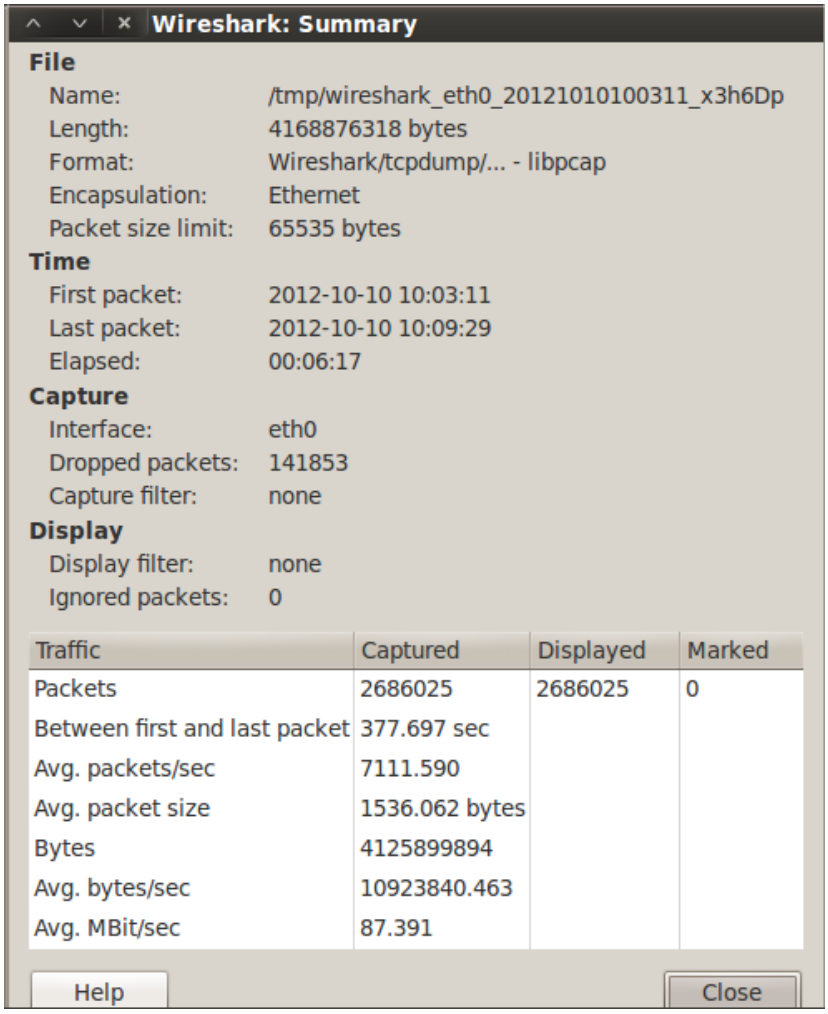


Figura 36. Análise do tráfego de rede. (dados)
Fonte: Autoria própria.

Na figura 36 pode-se observar, em forma de estatística que houve pacotes descartados e levando-se em consideração as variações das linhas do gráfico na figura 35, que dizem respeito à mesma análise. As depressões geradas na figura 35 representavam os pacotes que foram descartados ao longo da transmissão. E que a perda chegou a representar exatos 5,28% de todos os pacotes analisados.

A seguir na figura 37 pode-se observar em forma de gráfico os dados recebidos pelo lado do servidor *Jperf,* para a *Vlan* de Voz, que como já visto possuí implementado o *QoS* com o campo *Cos = 5* (cinco) conforme recomendação de marcação contida na figura 31. Neste teste foi utilizado apenas um fluxo de dados:

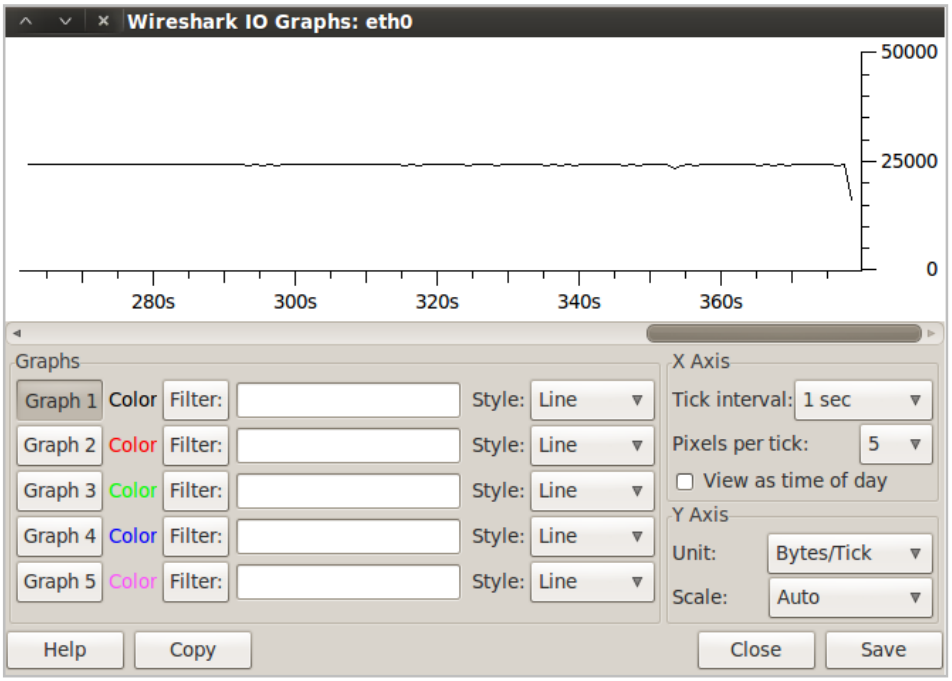


Figura 37. Análise da variação do tráfego de rede pelo tempo. (voz)
Fonte: Autoria própria.

Na figura 37 pode-se observar que o gráfico é completamente diferente do visto na figura 35. É possível notar que quase não há variação na linha que representa a taxa do tráfego recebido, ele mantém-se quase constante.

A seguir na figura 38 pode-se observar em forma de estatística que não houve pacotes descartados. Em comparação com os resultados exibidos pela figura 36 fica evidenciado que a configuração de *QoS* garantiu que nenhum pacote fosse descartado durante a transmissão dos dados.

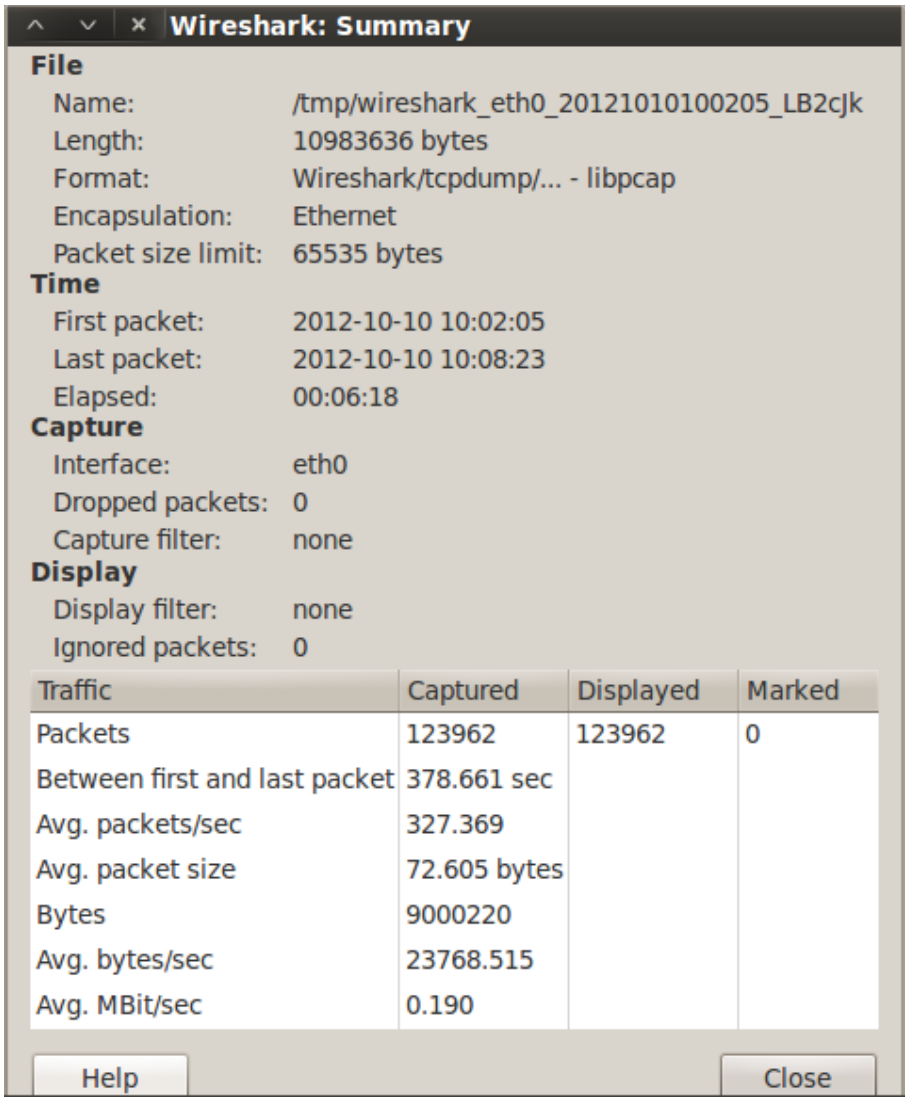


Figura 38. Análise do tráfego de rede. (voz)
Fonte: Autoria própria.

Neste experimento foram realizados testes onde se procurava saber: se havia ou não diferença em realizar *QoS* ao utilizar *VOIP,* qual seria o impacto em relação aos pacotes desta rede e por último mensurar o real impacto em relação aos dois cenários.

Foi observado por meio da análise das figuras geradas em equipamentos reais, porém em um ambiente controlado. Foram feitos testes com *Softphones* no próximo experimento a fim de comprovar na prática se haverá de fato degradação durante a utilização dos equipamentos sob os mesmos ambientes já vistos e analisados neste experimento.

3.2 EXPERIMENTO Nº 2:

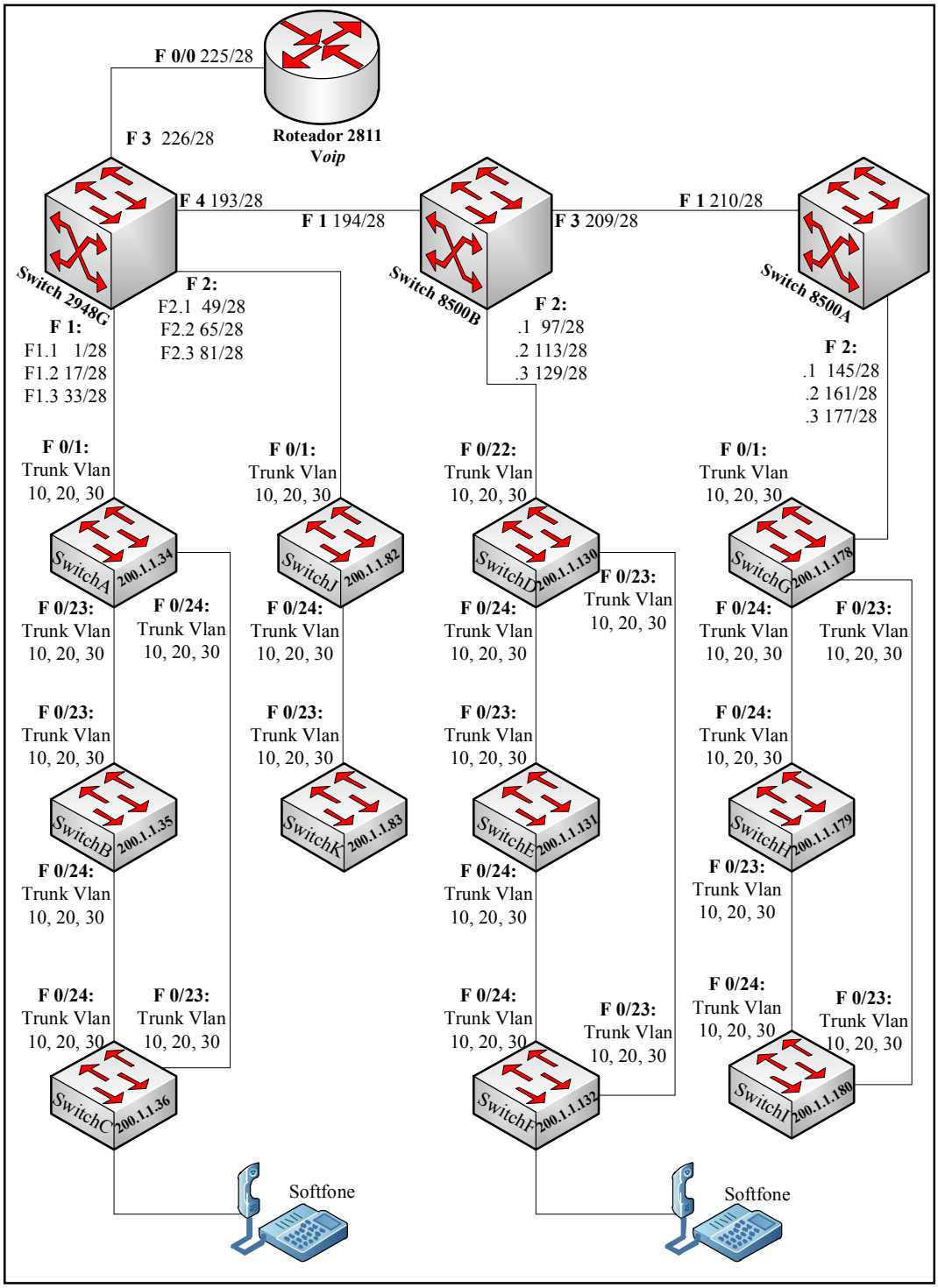


Figura 39. Toplogia do cenário nº 2.
Fonte: Autoria própria.

A figura 39 representa o cenário topológico número 2, o qual possuiu em sua estrutura física um total de: onze switches, três switches camada 3 e um roteador. Os switches

estão executando o protocolo *STP* (*Spanning Tree Protocol)* o qual tem um papel importante de evitar que ocorram loops na Camada de Enlace.

3.2.1 Procedimentos realizados nos equipamentos:

- Foi configurado em cada um dos switches 03 *Vlans*: Dados (10), Voz (20) e Gerência (30). Também foi adicionado a cada um dos *switches* um *IP* de gerência conforme ilustra a figura 39. Na figura 40 logo abaixo, exibe os comandos executados na console dos *switches* para criação de *Vlans* e atribuição delas em portas específicas:

```
SwitchC >enable
SwitchC #conf term
SwitchC (config)#vlan 10
SwitchC (config-vlan)#name dados
SwitchC (config-vlan)#exit
SwitchC (config)#vlan 20
SwitchC (config-vlan)#name voz
SwitchC (config-vlan)#exit
SwitchC (config)#vlan 30
SwitchC (config-vlan)#name gerencia
SwitchC (config-vlan)#exit
SwitchC (config)#interface range fastEthernet 0/3-7
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 10
SwitchC (config-if-range)#exit
SwitchC (config)#interface range fastEthernet 0/8-11
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 20
SwitchC (config-if-range)#exit
SwitchC (config)#interface range fastEthernet 0/12-15
SwitchC (config-if-range)#switchport mode access
SwitchC (config-if-range)#switchport access vlan 30
SwitchC (config-if-range)#exit
```

Figura 40. Console do SwitchC.
Fonte: Autoria própria.

- Foram utilizados para a execução dos testes 02 (dois) computadores dotados do sistema operacional Windows XP Professional. Nestes foram utilizados os seguintes programas: *Softphone Cisco IP Communicator, Iperf* e *Jperf*.

- Foi configurado também no roteador a funcionalidade de distribuição de *IPs* para os *Softphone*s. Na figura 41 logo abaixo os comandos realizados na console do *Cisco 2811 Integrated Services Router*:

```
RouterA >enable
RouterA #conf term
RouterA (config)#interface fastEthernet 0/0
RouterA (config-if)#ip add 192.168.10.1 255.255.255.0
RouterA (config-if)#no shutdown
RouterA (config-if)#exit
RouterA (config)#ip dhcp pool voicelab
RouterA (dhcp-config)#network 192.168.10.0 255.255.255.0
RouterA (dhcp-config)#default-router 192.168.10.1
RouterA (dhcp-config)#option 150 ip 192.168.10.1
RouterA (dhcp-config)#exit
```

Figura 41. Console do RoteadorA.
Fonte: Autoria própria.

- Foi realizado a configuração do *Cisco Unified Communications Manager Express – CME* (é uma aplicação de processamento de chamadas no *software Cisco IOS* que permite que os roteadores Cisco realizem o papel de uma central telefônica). Na figura 42 logo abaixo os comandos realizados na console do *Cisco 2811 Integrated Services Router*:

```
RouterA>enable
RouterA#conf term
RouterA(config)#telephony-service
RouterA(config-telephony)#max-dn 5
RouterA(config-telephony)#max-ephones 5
RouterA(config-telephony)#ip source-address 192.168.10.1 port2000
RouterA(config-telephony)#auto assign 1 to 5
RouterA(config-telephony)#exit
RouterA(config)#ephone-dn 1
RouterA(config-telephony)#number 54001
RouterA(config-telephony)#exit
RouterA(config)#ephone-dn 2
RouterA(config-telephony)#number 54002
RouterA(config-telephony)#exit
RouterA(config)#ephone-dn 3
RouterA(config-telephony)#number 54003
RouterA(config-telephony)#exit
RouterA(config)#ephone 1
RouterA(config-ephone)#mac-address E803.9A46.5374
RouterA(config-ephone)#exit
RouterA(config)#ephone 2
RouterA(config-ephone)#mac-address AA13.BD02.2266
RouterA(config-ephone)#exit
RouterA(config)#ephone 3
RouterA(config-ephone)#mac-address C813.20D6.2320
RouterA(config-ephone)#exit
```

Figura 42. Console do RoteadorA.
Fonte: Autoria própria.

- Foi configurado nos *Softphone*s as opções de: Preferências > Rede > *TFTP Servers* > Endereço do servidor *TFTP*. Esta etapa é necessária visto que os *Softphone*s precisam buscar o firmware e arquivos de configuração. Na figura 43 pode-se visualizar o local onde deverá ser inserido o endereço *IP*:

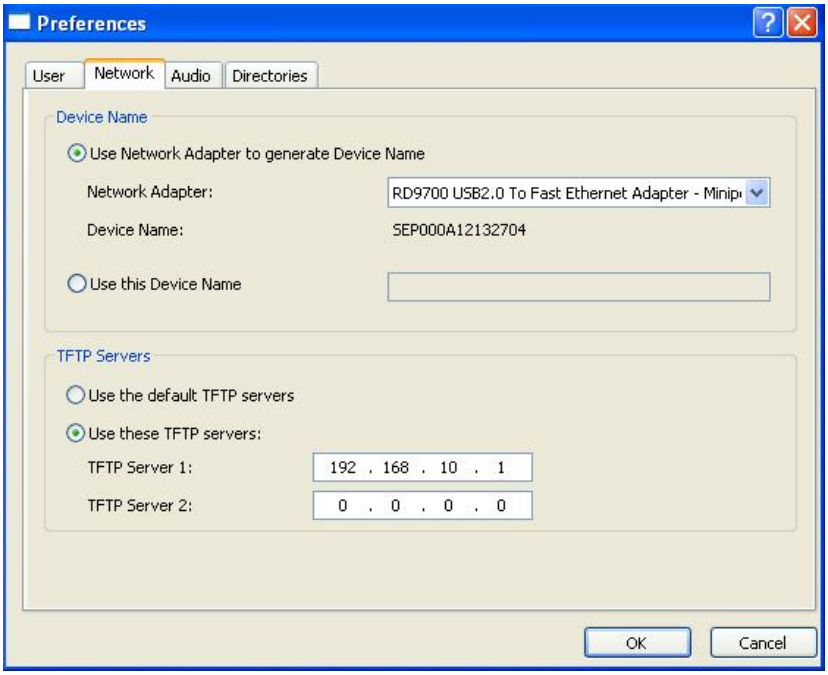


Figura 43. Menu de preferências do Console do *Softphone*.
Fonte: Autoria própria.

3.2.2 Testes Realizados nos Equipamentos:

- Foi realizada uma chamada entre os dois *Softphone*s utilizando a *VLAN* de voz no mesmo instante que era disparado uma grande quantidade de pacotes pela outra *VLAN* de dados. Na figura 44 pode-se visualizar o *Softphone* após vinte minutos de testes. Não foram observados problemas de comunicação que impedissem o bom entendimento da conversa:

Figura 44. *Softphone* durante uma ligação.
Fonte: Autoria própria.

- Foi realizada uma chamada entre os dois *Softphone*s utilizando a *VLAN* de dados no mesmo instante que trafegava uma grande quantidade de pacotes, concorrendo com a comunicação *VOIP*. Foram percebidos alguns problemas durante a execução deste teste: Primeiramente um atraso na voz em relação ao tempo real, em seguida na medida que os pacotes foram aumentando foi percebido uma metalização da voz e algumas acelerações nos diálogos, mais adiante a comunicação foi seriamente comprometida na medida que começou a falhar o som, ouvia-se a voz "picotar" e por fim a comunicação caiu e não foi mais possível restabelecer uma chamada entre os dois *Softphone*s. Na figura 45 pode-se visualizar o os resultados do comando *ping,* através dele é possível obter as seguintes informações: A

quantidade de pacotes perdidos representou cerca de 24%, o tempo de *ping* (latência) mais baixo ficou em 118ms e o *Jitter* (variação estatística do atraso dos pacotes ao longo do tempo) em aproximadamente 176ms.

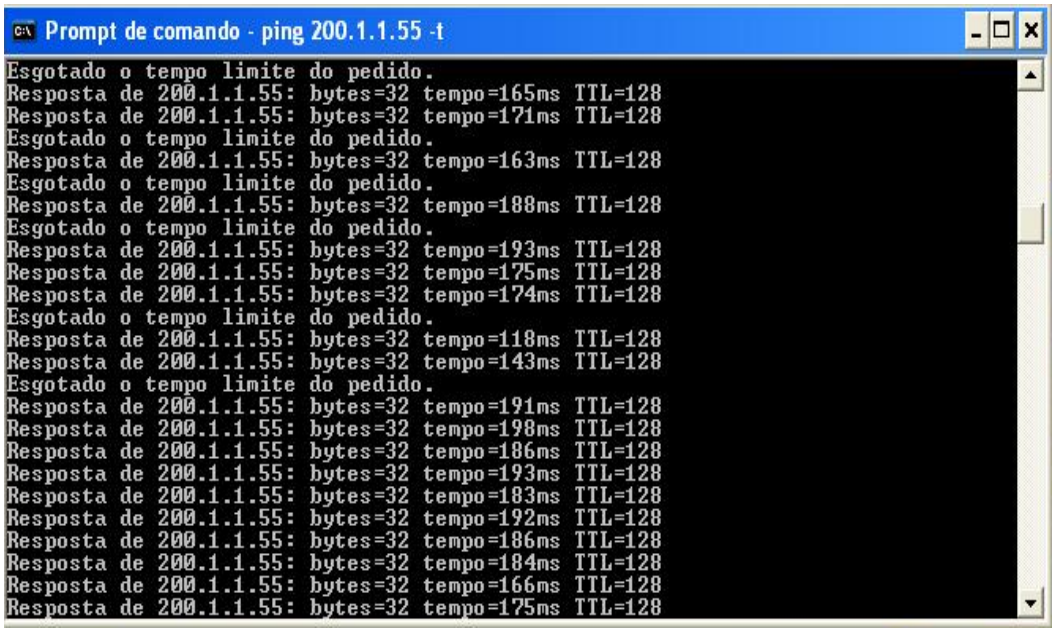


Figura 45. Resultado do comando ping no computador durante a comunicação entre dois *Softphones*.
Fonte: Autoria própria.

4 CONCLUSÃO

Fazendo a análise do tráfego em uma rede de computadores, pôde-se constatar que um ambiente de estresse de tráfego de pacotes ocorre uma diferença entre ambientes sem a aplicação de qualidade de serviço e com a aplicação. Em um ambiente de melhor esforço, os hosts tentam competir pela maior largura de banda ao mesmo tempo, não priorizando determinados fluxos, como o de *Voip*. A utilização de uma comunicação *Voip* neste ambiente mostrou-se inadequado para uma comunicação eficaz (figura 34) gerando falhas e distorções diretamente proporcionais ao aumento do tráfego de fluxos de pacotes concorrentes na rede. O agravo na comunicação ocorreu no momento em que houve um estresse tão grande na rede que ocasionou a queda da conectividade e impossibilidade de restabelecimento.

A aplicação de uma política de *QoS* permite a reserva de recursos na rede e possibilita uma entrega garantida e com baixo *Jitter* (figura 38) permitindo que a comunicação *Voip* não seja afetada. Ao realizarmos uma comunicação *Voip*, compartilhando um meio em que haja estresse de tráfego de pacotes, os equipamentos verificam e priorizam a comunicação marcada como prioritária e descartam na proporção necessária os que possuem marcação inferior. Ao comparar com o primeiro ambiente percebemos que há evidente comprometimento da comunicação *Voip* em cenários onde não existam políticas de *QoS* que priorizem determinados fluxos de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

COLCHER, Sérgio, et al. ***VOIP*** – Voz sobre IP**.** 3ª tiragem. Rio de Janeiro: Elsevier Editora, 2005. 288p.

COMER, Douglas E. **Redes de Computadores e Internet**. 4ª ed. Porto Alegre: Bookman Editora, 2007. 632p.

FILIPPETTI, Marco A. **CCNA 4.1 – Guia Completo de Estudo.** 5ª ed. Florianópolis: Visual Books Editora, 2008. 480p.

ODOM, Wendell. **CCNA ICND1** – Guia Oficial de Certificação do Exame. 3ª tiragem. Rio de Janeiro: Alta Books Editora, 2011. 455p.

ODOM, Wendell. **CCNA ICND2** – Guia Oficial de Certificação do Exame. 2ª ed. Rio de Janeiro: Alta Books Editora, 2008. 490p.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados** – Teoria e aplicações corporativas**.** 5ª tiragem. Rio de Janeiro: Elsevier Editora, 2005. 449p.

TANENBAUM, Andrew S. **Redes de Computadores**. 5ª ed. São Paulo: Pearson Editora, 2011. 582p.

SYSTEMS INC, Cisco. **Hub Cisco 1538 Series**. Disponível em: <http://www.cisco.com/warp/public/752/qrg/cpqrg2.htm#29815>. Acesso em 18/10/2012.

SYSTEMS INC, Cisco. **Cisco Catalyst 2960 Series Switches**. Disponível em: <http://www.cisco.com/en/US/products/ps6406/prod_view_selector.html>. Acesso em 18/10/2012.

SYSTEMS INC, Cisco. **Cisco Integrated Services 2811**. Disponível em: <http://www.cisco.com/en/US/products/ps5881/prod_view_selector.html>. Acesso em 18/10/2012.

SYSTEMS INC, Cisco. **Cisco Unified IP Phone 7941G**. Disponível em: <http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps6513/product_data_sheet0900aecd802ff012.html>. Acesso em 18/10/2012.

SYSTEMS INC, Cisco. **Delay Specifications**. Disponível em: <http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml >. Acesso em 21/10/2012.

SYSTEMS INC, Cisco. **Cisco QoS Baseline/Technical Marketing (Interim) Classification and Marking Recommendations**. Disponível em: <http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html>. Acesso em 21/10/2012.

BIANCHINI, Alessandro C. **Perfil de tráfego x Requisitos de *QoS***. Disponível em: <http://www.alessandrobianchini.com.br/VOIP/Qualidade%20de%20servico.pdf>. Acesso em 21/10/2012.

SYSTEMS INC, Cisco. **Planning for Quality of Service**. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/class/qpm1_1/using_qo/c1plan.htm>. Acesso em 03/10/2012.

SYSTEMS INC, Cisco. **Understanding Delay in Packet Voice Networks**. Disponível em: < http://www.cisco.com/warp/public/788/voip/delay-details.pdf>. Acesso em 18/10/2012.

SYSTEMS INC, Cisco. **Cisco Unified Communications Manager Express Command Reference**. Disponível em: <http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cmeallht.pdf >. Acesso em 27/09/2012.

SYSTEMS INC, Cisco. **IP Addressing and Subnetting for New Users.** Disponível em: < http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml>. Acesso em 15/09/2012.