UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

KELLY CRISTINA SCHULTZ

IMPLEMENTAÇÃO E ANÁLISE DE UMA ESTRUTURA DE REDE, CONTEMPLANDO GERENCIAMENTO, QUALIDADE DE SERVIÇOS E SEGURANÇA

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2013

KELLY CRISTINA SCHULTZ

IMPLEMENTAÇÃO E ANÁLISE DE UMA ESTRUTURA DE REDE, CONTEMPLANDO GERENCIAMENTO, QUALIDADE DE SERVIÇOS E SEGURANÇA

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Conclusão de Curso 2, do Curso Superior de Bacharelado em Sistemas de Informação, do Departamento Acadêmico de Informática da Universidade Tecnológica Federal do Paraná, como requisito parcial para obtenção do título de Bacharel.
Orientador: Prof. Fabiano Scriptore de Carvalho. Msc.

CURITIBA
2013

AGRADECIMENTOS

Quero agradecer primeiramente a Deus por ter me iluminado e ajudado a dar forças nessa caminhada até aqui.

Quero agradecer a milha família, principalmente meus pais, Cintia e Luis, por ter me ensinado a ser o que sou hoje e ter me motivado e incentivado a sempre batalhar pelo meu futuro. A minha avó Maria Helena por todos esses anos de faculdade ter me levado e buscado sempre, para me ajudar nesse período de estudos.

Ao meu namorado Gabriel, que sempre esteve ao meu lado nos momentos difíceis e cansativos da realização desse trabalho e que em todas as vezes que achei que não iria conseguir, ele me deu forças e acreditou em mim.

E ao meu orientador Prof. Fabiano Scriptore de Carvalho, que sem ele não conseguiria terminar esse trabalho, pelo sua dedicação, apoio e por ter disponibilizado o laboratório e todos os equipamentos necessários.

RESUMO

SCHULTZ, Kelly C. **Implementação e análise de uma estrutura de rede, contemplando gerenciamento, qualidade de serviço e segurança**. 2013. 83 folhas. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Este trabalho tem como objetivo a implementação e análise de uma estrutura de redes de computadores visando a segurança, qualidade de serviços e gerenciamento. Visto que partes das redes locais são implementadas sem um planejamento adequado, juntamente com o aumento da demanda maiores taxas de transmissões para o tráfego de redes e o número crescente de ataques, torna-se necessária a configuração e manutenção de ferramentas que possam deixá-las mais seguras, confiáveis e não suscetíveis a falhas. O projeto visa também, a implantação de diretivas de qualidade de serviços para priorizar diferentes tipos de tráfegos, como dados e voz. Depois de implementada a estrutura, foi instalado e configurado um sistema de gerencia para a manutenção e suporte da rede.

Palavras-chave: Vlans, qualidade de serviço, gerenciamento, segurança.

ABSTRACT

SCHULTZ, Kelly C. **Implementation and analysis of a network structure, contemplating security, quality of service and networks management.** 2013. 83 pages. Course Work Conclusion (Bachelor of Information Systems) - Federal Technological University of Paraná. Curitiba, 2013.

This work aims the implementation and analysis of a network structure, contemplating security, quality of service and networks management. As that parts of local networks are implemented without a proper planning, connected with growing demand of bands more large for network traffics and growing number of attacks, necessitates a configuration and maintenance of tools to make them more safety, reliable and not susceptible to failures. The project also aims the implementation of quality of service guidelines to priorize different kinds of traffic, like data and voice. After the structure be implemented, will be installed and configured a management system to maintenance and network support.

Keywords: Vlans, quality of service, management, security.

LISTA DE FIGURAS

LISTA DE SIGLAS

ACL	Access List
ASA	Adaptative Security Appliance
ASDM	Adaptive Security Device Manager
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DDoS	Distributed Denial of Service
DHCP	Dynamic host configuration protocol
DiffServ	Differentiated Services
DMZ	DeMilitarized Zone
DoS	Denial-of-Service Attack
FIFO	First In First Out
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IntServ	Integrated Services
IP	Internet Protocol
LAN	Local Area Networks
MAC	Media Acess Control
MIB	Management Information Base
QoS	Quality of Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Networks
VoIP	Voice over IP

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia e o baixo custo dos equipamentos, não somente as grandes empresas e escritórios possuem redes de computadores, mas as pessoas estão começando a implementar redes dentro da própria casa ou pequenos estabelecimentos (STALLINGS, 2005). O proprietário de uma rede de pequeno porte normalmente não se preocupa com quesitos de gerenciamento, qualidade de serviço e segurança, com isso cria uma rede sem um planejamento prévio. À medida que a rede vai aumentando, cresce de forma desordenada, continuando sem planejamento e sem um controle de segurança podendo ocorrer ataques como: acesso a informações confidenciais, propagação de vírus de computadores e propagação de falsos IPs (*Internet Protocol*).

Uma rede local é a interconexão de diversos dispositivos em uma rede de computadores que concede um meio de troca de informações entre esses dispositivos (STALLINGS, 2005).

Com o uso de computadores e o surgimento de sistemas distribuídos e do transporte de dados por meio de redes e recursos de comunicação, tornou-se clara a necessidade de ferramentas de segurança que protegessem as informações armazenadas no computador (STALLINGS, 2005). Um ataque é caracterizado pela realização de uma ameaça intencional (SOARES; LEMOS; COLCHER, 1995). Alguns tipos de ataques comuns são: o *spoofing* de DNS, interrupção de serviços e modificação de informações importantes.

Atualmente as informações que estão sendo trafegadas nas redes de computadores não englobam somente dados, mas também voz e vídeo. Para que uma infraestrutura de redes possa utilizar uma aplicação de Voz sobre IP (VoIP), por exemplo, é necessário fazer uma classificação dos dados que estão sendo transmitidos, para que alguns fluxos possam ter prioridade. É necessário a aplicação de uma política de Qualidade de Serviço (QoS) para que os serviços possam ficar disponíveis. Por exemplo, se uma empresa deseja realizar uma videoconferência, a rede deve possuir uma política para que não haja um retardo ou um *jitter*[1] considerável.

O gerenciamento da rede deve ser considerado tanto quanto o projeto da rede (BIRKNER, 2003). Com isso, não basta somente implementar uma rede conforme a metodologia desejada sem ter ferramentas para fazer o gerenciamento da mesma. Com as

[1] "A variação (isto é, o desvio padrão) nos tempos de chegada de pacotes" (TANEMBAUM, 2003).

ferramentas corretas, um administrador de redes pode fazer o controle da rede de forma mais direta. O plano de gerenciamento permite que possam ser feitas verificações periódicas nas entidades, detectando falhas e defeitos, podendo minimizar os efeitos fazendo a proteção do sistema, propagando a informação de falha ou mau desempenho e realizando testes para poder achar a exata localização da falha (SOARES; LEMOS; COLCHER, 1995).

1.1 JUSTIFICATIVA

Visto que gerenciamento, qualidade de serviços e segurança são temas essenciais na implementação de redes de computadores, é necessário fazer um levantamento dos pontos que possam prejudicar o uso da rede, a partir de uma metodologia que permita a utilização de forma segura e correta.

Nas implementações atuais, muitos administradores de redes não fazem uma verificação e correção das vulnerabilidades, nem o gerenciamento adequado, fazendo com que a rede tenha pontos de falha. Uma rede com pontos de falha pode acarretar em uma baixa qualidade de serviços, a falta de segurança das informações compartilhadas e possibilidade de que dispositivos indesejáveis tenham acesso à rede.

Em uma rede bem estruturada, prevendo pontos de falha e problemas de *loop* e com segurança implementada, o não suporte ao QoS pode inviabilizar a utilização de determinadas aplicações como VoIP ou tráfego de vídeo.

Ainda assim uma rede com as diretivas de segurança necessárias e contemplado o QoS, pode-se tornar inviável sem um gerenciamento. Assim para dar suporte a uma rede com essas características, o administrador, ao ocorrer um possível problema de um enlace não estar funcionando, terá que analisar ponto a ponto para descobrir onde está o erro, sendo que um gerenciamento adequado mostraria para ele onde está o possível problema.

Em suma, fica visível a importância de se construir uma estrutura de rede que contemple esses três aspectos descritos acima para melhorar as redes utilizadas.

1.2 OBJETIVO GERAL

Implementar e analisar uma estrutura de rede de computadores, contemplando conceitos de gerenciamento , qualidade de serviço e segurança.

1.3 OBJETIVOS ESPECÍFICOS

- Fazer uma análise dos conceitos que poderão ser utilizados;
- Verificar as ferramentas disponíveis para a implantação da rede (como o Cacti, Iperf e GNS3);
- Realizar a configuração física da estrutura de rede que será utilizada;
- Fazer a implementação lógica da rede;
- Testar a rede sem as diretivas propostas de gerenciamento, qualidade de serviços e segurança;
- Configurar os switches com QoS;
- Analisar o tráfego da rede, verificando se está atendendo o quesito de qualidade de serviços desejada;
- Demonstrar a importância da utilização de qualidade de serviços em redes;
- Implementar as políticas internas de segurança da rede;
- Configurar o GNS3 para simular um *firewall*;
- Promover alguns possíveis ataques internos e externos a rede;
- Provar a importância de pensar na segurança interna e externa de uma rede;
- Configurar o Cacti para garantir o gerenciamento da rede;
- Avaliar quais os ganhos de ter empregado um *software* de gerenciamento.

1.4 METODOLOGIA

A metodologia utilizada para a realização deste trabalho foi um estudo de caso empírico, que envolvendo uma experiência, a implementação da estrutura de rede, e a observação e análise da mesma.

Para este trabalho primeiramente foi realizado um estudo teórico sobre um conceito geral de redes de computadores com um aprofundamento em questões de gerenciamento, qualidade de serviços e segurança das mesmas. Posteriormente foi feito um levantamento e estudo de equipamentos e *softwares* que poderão ser utilizados na implantação da rede. Após esse levantamento, uma topologia de rede foi modelada contemplando os aspectos de gerenciamento, qualidade de serviços e segurança estudados. Com a topologia pronta foram feitas as implementações física e lógica da rede, a análise do tráfego, a implementação da

segurança e do gerenciamento, e com isso pôde-se verificar se a topologia da rede proposta contemplava os requisitos de segurança, QoS e gerenciamento.

Foram utilizados para a implementação da rede os seguintes equipamentos e *softwares*:

- 2 *switches* camada 2;
- 1 *switch* camada 3;
- 1 roteador;
- 8 computadores;
- *Software* Cacti, para gerenciamento de redes;
- *Software* simulador de *firewall* ASA, com o auxílio do GNS3;
- *Software* simulador de tráfego de rede, o Iperf.

A Figura 1 representa a estrutura de rede utilizada, englobando as camadas de núcleo, distribuição e acesso em uma topologia de malha parcial.

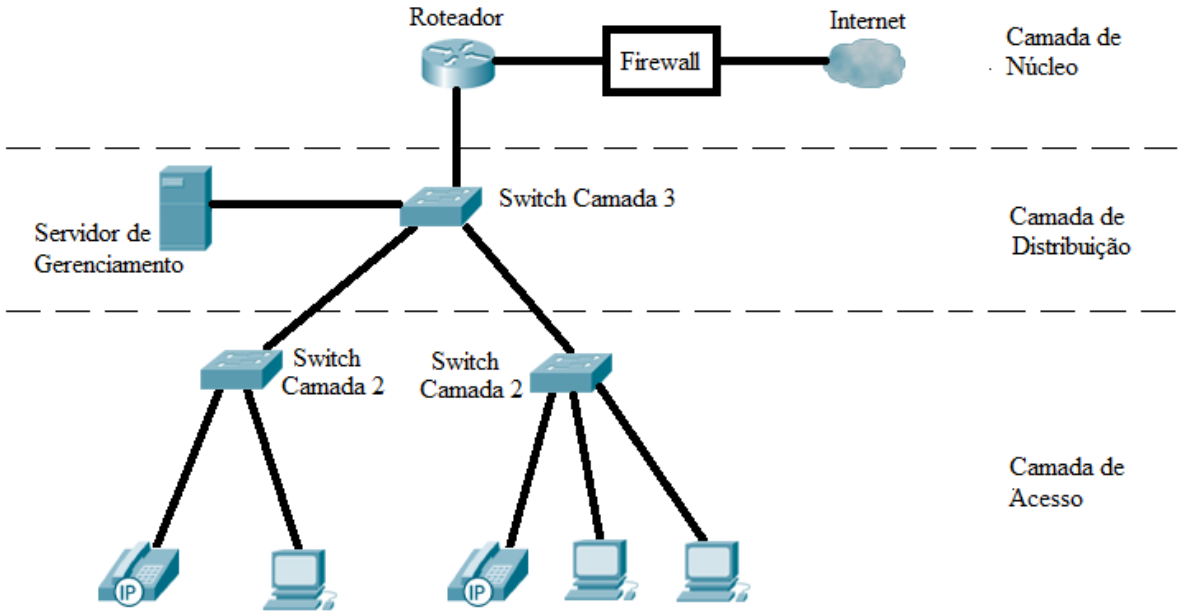


Figura 1 - Estrutura da Rede Proposta

Fonte: autoria própria

A rede como um todo foi dividida em sub-redes lógicas, as VLANs (*Virtual Local Area Networks)*, para diminuir os problemas de tempestades de broadcast. Em uma empresa,

por exemplo, cada VLAN poderia simbolizar um setor da organização, pois mesmo que tenha poucos computadores, devem ser separados em domínios de broadcast diferentes. Já na topologia utilizada, dois computadores serão alocados em uma VLAN de voz, que simularam um *softphone*, dois computadores em uma VLAN de dados e um quinto em uma VLAN de gerenciamento.

Outros três computadores foram utilizados para os testes, um para simular o *firewall* ASA, outro como servidor de gerenciamento com o Cacti instalado e um terceiro como um computador da Internet, ou seja, um computador externo a rede testada.

A implementação do QoS foi feita nos switches camada 2, que teve um tratamento diferenciado para cada tipo de serviço (voz e dados), tendo como prioridade mais alta o tráfego de voz e com uma prioridade mais baixa o tráfego de dados.

Como mostra a Figura 1, o *firewall* fica entre o roteador e a Internet (rede externa) fazendo a análise dos dados que possam entrar na rede e os que serão descartados.

A Figura 2 apresenta uma foto do Laboratório de Redes (LabRedes), do Departamento Acadêmico de Informática (DAINF) da UTFPR, onde foram realizados os experimentos e simulações. A Figura 3 apresenta uma foto dos equipamentos reais que foram utilizados implementação da rede.

Figura 2 - Foto do laboratório

Fonte: autoria própria

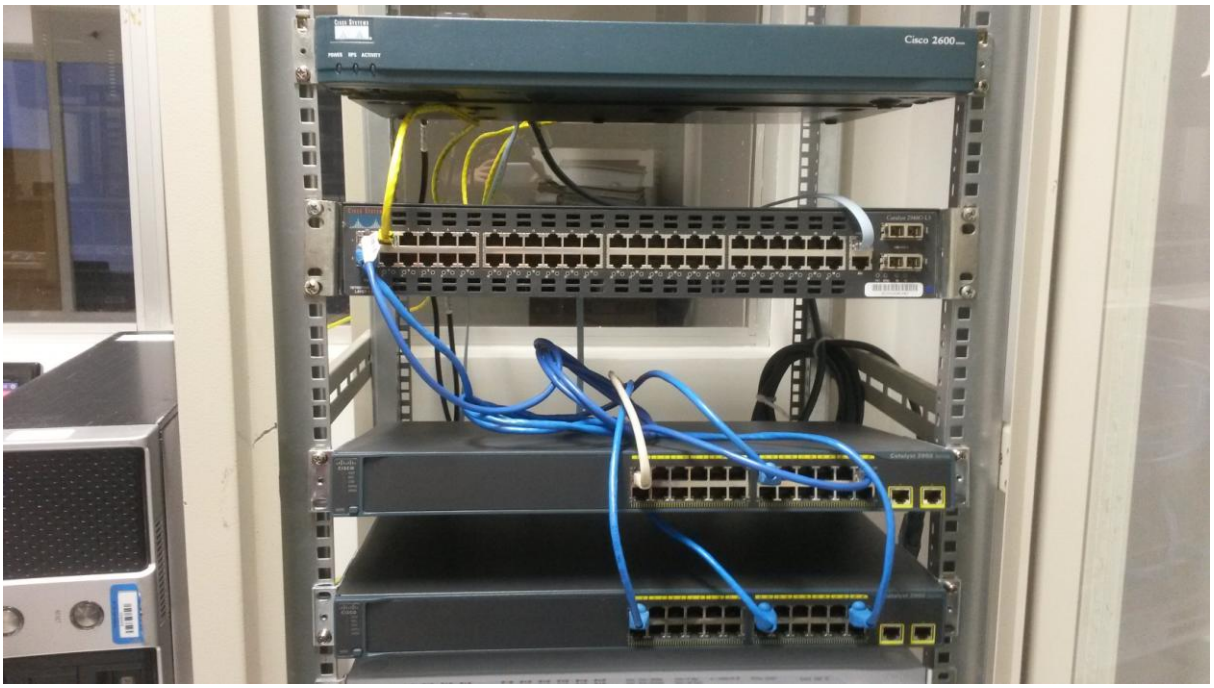


Figura 3 - Foto dos equipamentos

Fonte: autoria própria

1.5 ORGANIZAÇÃO DO DOCUMENTO

Este documento é composto por 4 capítulos. O capitulo 1, contempla a introdução da proposta, descrevendo a justificativa e os objetivos. No capitulo 2 é descrito o estado a arte do trabalho e o referencial teórico da proposta com temas como: redes de computadores, pilha de protocolos TCP/IP, equipamentos de rede, gerenciamento de redes, qualidade de serviços, segurança e as ferramentas utilizadas.

No capitulo 3 é apresentado o estudo de caso, contendo os cenários de testes e os resultados. Por fim no capitulo 4 contém a conclusão e os trabalhos futuros.

2 ESTADO DA ARTE E LEVANTAMENTO BIBLIOGRÁFICO

Há vários trabalhos relacionados a gerenciamento, qualidade de serviços e seguranças de redes. No trabalho (BLACK, 2008), o pesquisador comparou 9 ferramentas (RRD, ZENOSS, ManageOP Engine, BigBrother4, SpiceWorks, Look@LAN, Zabbix e Nagios) de gerenciamento e monitoração de redes, com parâmetros como desempenho, facilidade de utilização e necessidade de recursos, com o objetivo de ajudar os gerentes de redes a escolher a ferramenta que mais atende as suas necessidades. Os resultados obtidos foram apresentados em uma tabela contendo as principais características que cada ferramenta apresenta ou não.

Na monografia de (BRUN; VOGT; MENDES, 2002) foram estudadas as alternativas que tornassem a qualidade de serviços sobre IP viáveis, apresentando as vantagens e desvantagens das tecnologias que existiam para cada necessidade especifica.

Em (BRUN; VOGT; MENDES, 2002) foi analisado o *software* Cisco IOS e constatado que ele trata de vários aspectos e soluções de QoS. A tecnologia de suporte à QoS disponibilizado nos equipamentos Cisco beneficiam tanto redes de pequeno porte quanto grandes corporações, controlando com eficiência os aspectos como largura de banda, retardo, *jitter* e perda de pacotes.

O artigo de (TSAUR; HORNG, 1998), tem como objetivo apresentar conexões seguras de redes locais, e alcançar ambientes de *Internet* seguros por meio de LANs (*Local Area Networks*) de *switches* e *firewalls*.

Foi proposta uma estrutura de LAN em forma de uma árvore simétrica, em que as estações de usuários são representadas pelas folhas, os *hubs* são os nós internos e as ligações representam a comunicação *full-duplex* entre os pares (TSAUR; HORNG, 1998).

Na proposta de (BERTHOLDO, 1997) tem-se uma filosofia de gerência de segurança, que teve como resultado um sistema que alerta quando há tentativas de ataques e situações de risco, chamado CUCO. O objetivo do CUCO é alertar o gerente da rede quando identificada alguma alteração que possa comprometer a segurança.

Já o artigo (FARROW, 2003), discute questões relacionadas utilização e segurança de VLANs, como as redes virtuais trabalham, as vantagens de ter segurança ou não em VLANs, como minimizar os pontos fracos quando se utiliza VLANs, entre outras questões relacionadas com VLANs e sua segurança.

Para o bom entendimento do seguinte trabalho alguns temas serão abordados a seguir: a visão geral de redes de computados, uma breve explicação da pilha de protocolos TCP/IP, a diferença entre os equipamentos utilizados, o estudo dos três tópicos importantes para o trabalho (gerenciamento, qualidade de serviços e segurança de redes), e por fim as ferramentas que foram necessárias.

2.1 REDES DE COMPUTADORES

As redes de computadores são usadas para interligar computadores pessoais, estações de trabalho e instalações de empresas, com o intuído de trocar informações e compartilhar recursos. As redes locais (LANs) se diferem dos outros tipos de redes por três motivos: tem um tamanho restrito, as tecnologias de transmissões utilizadas em LANs fazem uso de controles de acesso ao meio muitas vezes compartilhados, como é o caso do CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), e a possibilidade se de serem implementadas em diversas topologias (TANEMBAUM, 2003).

Algumas topologias físicas usadas em redes locais são (Figura 4): a topologia em estrela (a), em que existe um nó central ligado a todos os outros nós e por onde é passado todas as mensagens; a topologia em anel (b), que consiste em varias máquinas interligadas por meio de um caminho fechado que trabalham como repetidores, até que a mensagem seja retirada da rede pelo nó de destino; e a topologia em barramento (c), nessa topologia todos os nós se ligam ao mesmo meio de transmissão e cada nó pode ver todas as informações transmitidas (SOARES; LEMOS; COLCHER, 1995).

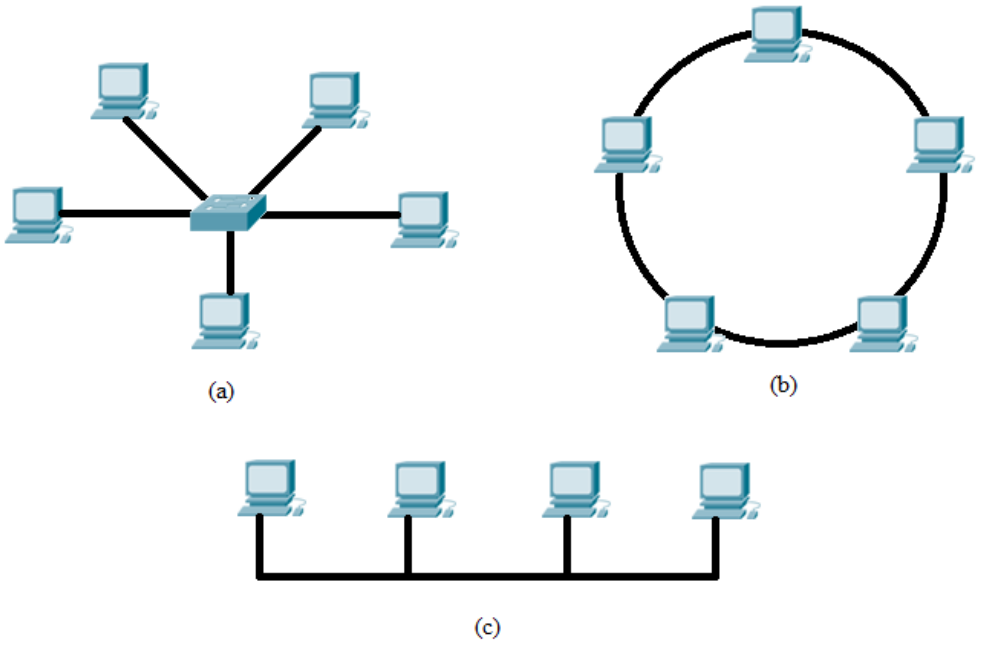


Figura 4 - Topologias de Rede: (a) Estrela, (b) Anel e (c) Barramento

Fonte: autoria própria

Outra topologia também utilizada refere-se às redes em malha, essas redes podem ser classificadas em malha total e malha parcial. Em uma rede em malha total, representada na Figura 5, todos os nós estão obrigatoriamente ligados a todos os outros nós. Quando um novo nó é inserido este terá que ser ligados a todos os outros, tornando essa topologia inviável para redes muito grandes, pela quantidade de cabos utilizados. Uma das vantagens da utilização desta topologia é o grau de redundância elevado. Com isso a rede de malha parcial, representada na Figura 6 é a mais viável. Nesta topologia é necessário que todos os nós possam se comunicar, tendo um grau de redundância aceitável, porém não é preciso que todos os nós estejam conectados entre si.

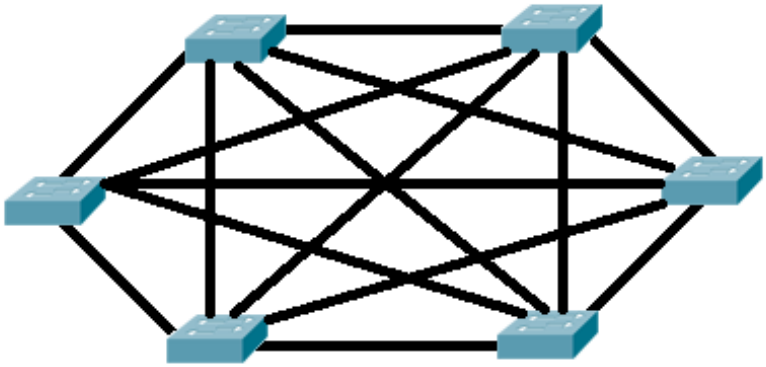


Figura 5 - Malha Total

Fonte: autoria própria

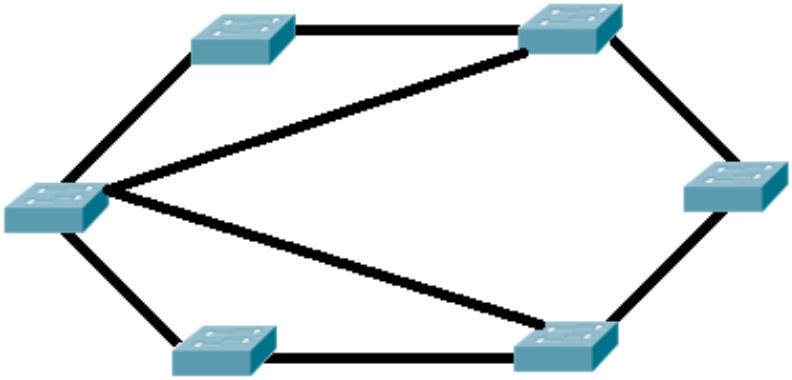


Figura 6 - Malha Parcial

Fonte: autoria própria

Com o intuito de separar a topologia física da topologia lógica, conseguindo assim maior flexibilidade e escalabilidade, as redes virtuais (VLANs) foram criadas (TANEMBAUM, 2003). Assim a rede pode ser dividida, por exemplo, por departamento ou funções independentemente da localidade física dos equipamentos. Isso possibilita aumento de segurança e melhor gerenciabilidade da rede local (FELIPPETTI, 2008).

2.2 PILHA DE PROTOCOLOS TCP/IP

A pilha de protocolos TCP/IP é um modelo teórico, em que um grupo de tarefas específicas é representado por cada uma das camadas (SCRIMGER; LASALLE; PARIHAR; GUPTA, 2002).

Tanto para (STALLINGS, 2005) quanto (SCRIMGER; LASALLE; PARIHAR; GUPTA, 2002) o modelo TCP/IP é dividido em cinco camadas, sendo elas: camada física, camada de acesso/interface de rede, camada inter-rede, camada de transporte e camada de aplicação, como mostra a Figura 7.

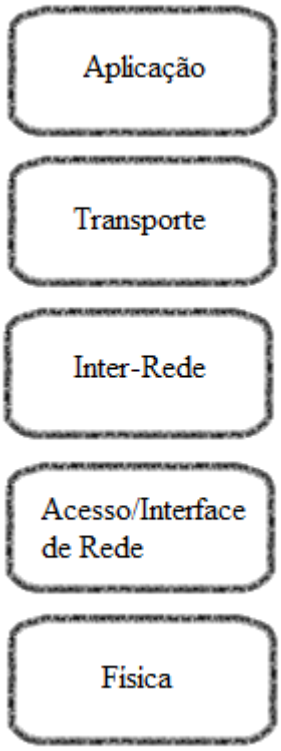


Figura 7 - Pilha de Protocolos TCP/IP

Fonte: autoria própria

A camada física é responsável por receber os dados passados pelas outras camadas e converte-los em bits para serem transferidos pelo meio de transmissão, que podem ser cabos ou ondas de rádio entre outros. A camada de acesso/interface de rede é responsável por transformar os bits recebidos da camada física em quadros, identificar a partir dos endereços MAC (*Media Acess Control*) os dispositivos da rede e perceber erros das camadas superiores (SCRIMGER; LASALLE; PARIHAR; GUPTA, 2002). Já a camada inter-rede, diferente da

camada anterior, que abrangia dispositivos da mesma rede, é responsável por fazer o roteamento entre dispositivos que estão conectados a diferentes redes. A camada de transporte é responsável por coletar os mecanismos que fornecem a confiabilidade das trocas de dados, os protocolos mais comuns são o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*). Por fim a camada de aplicação é responsável por dar suporte a várias aplicações do usuário. (STALLINGS, 2005).

Tanto para (FOROUZAN, 2006), como para (COMER, 2007) um protocolo é um conjunto de regras acordado por todos os envolvidos em uma comunicação. Assim para o entendimento deste trabalho é importante que sejam abordados alguns protocolos específicos.

O *Spanning Tree Protocol* (STP) que é um protocolo de camada 2, que tem como função monitorar constantemente a rede para identificar os enlaces ativos e bloquear as portas redundantes dos *switches* para evitar os quadros fiquem em *loop* na rede. (FELIPPETTI, 2008). Para isso o STP define para cada interface dois possíveis estados: *blocking*, que não pode enviar ou receber quadros; e *forwarding*, habilitada a enviar e receber os quadros de dados. (ODOM, 2003). Com isso um único caminho é permitido entre as LANs, formando assim uma árvore. (KUROSE; ROSS, 2003).

O *Telnet* é um protocolo da camada de aplicação que permite a um usuário que esteja em um computador possa efetuar o *login* em outro computador remoto. (KUROSE; ROSS, 2006). O tráfego da comunicação entre os terminais é dado por uma conexão TCP. (STALLINGS, 2005).

O *Secure Shell* (SSH) também é um protocolo da camada de aplicação, porém permite, de forma mais segura que o *Telnet*, o acesso remoto à computadores e equipamentos de redes (MORIMOTO, 2008). Para obter essa segurança os dados são criptografados pelo SSH antes de serem enviados pela Internet. (COMER, 2007)

O *Dynamic Host Configuration Protocol* (DHCP), ou em português Protocolo de Configuração Dinâmica de Endereços de Rede, não exige que um administrador precise configurar manualmente os endereços IPs para cada computador que se conecte a rede. Este protocolo permite que a máquina receba sua configuração automaticamente. (MORIMOTO, 2008). Para isso é utilizado uma abordagem cliente-servidor, em que cada novo computador que entrar na rede, envie por *broadcast* uma requisição DHCP, o servidor DHCP ao receber essa mensagem, procura em sua base de dados se já contem uma entrada especifica para esse computador, se houver, faz a alocação do IP a máquina solicitante. Se não houver, o servidor

associa temporariamente o próximo endereço IP do conjunto a esse computador e o envia para o cliente. (COMER, 2007).

O *File Transfer Protocol* (FTP) é um protocolo utilizado para a transferência de arquivos de um computador a outro, um arquivo arbitrário. (COMER, 2007). O FTP oferece recursos para controlar o acesso de usuários, solicitando um identificador, a senha e quais os arquivos e as ações de arquivas que são desejadas. (STALLINGS, 2005).

Por fim o *HyperText Transfer Protocol* (HTTP) é um protocolo da camada de aplicação implementado em dois programas (Cliente-Servidor), que conversam entre si por meio de troca de mensagens HTTP. É o próprio HTTP que determina a estrutura das mensagens e o modo como são trocadas. (KUROSE; ROSS, 2006). O HTTP utiliza o TCP para garantir confiabilidade. (STALLINGS, 2005). Há quatro operações básicas suportadas por esse protocolo: *GET* (pede um item ao servidor), *HEAD* (requer informações de status de um item), *POST* (envia dados para o servidor anexar a um item) e *PUT* (envia dados para o servidor substituir um item). (COMER, 2007).

2.3 EQUIPAMENTOS DE REDE

Os *switches*, também chamados de comutadores (Figura 8), podem ser divididos em dois grupos: os *switches* de camada 2, que operam nas camadas física e enlace e os *switches* de camada 3, utilizados na camada de rede, fazendo o roteamento dos pacotes. (FOROUZAN, 2006).

Figura 8 - *Swicthes*

Fonte: (Cisco, 2012)

Para (KUROSE; ROSS, 2006) os *switches* camada 2 enviam os quadros com base no endereço de *hardware* (*MAC Address*) do *host* de destino. Os comutadores, para que possam aprender onde estão localizadas as máquinas, contêm uma tabela que faz o mapeamento dos endereços de MAC dos dispositivos às portas as quais eles se encontram. (FELIPPETTI, 2008). Na Figura 9, quando um computador A envia uma informação para um computador B e o *switch* não conhece nenhum dos endereços, primeiramente preenche a tabela com o endereço físico de A e depois envia o quadro para todos os outros dispositivos. Essa transmissão é chamada de *broadcast*. Quando o computador B responder o quadro, o novo endereço será armazenado na tabela, fechando assim um canal exclusivo de comunicação entre os dois computadores. (MORIMOTO, 2008).

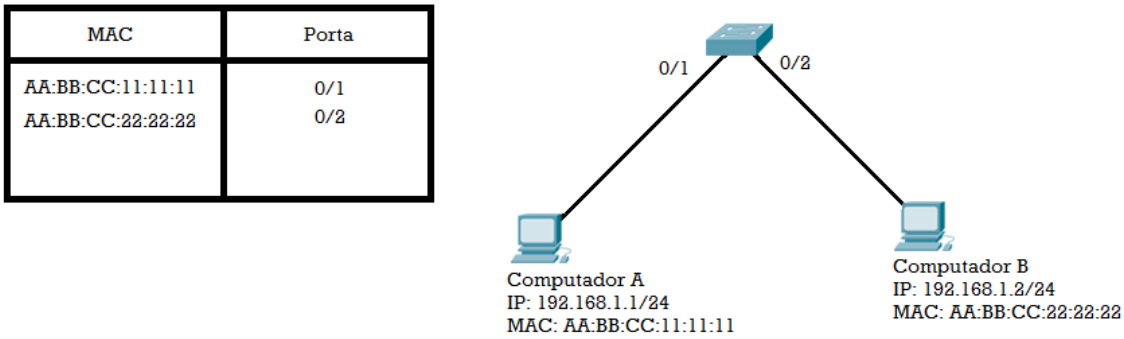


Figura 9 - *Swicth* camada2

Fonte: autoria própria

Já o *switches* de camada 3 tem a função de fazer o roteamento de pacotes entre redes distintas, utilizando o endereço lógico (IP) como ponto de referência para a sua tabela de roteamento (FOROUZAN, 2006). Os *switches* L3 dão suporte a subredes, impedindo assim as tempestades de *broadcast* (STALLINGS, 2005), ou seja, a propagação continua de frames na rede. (FELIPPETTI, 2008).

Os *routers*, ou roteadores (Figura 10) atuam na camada de rede. Com isto têm a função de rotear endereços IP em vez de endereços MAC. Também são usados para interligar redes que estão separadas de forma lógica, utilizando um esquema de endereçamento e podem interligar um grande numero de redes diferentes que mesmo assim irão escolher a rota mais rápida para a entrega de um pacote de dados. (MORIMOTO, 2008) A função dos *routers* é fazer o roteamento utilizando a comutação por pacotes, possibilitando com isto a entrega dos dados aos sistemas autônomos de destino. Atualmente os esquemas de endereçamento

utilizam o IPv4 e o IPv6 para fazerem o encaminhamento dos pacotes entre as redes (STALLINGS, 2005).

Figura 10 - *Routers*

Fonte: (Cisco, 2012)

O *firewall* é um mecanismo para proteção que combina *hardware* e *software* e tem como função filtrar todo o tráfego que entra e sai da rede, conforme a Figura 11. (KUROSE; ROSS, 2006). Fazendo uma analogia, da mesma forma como os medievais construíam muros e fossos profundos em torno de seus castelos, forçando quem quisesse entrar ser revistado, ao passar por uma ponte levadiça, o *firewall* analisa os pacotes que entram e saem, para que sejam descartados os pacotes que possam trazer algum tipo de ameaça à rede. (TANEMBAUM, 2003).

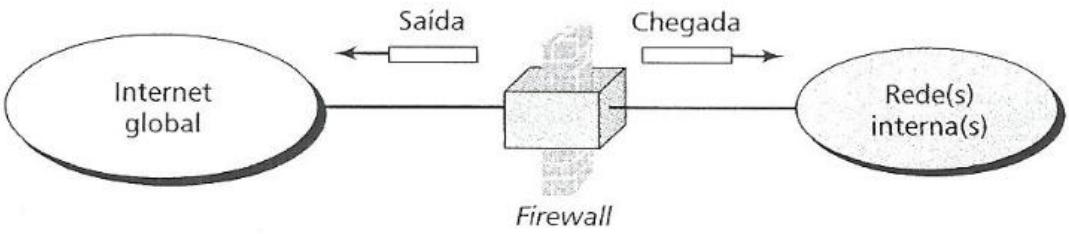


Figura 11 - *Firewall*

Fonte: (FOROUZAN, 2006)

Um *firewall* pode ter dois tipos de componentes: o filtro de pacotes e o *gateway* de aplicação ou também chamado de servidor de *proxy*. O filtro de pacotes tem a função de filtrar o tráfego de entrada e saída da rede de acordo com as decisões do administrador da rede, que podem ser baseadas nos endereços IPs, portas TCP e UDP de origem e destino e os tipos de mensagens (KUROSE; ROSS, 2006). Diferente do filtro de pacotes que opera nas

camadas de rede e transporte o servidor *proxy* atua na camada de aplicação, podendo assim examinar o conteúdo da mensagem em si. (FOROUZAN, 2006)

Conforme (FELIPPETTI, 2008) a Cisco lançou o *Adaptative Security Appliance* (ASA), uma nova geração de equipamentos de segurança que podem ser utilizados como *firewalls*, representado na Figura 13. A Cisco disponibiliza uma interface gráfica, o *Adaptive Security Device Manager* (ASDM) (Figura 12) para configuração e administração do ASA. O ASDM possibilita, por exemplo, que o administrador da rede veja uma possível tentativa de invasão em tempo real, podendo com isto tomar as devidas providências.

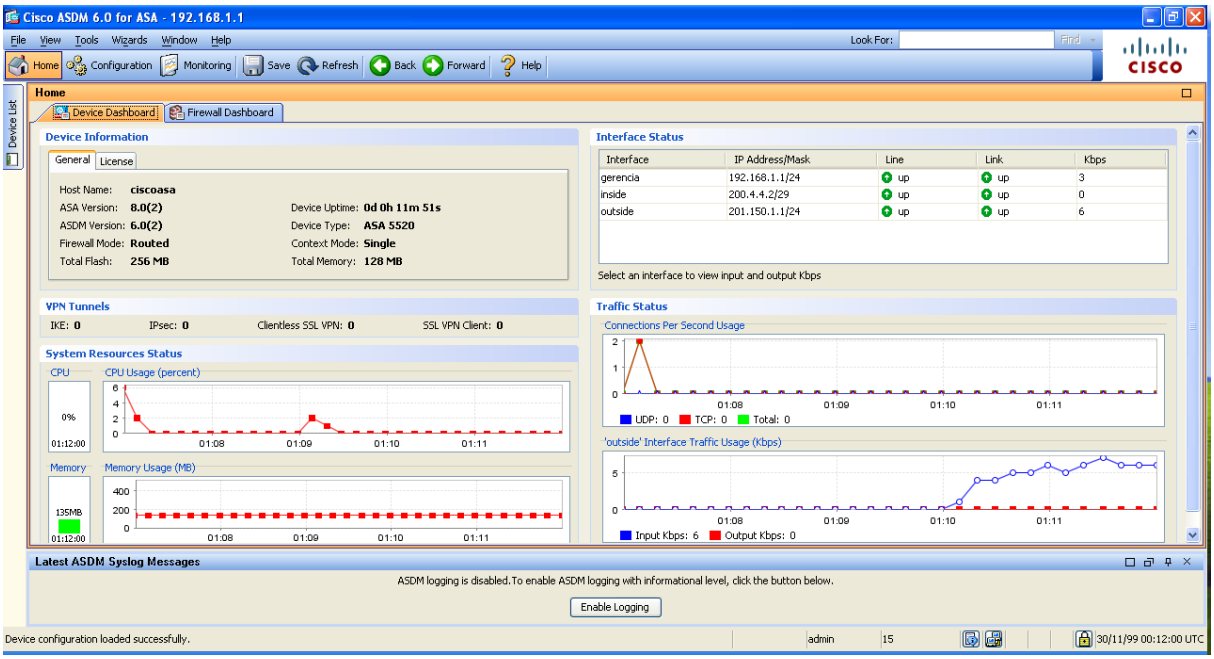


Figura 12 - ASDM

Fonte: autoria própria

Figura 13 - ASA

Fonte: (Cisco, 2012)

2.4 GERENCIAMENTO DE REDES

Tanto para (STALLINGS, 2005), (HEIN; GRIFFITHS, 1995), (CORREIA, 2004) os requisitos de gerenciamento de redes podem ser divididos em cinco principais áreas:

- ✓ Gerenciamento de falhas;
- ✓ Gerenciamento de contabilidade;
- ✓ Gerenciamento de configuração e de nome;
- ✓ Gerenciamento de desempenho;
- ✓ Gerenciamento de segurança.

O gerenciamento de falhas contempla o funcionamento correto de todo o sistema e de cada componente individualmente (STALLINGS, 2005). Para (CORREIA, 2004) há três divisões das funções do gerenciamento de falhas: supervisão de alarmes, teste e relatório de problemas. (STALLINGS, 2005) e (HEIN; GRIFFITHS, 1995) englobam a requisito as ações de detecção, isolamento e correção/eliminação da falha ocorrida.

No gerenciamento de contabilidade é preciso coletar dados da rede, analisá-los e contabilizá-los (CORREIA, 2004), para assim, controlar o uso de recursos de redes por usuários ou por classe de usuários, para que não haja a sobrecarga da rede por abuso de privilégios e para que o crescimento da rede seja planejado mais facilmente. (STALLINGS, 2005).

Já o gerenciamento de configuração e de nome tem como propósito manter, acrescentar e atualizar o estado dos componentes e suas as relações durante a execução da rede (STALLINGS, 2005). Para (HEIN; GRIFFITHS, 1995) o gerenciamento de configuração tem como principais funções supervisionar a configuração atual de todos os dispositivos, bem como armazenar essas configurações, realizar o inventário dos dispositivos utilizados na rede e modificar as configurações individuais para atender a demanda.

O gerenciamento de desempenho engloba a função monitoramento, que é o acompanhamento das atividades da rede e a função de controle onde é possível fazer ajustes com o intuito de melhorar o desempenho da rede (STALLINGS, 2005). Também é importante a simulação de certos eventos e a coleta e análise de dados, para serem apresentados como estatísticas (HEIN; GRIFFITHS, 1995), podendo conter o perfil do comportamento da rede e os limiares mínimos e máximos sobre a utilização (CORREIA, 2004).

E por fim o gerenciamento de segurança que tem como principio gerar, manter e distribuir as senhas e informações de autenticação ou de controle de acesso. (STALLINGS, 2005). Para (HEIN; GRIFFITHS, 1995) deve obter mecanismos de segurança para identificar os recursos relevantes, definir claramente os pontos de acesso a esses recursos que devem ser protegidos e implementar um protocolo de gestão para administrá-los. Diferentes abordagens podem ser utilizadas para realizar essas funções: proteção do sistema operacional, proteção física e protocolos de proteção.

Para um administrador de redes, dar suporte a uma infraestrutura que tenha todos os requisitos de gerenciamento implementados é uma boa prática, pois o *software* utilizado para gerenciar a rede vai apontar os pontos de possíveis falhas, problemas de *loops* no cabeamento que podem sobrecarregar a rede ou equipamentos com as funcionalidades comprometidas. Já em uma rede sem gerenciamento, o administrador tem que procurar o problema pelo método de tentativa e erro, o que requer muito mais tempo e esforço do profissional.

2.4.1 SNMP

"O SNMP (*Simple Network Management Protocol*) é um protocolo da camada de aplicação que foi desenvolvido para facilitar a troca de informações de gerenciamento entre dispositivos de rede." (MOURA, 2003, p.31). A utilização deste protocolo, facilita aos administradores de redes gerenciar o desempenho, encontrar e solucionar possíveis problemas e se for preciso, expandir a rede com maior precisão (GUIMARÃES, 1997).

Para este trabalho foi necessário entender os três conceitos básicos do SNMP:

- ✓ Gerente de rede;
- ✓ Agentes;
- ✓ MIB.

O gerente de rede pode ser uma ou mais máquinas que receberam a informação dos outros dispositivos da rede. Já para (KUROSE; ROSS, 2006) o agente de gerenciamento é o processo a ser executado em cada dispositivo da rede que será gerenciado, comunicando assim com o gerente da rede que comanda e controla a execução das ações locais. Por fim, o MIB (*Management Information Base*), ou em português, base de informações de gerenciamento, é uma base que contêm todas as informações coletadas pelo gerente da rede.

Alguns parâmetros importantes são estabelecidos pela arquitetura SNMP (HEIN; GRIFFITHS, 1995):

- ✓ A amplitude da gestão de informação na rede;
- ✓ A forma como os dados transferidos;
- ✓ As operações de gestão que podem ser executadas;
- ✓ A forma como os dados serão trocados entre as entidades gerenciadoras;
- ✓ As relações entre todas as entidades administradas.

Segundo (FEIT, 1995) e (HEIN; GRIFFITHS, 1995) existem 5 tipos diferentes de mensagens que podem ser trocadas entre as entidades, representadas na Figura 14:

- ✓ *Get-request:* serve para uma entidade gerenciadora solicitar uma ou mais variáveis para *um agente da rede;*
- ✓ *Get-next-request:* é utilizado para a entidade gerenciadora solicitar a próxima variável, depois das que já foram especificadas pelo agente, ou seja, o gerente da rede pede valores sequencialmente. Por exemplo, ler as linhas de uma tabela;
- ✓ *Set-request:* possibilita que o gerente da rede peça para o agente atualizar o valor de uma ou mais variáveis;
- ✓ *Get-response:* permite que o agente retorne o valor de uma ou mais variáveis solicitadas pela entidade gerenciadora;
- ✓ *Trap*: serve para um agente informar para o gerente da rede um importante evento ou problema ocorrido.

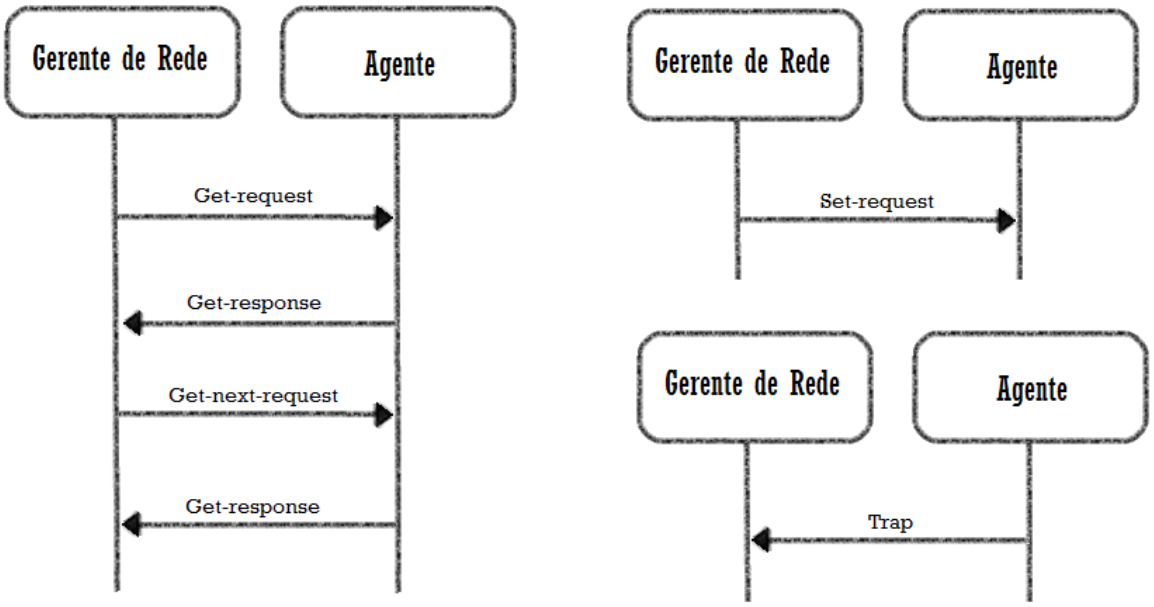


Figura 14 - Mensagens SNMP

Fonte: autoria própria

2.5 QUALIDADE DE SERVIÇO

Segundo (TANEMBAUM, 2003), a qualidade de serviço (QoS – *Quality of Service*) é definida por quatro parâmetros: confiabilidade, retardo, flutuação e largura de banda. Porém, cada aplicação pode ter sua rigidez (alta, media ou baixa) em relação a cada requisito. A confiabilidade é que todos os bits devem ser entregues de forma correta. O retardo é o tempo de atraso dos pacotes até a chegada ao destino. A flutuação é a chegada de pacotes em tempos irregulares entre eles. E a largura de banda é o volume de banda necessário para a execução de cada aplicação.

Por exemplo, o IP convencional utiliza a lei do *best effort*, ou melhor esforço para entregar todas as informações, sem diferenciar os tipos de informações ou garantir as características de entrega, da melhor forma permitida pelo estado da rede naquele momento, ou seja não oferece nenhuma garantia de QoS a rede. (COLCHER; GOMES; SILVA; FILHO; SOARES, 2005).

De acordo com (WANG, 2001) e (VEGESNA, 2001) existem duas principais arquiteturas em relação ao QoS, *Integrated Services* (IntServ), ou seja, Serviços Integrados e

Differentiated Services (DiffServ), ou seja, Serviços Diferenciados. No modelo IntServ (Figura 15) ao chegar uma requisição é traçada toda a rota de envio e reservado os recursos da rede, para somente depois passar os pacotes. Esse modelo é inviável em redes com muitos nós e conexões (GONZAGA; SALLES, 2007).

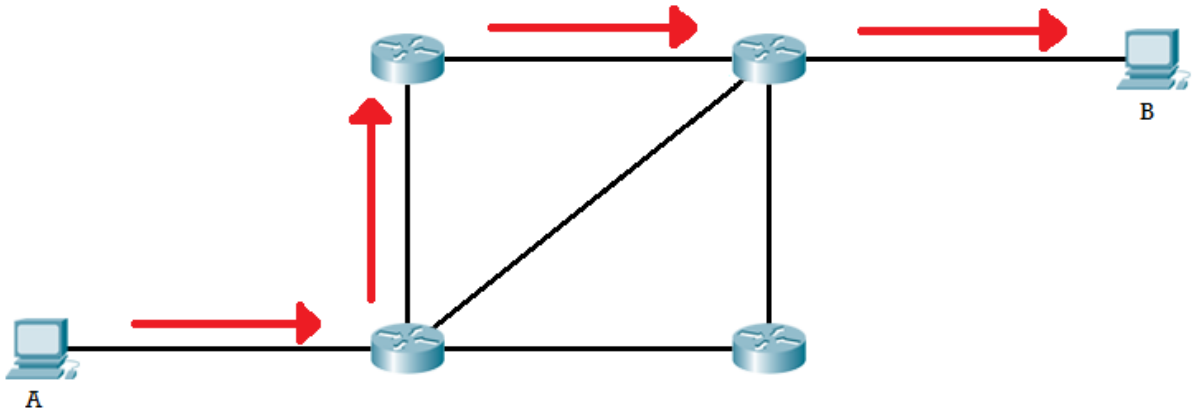


Figura 15 - Roteador com IntServ

Fonte: autoria própria

Já o DiffServ diferencia os tipos de serviços e atribui uma prioridade diferente para cada um. Em uma aplicação um roteador sem o DiffServ trataria os pacotes com a estrutura *First In First Out* (FIFO), ou seja, o primeiro pacote que entra é o primeiro que sai. No caso do *buffer* estar cheio, descartaria os pacotes mais novos, sem se preocupar com o serviço deles, conforme Figura 16, em que o quinto pacote que é um serviço de voz que irá ser descartado. Já em uma estrutura com a arquitetura DiffServ, no roteador os pacotes são diferenciados pelo seu tipo de serviço e tem prioridades diferentes. Essa separação é chamada por (WANG, 2001) de *forwarding classes.* Em cada classe a quantidade de tráfego que o usuário pode utilizar é limitada na extremidade da rede. Na Figura 17, os serviços de voz e vídeo tem prioridade 1 e os serviços de dados tem prioridade 2, ou seja, serviços de voz e vídeo tem uma prioridade mais alta que os de dados.

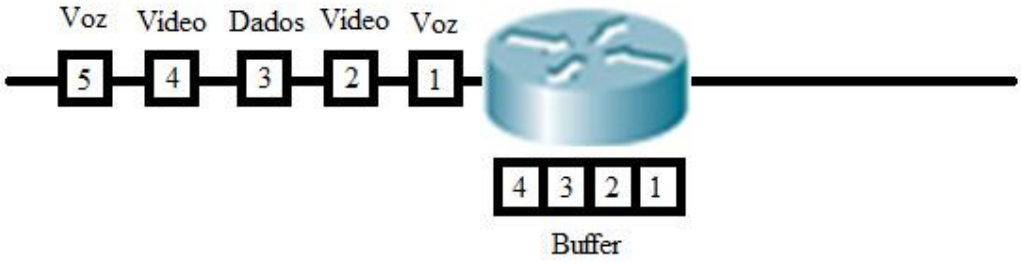


Figura 16 - Roteador Sem QoS

Fonte: autoria própria

Figura 17 - Roteador Com Diffserv

Fonte: autoria própria

O mesmo pode ser feito em *switches*. Na Figura 18, os *switches* estão configurados para suportar QoS na rede local e com isso se dois usuários estiverem conversando um com o outro utilizando VoIP, mesmo que os outros usuários estiverem gerando muito trafego de dados na rede, não haverá problema na VLAN de voz. Já se não estivesse implantado o QoS, esta situação poderia tornar a conversa por VoIP inviável.

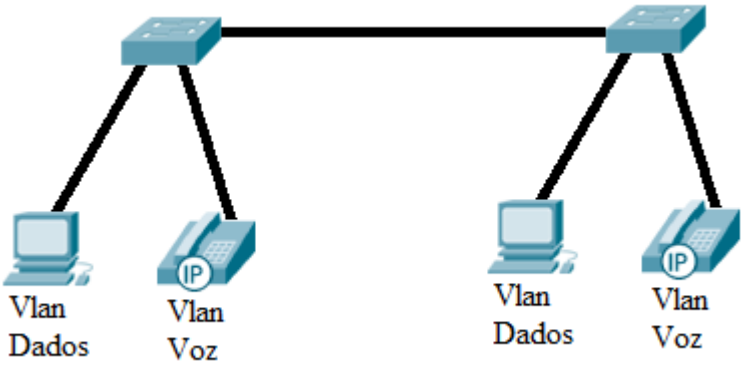


Figura 18 - Switches com QoS

Fonte: autoria própria

2.5.1 VoIP e Telefonia IP

O VoIP (*Voice over IP*) , em português, Voz sobre IP ou também chamado telefonia IP é a utilização do IP como base para o serviço telefônico (COMER, 2006). Com isso é necessário "fazer amostra contínua de áudio, converter cada amostra para a forma digital, enviar a cadeia digitalizada resultante através de uma rede IP em pacotes e converter de volta a cadeia digitalizada para a forma auditiva analógica" (COMER, 2007).

Já (COLCHER; GOMES; SILVA; FILHO; SOARES, 2005) especifica VoIP diferente de telefonia IP. O VoIP seria tanto as técnicas utilizadas de empacotamento e transmissão de amostras de voz, quanto os mecanismo de sinalização que são necessários para estabelecer chamadas telefônicas em redes IP. A telefonia IP é a aplicação das tecnologias de VoIP na transmissão e sinalização, contempla também o caminho percorrido até o usuário final e a possibilidade de integração com outros tipos de serviços da Internet.

Há três tipos de utilização do VoIP para (COLCHER; GOMES; SILVA; FILHO; SOARES, 2005):

- ✓ De terminal IP para terminal IP;
- ✓ De terminal IP para telefone;
- ✓ De telefone para telefone.

A utilização do VoIP de um terminal IP para outro terminal IP se dá através de um equipamento, geralmente chamado de terminais ou agentes de usuário. Estes equipamentos podem ser, por exemplo, *softphones* ou telefones IP. Ambos têm a capacidade de codificar e decodificar amostras de sinais de voz em fluxos de áudio digital e receber e transmitir os

fluxos codificados em uma rede IP. Porém o *softphone* é a utilização de um *software* instalado em um computador para realizar essas funcionalidades, enquanto o telefone IP é um aparelho que oferece aos usuários uma interface similar a telefones convencionais (COLCHER; GOMES; SILVA; FILHO; SOARES, 2005).

O VoIP utilizado para a comunicação de um terminal IP para um telefone convencional necessita de um *gateway* que faça a ligação entre os dois. O *gateway* permite que a chamada seja iniciada de qualquer um dos lados e tem como função traduzir e encaminhar tanto a requisição que chega como sua resposta. Após a chamada estabelecida o equipamento precisa encaminhar a voz nos dois sentidos, traduzindo a codificação usada em cada um dos lados (COMER, 2006 p 335).

Por fim, quando se utiliza o VoIP entre dois telefones convencionais, diferencia do cenário anterior, por normalmente a comunicação se estabelecer entre duas centrais telefônicas diferentes. Com isso pode ser utilizado um único *gateway* ou um *gateway* diferente para cada central. A utilização desses equipamentos de sinalização possibilita a interligação das centrais distintas através de redes IP (HARFF, 2008).

2.6 SEGURANÇA DE REDES

A segurança de redes é uma parte essencial para a proteção da informação. Para isso três principais requistos podem ser definidos, conforme a Figura 19 (NAKAMURA; GEUS, 2007):

- ✓ Confiabilidade/Sigilo;
- ✓ Integridade;
- ✓ Disponibilidade.

A confiabilidade ou sigilo é o ato de manter a informação longe de pessoas não autorizadas, ou seja, somente pessoas autorizadas podem acessar os dados. No principio de integridade os dados só podem ser escritos, alterados, mudados o estado, excluídos ou criados por pessoas autorizadas. O requisito de disponibilidade é o ato que todos os elementos de rede por onde passa a informação desde sua origem ate o seu destino devem estar disponíveis.

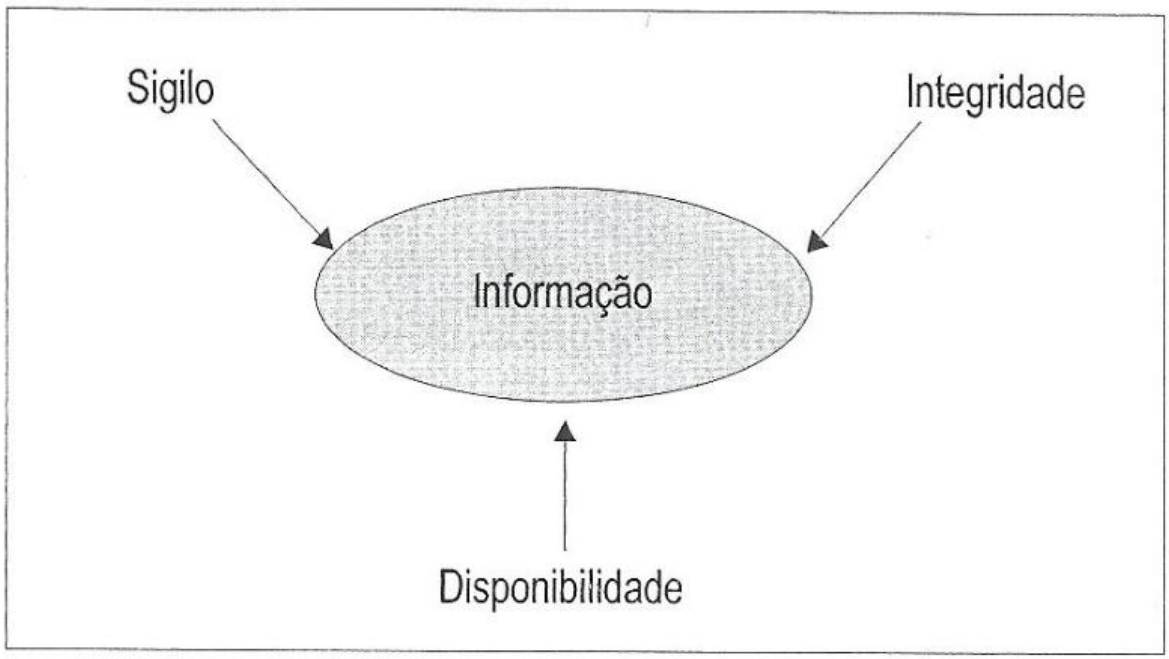


Figura 19 - Propriedades importantes de segurança

Fonte: (NAKAMURA; GEUS, 2007)

Um conjunto de condições que possibilita a violação de uma política de segurança explicita ou implícita é chamada de vulnerabilidade (SEACORD; HOUSEHOLDER, 2005). Para (CERT.br, 2006) na área de tecnologia da informação, exemplos de vulnerabilidade poderiam ser falhas de configuração de programas, serviços ou equipamentos de redes. Assim as vulnerabilidades podem ser "pontos nos quais o sistema é suscetível a ataques e ameaças de segurança" (SCHWEITZE, 2005).

Há dois tipos de ameaças possíveis: ameaças acidentais, em que não há a intenção premeditada e ameaças intencionais. Essas ameaças ainda podem ser passivas ou ativas. Uma ameaça passiva não tem como resultado nenhuma modificação das informações espionadas. Já uma ameaça ativa resulta na modificação das informações (SOARES; LEMOS; COLCHER, 1995).

Os ataques também podem ser classificados como ataques passivos ou ativos. Os ataques passivos não têm como intuito afetar os recursos da rede, somente tentam aprender e utilizar as informações que são trafegadas. Alguns exemplos desse tipo de ataque são o vazamento de conteúdo das mensagens, como conversas telefônicas, e-mails ou arquivos e o de análise de tráfego. Já os ataques ativos tentam afetar a operação da rede e alterar seus recursos, como modificar um fluxo de dados ou criar um fluxo falso. Alguns exemplos deste

tipo de ataque são: o de falsidade, em que uma entidade se passa por outra diferente; de repetição, que envolve a retransmissão de unidades de dados capturadas; de modificação de mensagens, em que uma parte da mensagem legitima é alterada; e de negação de serviço (STALLINGS, 2005).

Um ataque de negação de serviço (*Denial-of-Service Attack* – DoS), é quando se gera uma grande quantidade de algum tipo de trabalho para a rede, hospedeiro ou outro componente da infraestrutura, fazendo com que o trabalho legítimo não possa ser realizado, tornando assim impossível a utilização do mesmo por um usuário autêntico da rede. (KUROSE; ROSS, 2006).

Tanto para (KUROSE; ROSS, 2006), (NAKAMURA; GEUS, 2007) e (MORIMOTO, 2008) uma variante do ataque de DoS é o ataque de negação de serviço distribuído (*Distributed Denial of Service* – DDoS), representado na Figura 20, que tem como objetivo a invasão e coordenação de vários hosts distribuídos por um *hacker*, para realizar ataques simultâneos aos alvos escolhidos. Assim com a utilização de diversos tipos de vulnerabilidades em sistemas, o atacante consegue formar um *botnet*, instalando e executando um programa escravo em inúmeras máquinas, que continuam de forma aparentemente normal, executando suas tarefas, aguardando o comando de seu mestre. Assim que a *botnet* estiver com um grande número de máquinas infectadas, com poucos comandos o atacante consegue lançar um ataque de DDoS em algum alvo escolhido. (MORIMOTO, 2008).

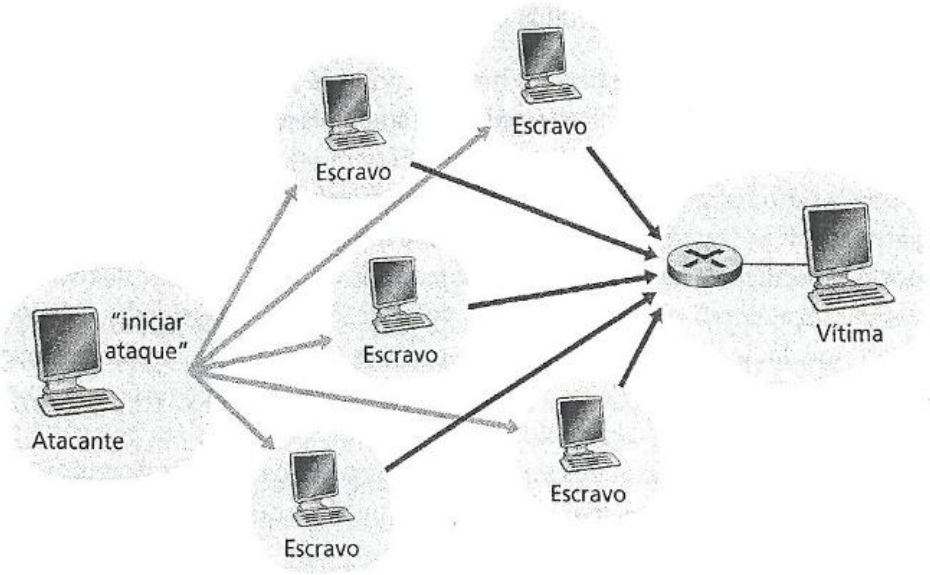


Figura 20 - DDoS

Fonte: (KUROSE; ROSS, 2006)

Um tipo importante de ataque passivo é o *scanning* de vulnerabilidades. Para isto, pode ser utilizado uma ferramenta de *port scanner.* Um dos mais utilizados é o *nmap*, que tem como funcionalidade, por meio do mapeamento de portas, a obtenção de informações de serviços que podem ser acessíveis. Assim o *scanner* de vulnerabilidades varre somente as vulnerabilidades especificas do que já foi identificado como alvo e os tipos de sistemas e serviços que neles são executados. Após checar os roteadores, serviços, *firewalls*, sistemas operacionais e outras entidades IP, alguns riscos podem ser analisados, como: compartilhamento de arquivos que não são protegidos por senhas; configurações incorretas; *softwares* desatualizados; falhas na camada de rede; configurações de roteadores potencialmente perigosas; checagem de senhas fáceis de serem adivinhadas; SNMP; e possibilidade de DoS. (NAKAMURA; GEUS, 2007).

Os ataques citados acima têm sua origem de fora da rede local, porém muito mais comuns são os ataques internos, ou seja, que tem origem dentro da própria rede (CRONKHITE; MCCULLOUGH, 2001). Tanto para (FELIPPETTI, 2008) como para (ODOM, 2003) algumas abordagens são essenciais para as políticas de segurança da rede local, como por exemplo, as listas de acesso (*Access List* - ACLs).

Para (FELIPPETTI, 2008, p.342):

> Listas de acesso são, essencialmente, listas de condições que controlam o acesso. Uma vez citadas, podem ser aplicadas tanto ao tráfego entrante (*inbound traffic*) quanto ao tráfego sainte (*outbound traffic*), em qualquer interface. A aplicação de listas de acesso fará com que o router examine cada pacote atravessando uma determinada interface em uma determinada direção e tome as providências apropriadas.

Assim as ACLs tem o objetivo: filtrar o tráfego indesejado da rede; encontrar pacotes com níveis de prioridades diferentes; e evitar que sistemas críticos sejam acessados por funcionários não designados. (ODOM, 2003).

Outra forma de proteger a rede interna é através da configuração de *Port Security,* que permite restringir uma porta do *switch* a um conjunto de endereços MAC. O administrador da rede pode configurar de forma estática quais os endereços MAC são permitidos para cada porta especifica ou de forma dinâmica, em que é necessário limitar o numero de endereços MAC que serão aprendidos. Assim a porta fornece acesso a quadros somente dos endereços que forem considerados seguros. (FROOM, 2010).

As portas protegidas pelo *Port Security* podem ser configuradas para responder de três maneiras (WATKINS; WALLACE, 2008):

- ✓ *Protect:* nesta configuração são bloqueados os quadros de endereços MAC de origem desconhecida, após atingir o numero limite de endereços possíveis a serem aprendidos

dinamicamente. Porém os quadros de endereços já cadastrados como seguros são transmitidos normalmente.

- ✓ *Restrict:* esta configuração é semelhante à *Protect*, porém ao ocorrer uma violação de porta além de ela ser bloqueada é enviado um *trap* de SNMP, uma mensagem de *syslog* e é incrementado um contador de violação.
- ✓ *Shutdown:* esta é a configuração mais rigorosa, pois além de ter todos os recursos da opção *Restrict*, ainda fecha a porta de forma que não haja mais tráfego transmitido por ela.

2.7 FERRAMENTAS UTILIZADAS

Para realizar esse trabalho a utilização de algumas ferramentas foi essencial, como por exemplo: o Iperf, para simular o tráfego em uma rede; o Wireshark, para capturar pacotes ou informações sobre o tráfego gerado; o GNS3, para poder simular o *firewall* ASA; o Nmap, para verificar os hosts e as vulnerabilidades de uma rede; e por fim o Cacti, para possibilitar o gerenciamento e análise dos equipamentos da rede. A seguir serão apresentados mais detalhes sobre cada um das ferramentas.

2.7.1 Iperf

É uma ferramenta criada pela NLANR/DAST que tem como objetivo de medir tanto em TCP quando em UDP o desempenho da largura de banda em redes de computadores. Para isto, é introduzido pacotes na rede de acordo com os vários parâmetros e características que podem ser ajustados. Outra importante funcionalidade é a visualização de relatórios periódicos, indicando a taxa de transmissão, o *jitter* e da perda de pacotes. (Iperf, 2013). Como o Iperf não tem interface gráfica, foi desenvolvido o Jperf, um *software* que é executado em Java, com uma interface amigável, para a configuração e execução do Iperf (Figura 21).

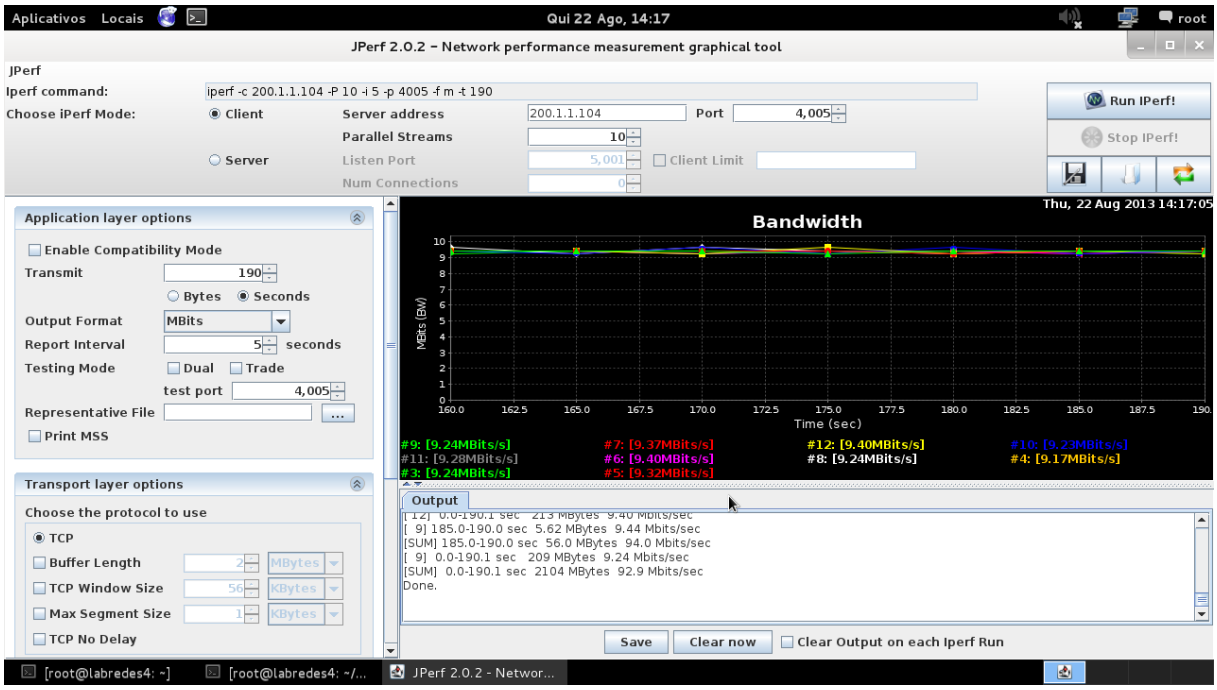


Figura 21 - Jperf

Fonte: autoria própria

A muitas opções de configurações que podem ser utilizadas no Iperf, porém os principais comandos são:

- ✓ -s: executa o Iperf no modo servidor;
- ✓ -c: executa o Iperf no modo cliente;
- ✓ -P: número de conexões paralelas permitidas;
- ✓ -p: a porta em que vai ser estabelecida a conexão;
- ✓ -i: intervalo em segundos que será reportado o status;
- ✓ -f: o formato das informações;
- ✓ -t: o tempo da transmissão.

2.7.2 Wireshark

O Wireshark é um *software* multiplataforma que tem como objetivo capturar o tráfego da rede. Com ele é possível capturar informações da rede ou do próprio computador e fazer análises do tráfego e dos protocolos encontrados. Um exemplo é apresentado na Figura 22. O Wireshark é um programa de código aberto. Seu projeto começou em 1998 e cresce até hoje com a contribuição de especialistas em redes do mundo todo. (Wireshark, 2013).

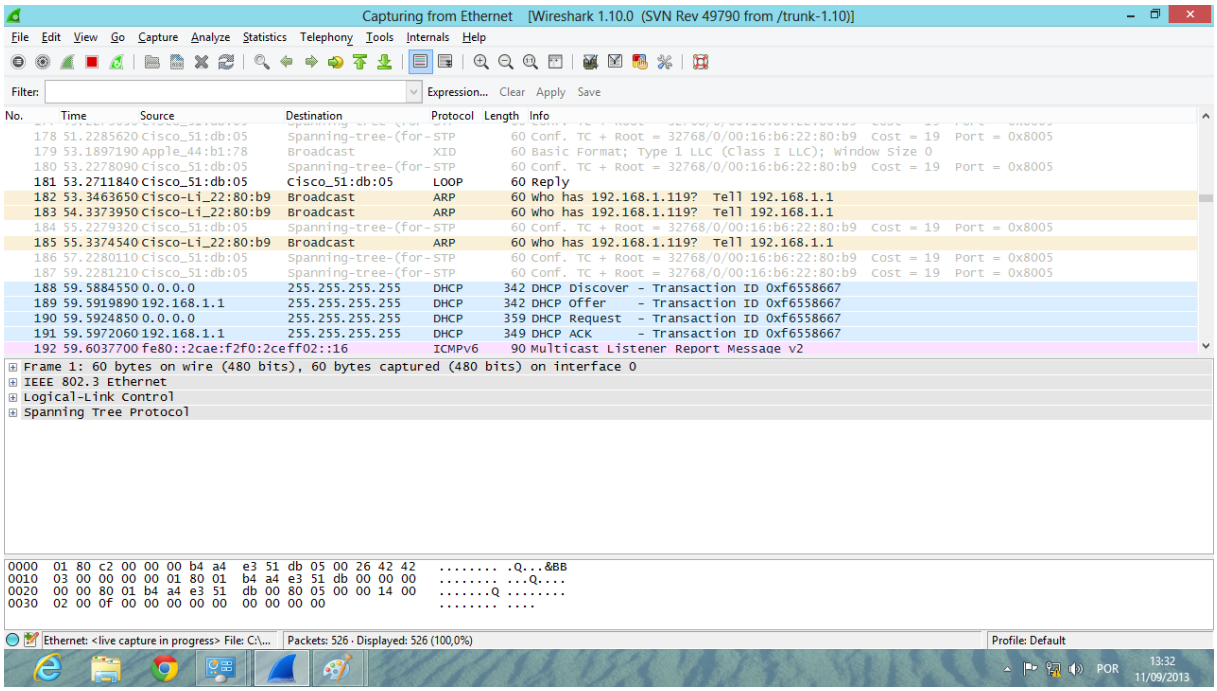


Figura 22 - Wireshark

Fonte: autoria própria

2.7.3 GNS3

O GNS3 (Figura 23) tem o objetivo de simular redes virtuais complexas, da forma mais próxima das redes reais, sem a utilização de um *hardware* de redes físico, sendo uma boa ferramenta complementar para laboratórios e estudantes que atuam na área de redes de computadores e telecomunicações. Com o GNS3, pode-se testar configurações e analisar características que possam futuramente ser implementadas em equipamentos reais. É um *software* de código aberto, com uma interface gráfica intuitiva e que permite ser executado em vários sistemas operacionais, como Windows, Linux e MacOS X. (GNS3, 2013).

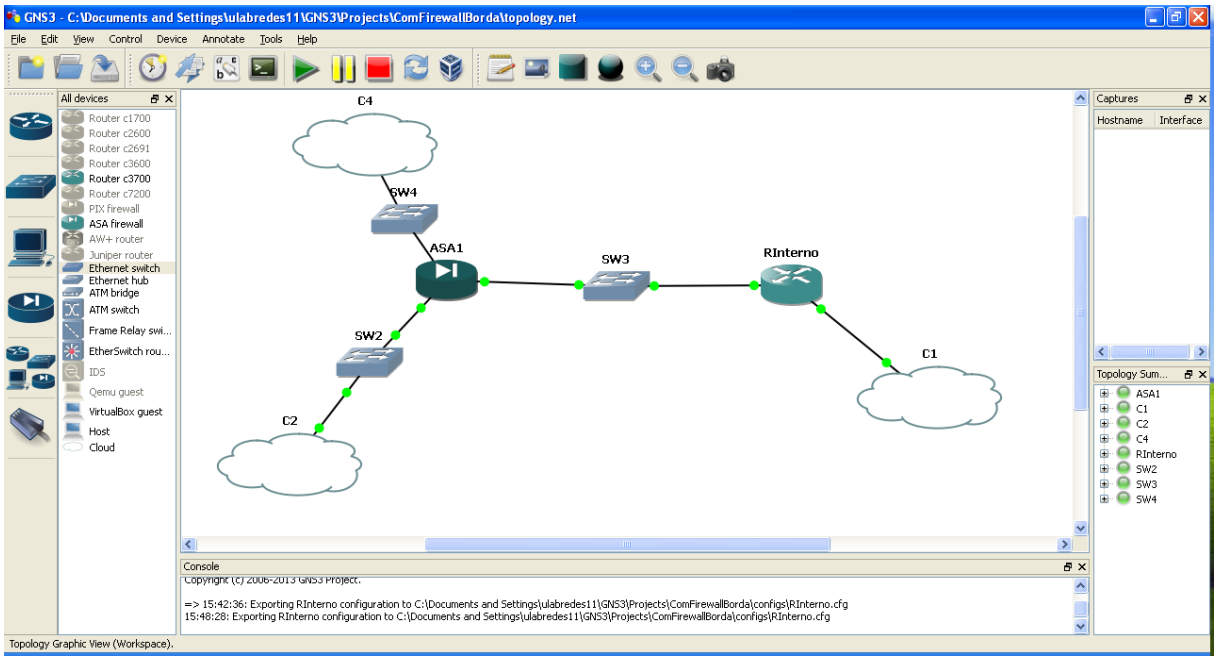


Figura 23 - GNS3

Fonte: autoria própria

2.7.4 Nmap

O Nmap é um *software* de código aberto, que tem como um dos objetivos ajudar administradores e auditores a explorar suas redes, a fim de torná-las mais seguras, pois disponibiliza descoberta de rede, auditoria de segurança, inventário de rede, gerenciamento de agendas de atualizações de serviços e monitoramento de hosts ou serviços *uptime*. É uma poderosa ferramenta que permite determinar várias características da rede, como por exemplo, quais *hosts* estão disponíveis na rede, quais são oferecidos, quais os sistemas operacionais estão sendo executados nas máquinas e qual o tipo de filtro de pacotes. Pode ser executado nos principais sistemas operacionais. Disponibiliza o Zenmap, que é uma interface gráfica avançada e visualizador de resultados, apresentado na Figura 24. (Nmap, 2013).

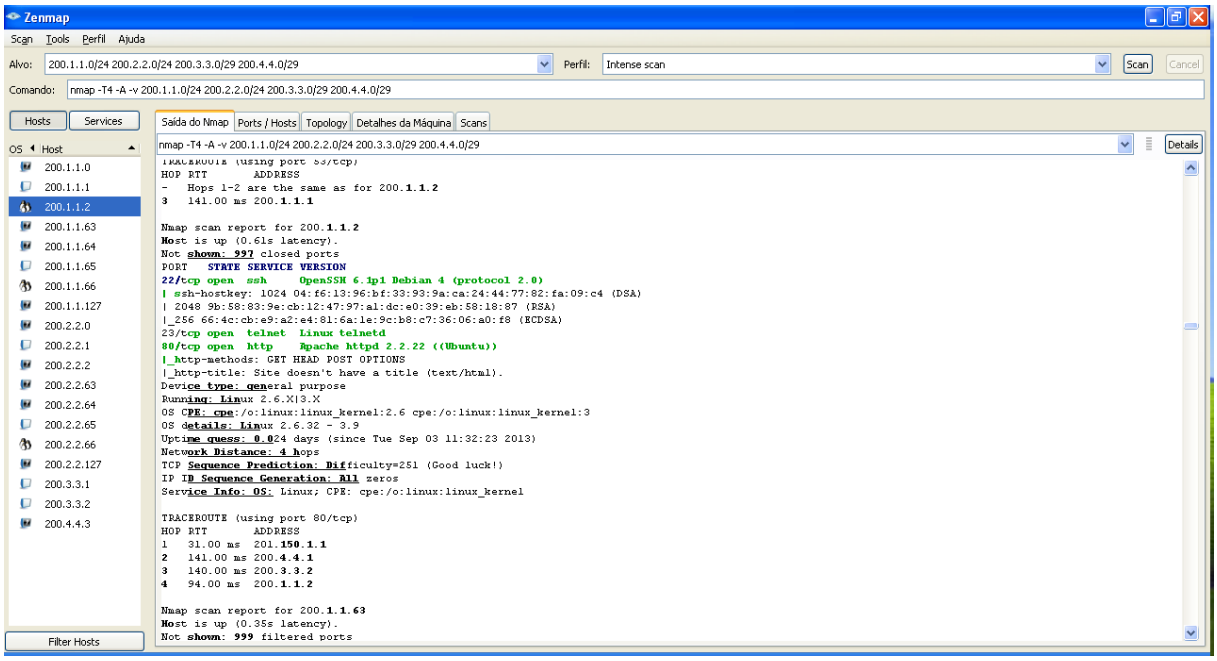


Figura 24 - Zenmap

Fonte: autoria própria

2.7.5 Cacti

O Cacti tem como objetivo coletar e consolidar informações, através de gráficos, do estado, atuando desde redes simples até redes complexas. Com isto é possível monitorar e gerenciar uma rede a partir de uma interface Web (Figura 25). Para dispositivos que suportem o SNMP a consulta de informações de rede e programas é feito pelo protocolo. É um *software* livre de administração de redes que disponibiliza *plugins* para a expansão de novas funcionalidades. (Cacti®, 2013).

Figura 25 - Cacti

Fonte: autoria própria

3 ESTUDO DE CASO

Os casos que foram estudados foram divididos em três grandes grupos: os testes de QoS, os testes de segurança e os testes de gerenciamento. Nos testes de QoS, foram necessários cinco cenários de testes para demonstrar a importância da sua implementação. Para os testes de segurança foi preciso quatro cenários de testes, divididos em dois para segurança interna e dois para segurança externa. Por fim, para os testes de gerenciamento apenas um único cenário foi suficiente para se avaliar quais as vantagens da utilização do gerenciamento de redes.

3.1 TESTES DE QoS

Para demonstrar a importância da aplicação de políticas de QoS em redes de computadores, foram necessários cinco cenários de testes. Para todos os cenários de testes de QoS, foram utilizados o Iperf para gerar tráfego entre as máquinas e o Wireshark para analisar esse tráfego. Para isso foram utilizados dois computadores, um como cliente e outro como servidor, para a simulação da comunicação de dados. Em paralelo, foram utilizados outros dois computadores, um cliente e outro servidor, para simular a troca de informações em uma conversa utilizando VoIP (voz).

3.1.1 Primeiro Cenário de QoS

O primeiro cenário de QoS (Figura 26) é representado por dois *switches* camada 2 interligados entre si somente com a VLAN padrão dos switches gerenciáveis, ou seja, a VLAN 1 que já vem criada e pronta para uso.

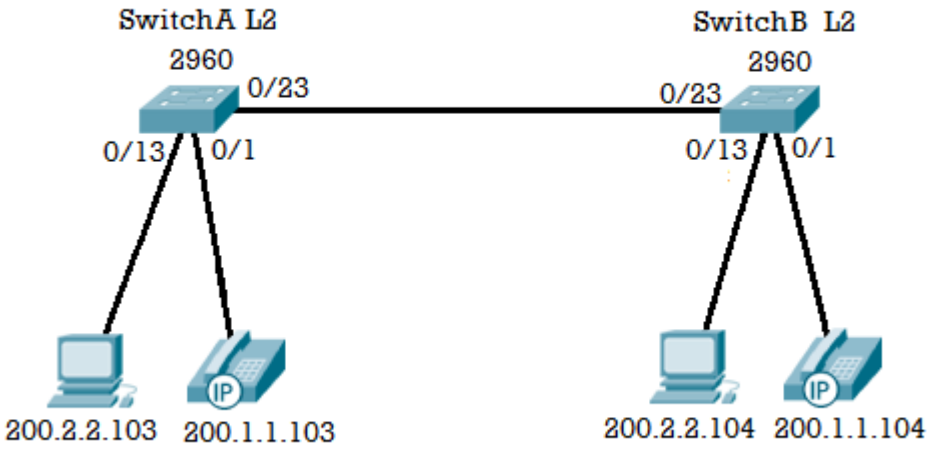


Figura 26 - Cenário 1 de QoS

Fonte: autoria própria

Para esse teste foram utilizadas as máquinas do SwitchA como clientes e as máquinas do SwitchB como servidores. Em cada computador foi configurado seu respectivo comando no Jperf:

- ✓ Servidor de Dados: iperf -s -P 10 -i 5 -p 4005 -f m
- ✓ Servidor de Voz: iperf -s -i 5 -p 5001 -f m
- ✓ Cliente de Dados: iperf -c 200.2.2.104 -P 10 -i 5 -p 4005 -f m -t 190
- ✓ Cliente de Voz: iperf -c 200.1.1.104 -i 5 -p 5001 -f m -t 190

O protocolo utilizado foi o TCP, sendo que o cliente de voz permite somente uma conexão, enquanto o cliente de Dados permite dez conexões simultâneas.

Para os *switches* A e B foram utilizadas as configurações padrões de fábrica, em que todas as portas estão na VLAN 1, que por default não vem aplicado nenhum serviço, como por exemplo, QoS e *port security.*

O *software* Iperf foi utilizado para gerar tráfego entre as máquinas interligadas (cliente/servidor). Com a inicialização deste *software*, foi utilizado o Wireshark (analisador de protocolos) para capturar e verificar o comportamento do tráfego gerado. A Figura 27 mostra a quantidade de *bits* por segundo (bps) analisados na comunicação entre as máquinas que estavam simulando o envio de dados, enquanto a Figura 28 mostra a simulação do envio de pacotes de voz.

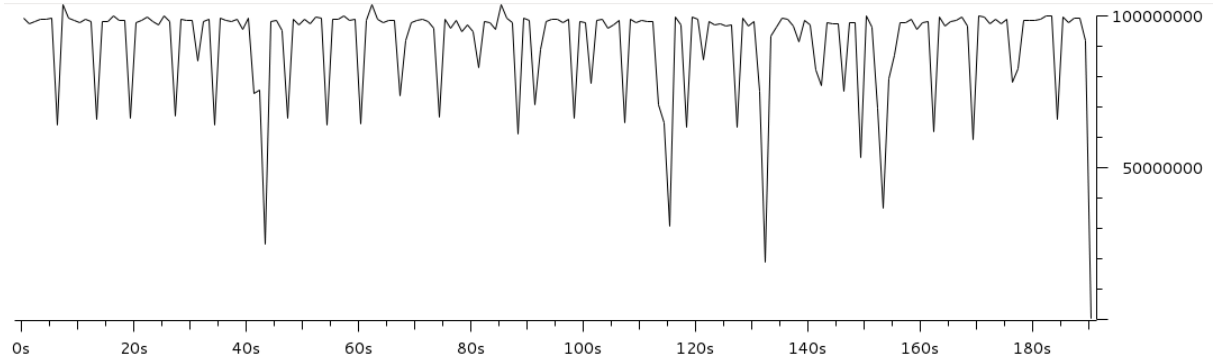


Figura 27 - Gráfico do servidor de Dados (Cenário 1 QoS)

Fonte: autoria própria

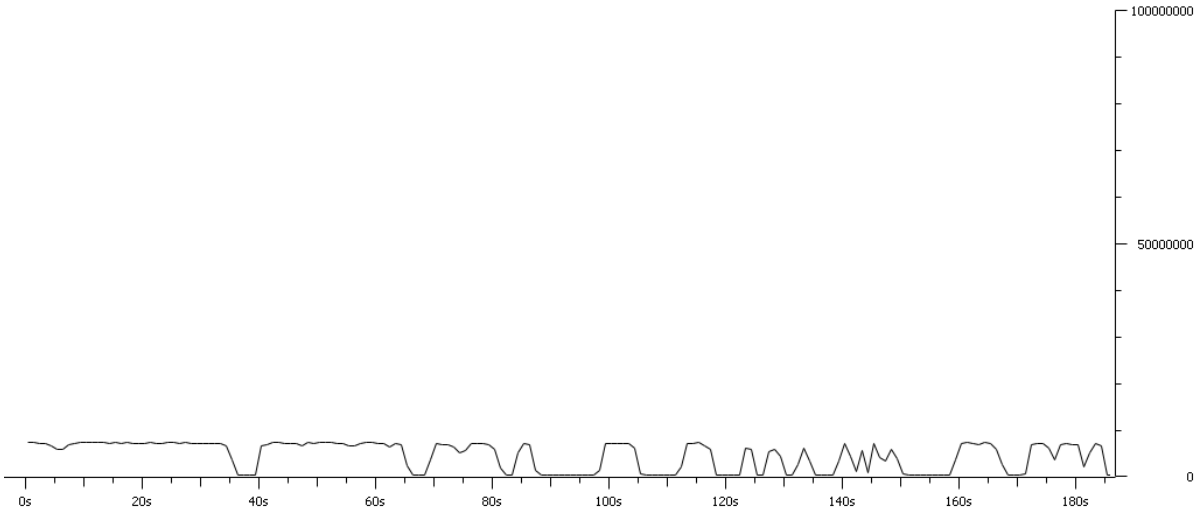


Figura 28 - Gráfico do servidor de Voz (Cenário 1 QoS)

Fonte: autoria própria

A Figura 27 apresenta, na maior parte do teste, que o enlace está sendo utilizado em 100% (100 Mbps). Isto é uma característica do padrão "*Best Effort*" que tenta utilizar o máximo da taxa de transmissão do enlace. O problema deste padrão é que, como todas as comunicações tentam utilizar ao máximo a banda disponível, podem ocorrer descartes de pacotes. Nem sempre o enlace consegue atender os usuários com a maior taxa de transmissão possível para todos. Isto pode ocasionar perda de pacotes e também elevar o *delay/jitter* em casos de congestionamento.

Na Figura 28, pode-se verificar que em alguns momentos, o tráfego de pacotes de voz chega a uma taxa de transmissão de 0 bps, ou seja, neste intervalo as máquinas não conseguem transmitir nenhuma informação de voz. Isso acontece porque, o congestionamento

das 11 conexões simultâneas, que estão enviando dados, tentam utilizar toda a taxa de transmissão do *switch* (*best effort*), concorrendo entre si pela taxa de transmissão disponível. Como o serviço de voz é sensível ao *jitter* e a perda excessiva de pacotes, este tipo de implementação pode tornar inviável uma comunicação de voz utilizando este modelo.

3.1.2 Segundo Cenário de QoS

O segundo cenário de QoS (Figura 29) contêm todos os componentes do primeiro cenário, porem foram criadas duas VLANs, separando o domínio de *broadcast*, a 10 de voz e a 20 de dados.

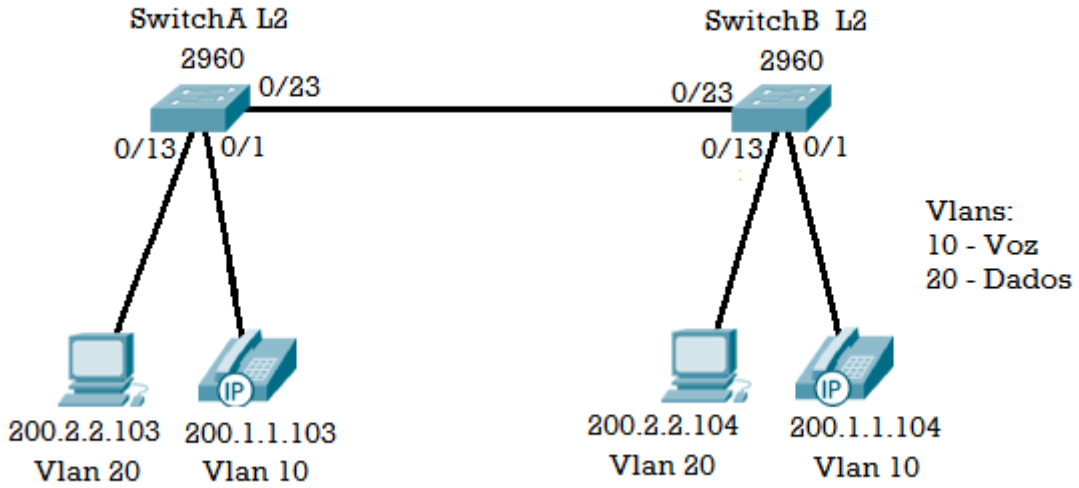


Figura 29 - Cenário 2 de QoS

Fonte: autoria própria

Para gerar tráfego na rede foram executados os mesmos comandos especificados no Cenário 1 de QoS no Jperf de cada máquina. As configurações para a criação das VLANs nos *switches* A e B estão apresentadas no Apêndice A.

Foram gerados pacotes pelo Jperf e ao capturar as informações pelo Wireshark (em bps), os resultados são apresentados na Figura 30 (Dados) e na Figura 31 (Voz).

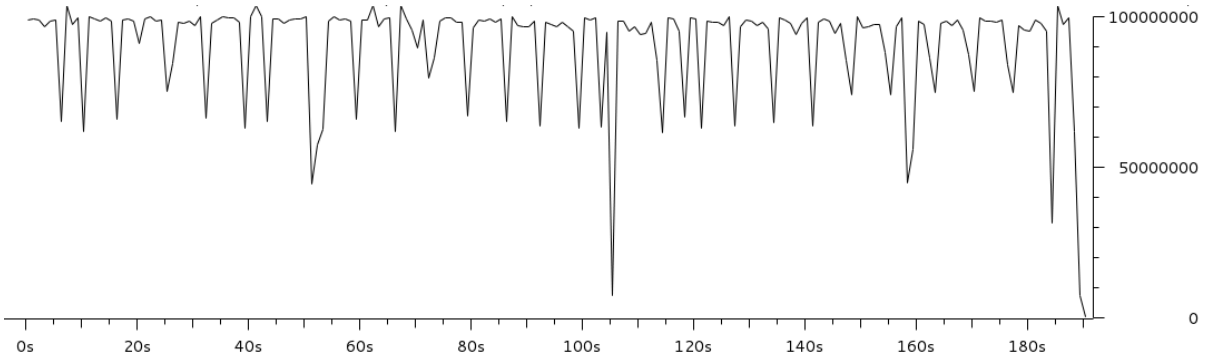


Figura 30 - Gráfico do servidor de Dados (Cenário 2 QoS)

Fonte: autoria própria

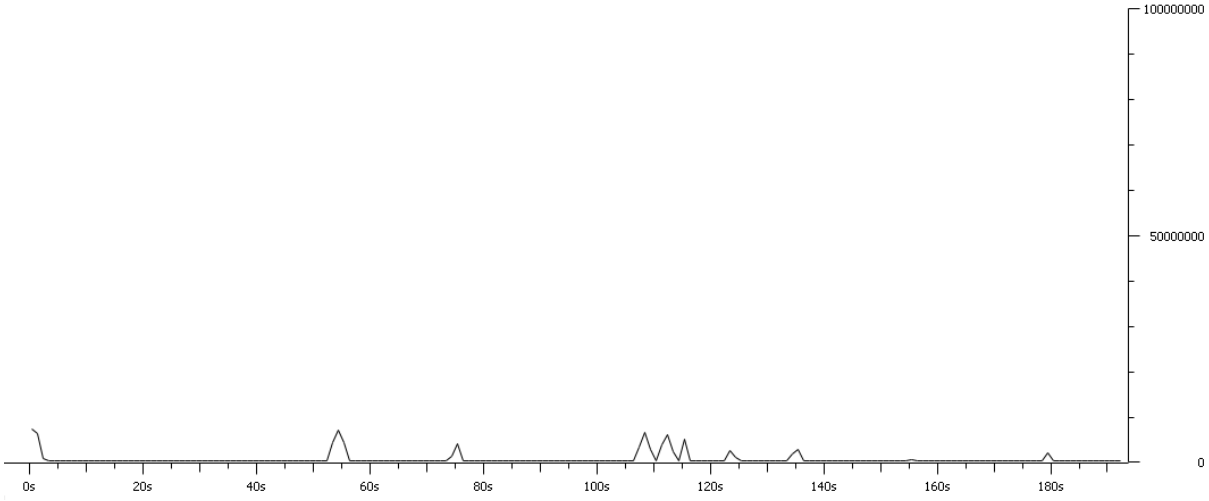


Figura 31 - Gráfico do servidor de Voz (Cenário 2 QoS)

Fonte: autoria própria

Pode-se verificar que mesmo com a criação das VLANs e a quebra o domínio de *broadcast*, a situação continua parecida com o cenário 1 de QoS. Isto se dá, porque a interligação de tronco entre o SwitchA e o SwitchB está sendo compartilhada entre as duas VLANs (Dados e Voz). Isto significa que nessa interface de tronco, as comunicações estão tentando utilizar o máximo da banda de dados disponíveis dos *switches* (*best effort*). A Figura 31 apresenta em alguns momentos a taxa e transmissão próxima ou igual a 0 bps. Este tipo de situação inviabiliza a transmissão do serviço de voz, que exige um mínimo de taxa de transmissão e *jitter*.

3.1.3 Terceiro Cenário de QoS

O terceiro cenário de QoS (Figura 32), além da criação das VLANs de Dados e Voz, foi configurado um switch camada 3 para fazer o roteamento entre o SwitchA e o SwitchB.

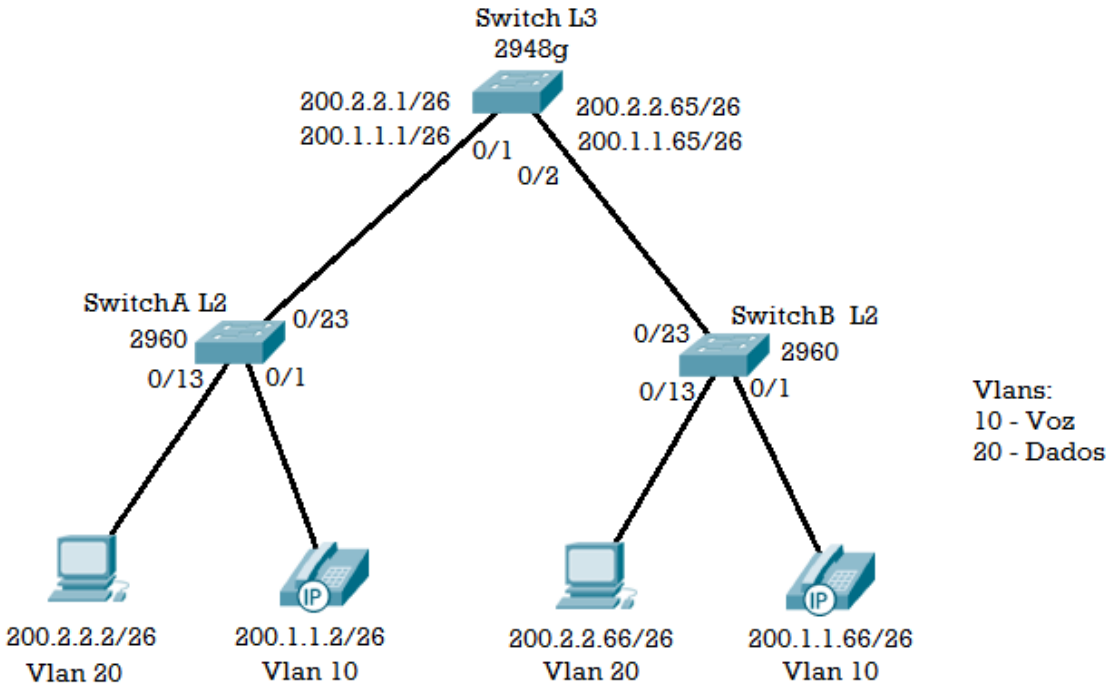


Figura 32 - Cenário 3 de QoS

Fonte: autoria própria

Para esse teste também foram utilizadas as máquinas do SwitchA como clientes e as máquinas do SwitchB como servidores. Em cada computador foi configurado seu respectivo comando no Jperf:

- ✓ Servidor de Dados: iperf -s -P 10 -i 5 -p 4005 -f m
- ✓ Servidor de Voz: iperf -s -i 5 -p 5001 -f m
- ✓ Cliente de Dados: iperf -c 200.2.2.66 -P 10 -i 5 -p 4005 -f m -t 190
- ✓ Cliente de Voz: iperf -c 200.1.1.66 -i 5 -p 5001 -f m -t 190

O cliente de voz continua permitindo somente uma conexão, enquanto o cliente de dados permite dez conexões simultâneas e o protocolo utilizado foi o TCP. As configurações utilizadas no *Switch* camada 3 são apresentadas no Apêndice B.

Assim ao gerar tráfego na rede pelo Iperf e capturar as informações pelo Wireshark (em bps), foram obtidos os resultados apresentados na Figura 33 (Dados) e na Figura 34 (Voz).

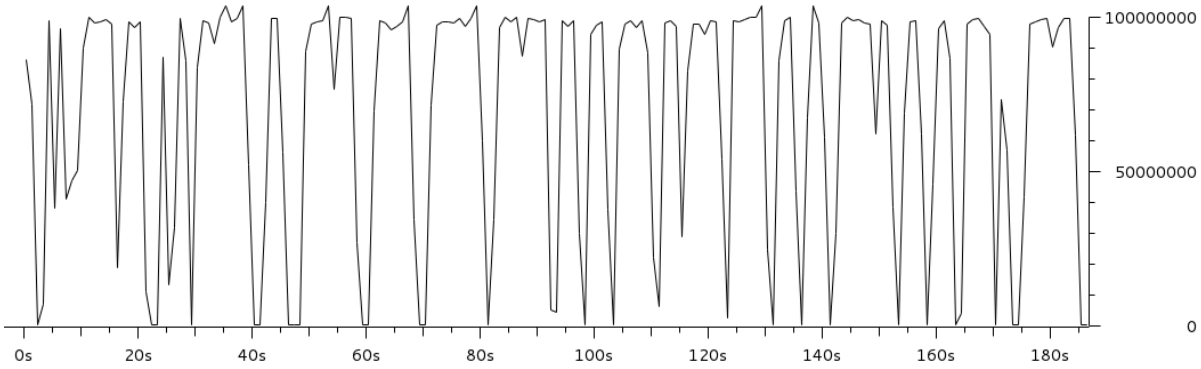


Figura 33 - Gráfico do servidor de Dados (Cenário 3 QoS)

Fonte: autoria própria

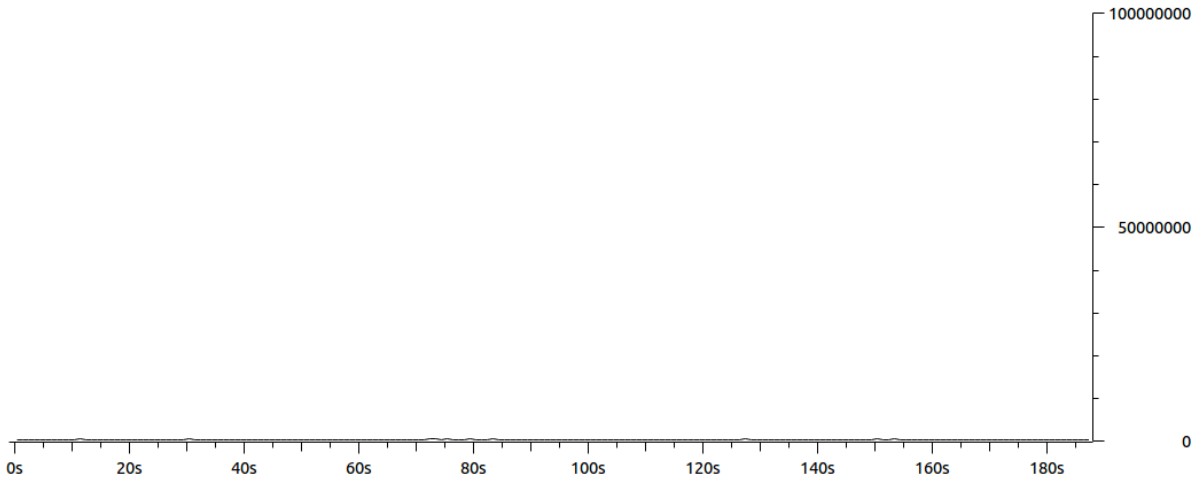


Figura 34 - Gráfico do servidor de Voz (Cenário 3 QoS)

Fonte: autoria própria

Mesmo com a configuração do switch camada 3, a situação da comunicação de Voz é pior que a do cenário 1 e 2 de QoS. Isto se dá, porque neste cenário há a ligação do SwitchL3 com os SwitchA e SwitchB, em que é feito o roteamento entre as duas VLANs (Dados e Voz). Isto significa que nessas interfaces de tronco, as comunicações estão tentando utilizar não somente o máximo da banda de dados disponíveis (*best effort*) nos *switches* A e B, mas agora também no *switch* camada 3. A Figura 34 apresenta que em vários momentos a taxa de

transmissão igual a 0 bps, este tipo de situação continua inviabilizando a transmissão do serviço de voz, que exige um mínimo de taxa de transmissão e *jitter*.

3.1.4 Quarto Cenário de QoS

O quarto cenário de QoS (Figura 35) contem todos os componentes do segundo cenário e as duas VLANs criadas (Voz e Dados), porem foram aplicados os conceitos de QoS nos *switches* A e B.

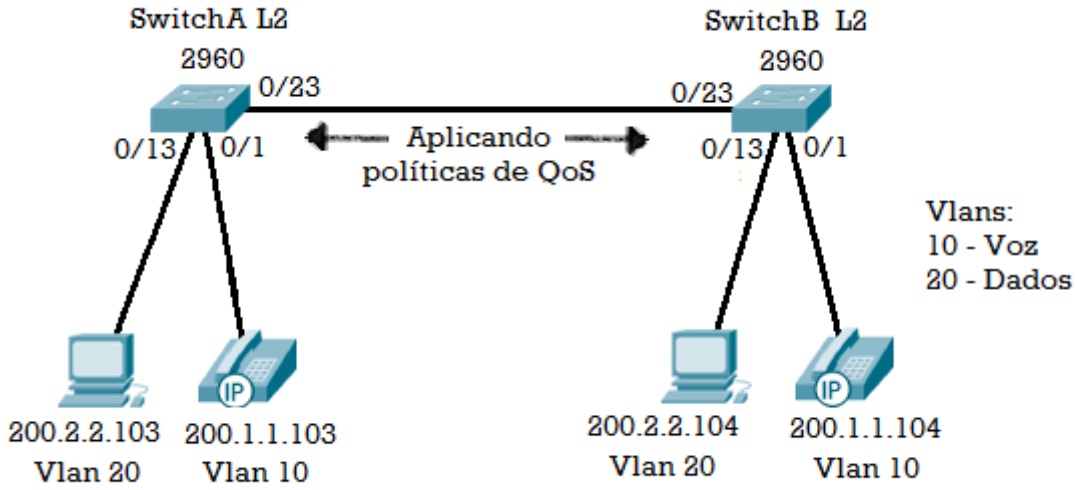


Figura 35 - Cenário 4 de QoS

Fonte: autoria própria

Para gerar tráfego na rede foram executados os mesmos comandos especificados no Cenário 1 de QoS no Jperf de cada máquina.

As configurações aplicadas nos *switches* A e B, para a configuração de QoS estão apresentadas no Apêndice C. Os custos utilizados nas VLANs foram escolhidos conforme a Figura 36, que apresenta as 11 principais classes de tráfego que podem ser utilizadas nos switches Cisco Catalyst 2960. Sendo assim, a VLAN 10 de Voz foi configurada com custo 5 (*Voice*) e a VLAN 2 de Dados com custo 0 (*Best Effort*).

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 36 - Principais classes de tráfego

Fonte: (SYSTEMS INC, Cisco. 2013)

Da mesma forma dos outros cenários, foram gerados pacotes pelo Jperf e ao capturar as informações pelo Wireshark (em bps), os resultados estão apresentados na Figura 37 (Dados) e na Figura 38 (Voz).

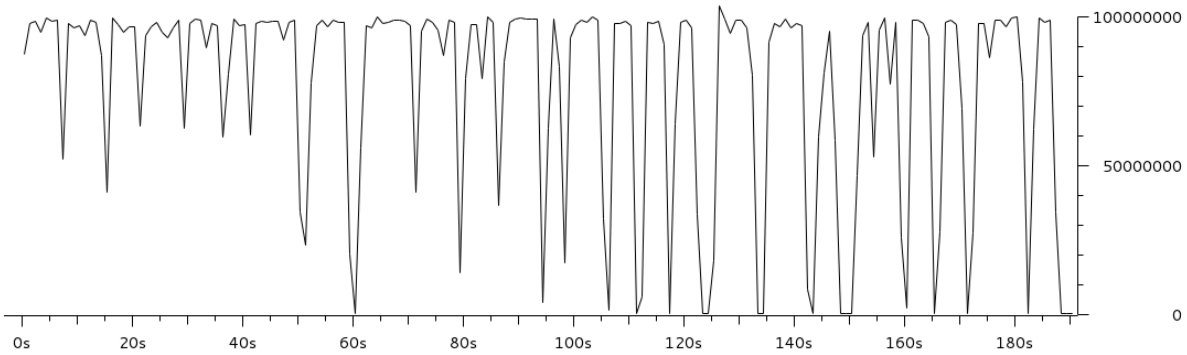


Figura 37 - Gráfico do servidor de Dados (Cenário 4 QoS)

Fonte: autoria própria

Figura 38 - Gráfico do servidor de Voz (Cenário 4 QoS)

Fonte: autoria própria

Conforme a Figura 38, pode-se verificar que com a aplicação de custos de QoS nas VLANs (Voz e Dados), não há quedas drásticas na taxa de transmissão, permanecendo estável, em torno de 4 Mbps. Tornando assim viável a transmissão de serviços VoIP.

3.1.5 Quinto Cenário de QoS

O quinto cenário de QoS (Figura 39) contem todos os componentes do terceiro cenário, porem foram aplicados os conceitos de QoS nos *switches* A e B.

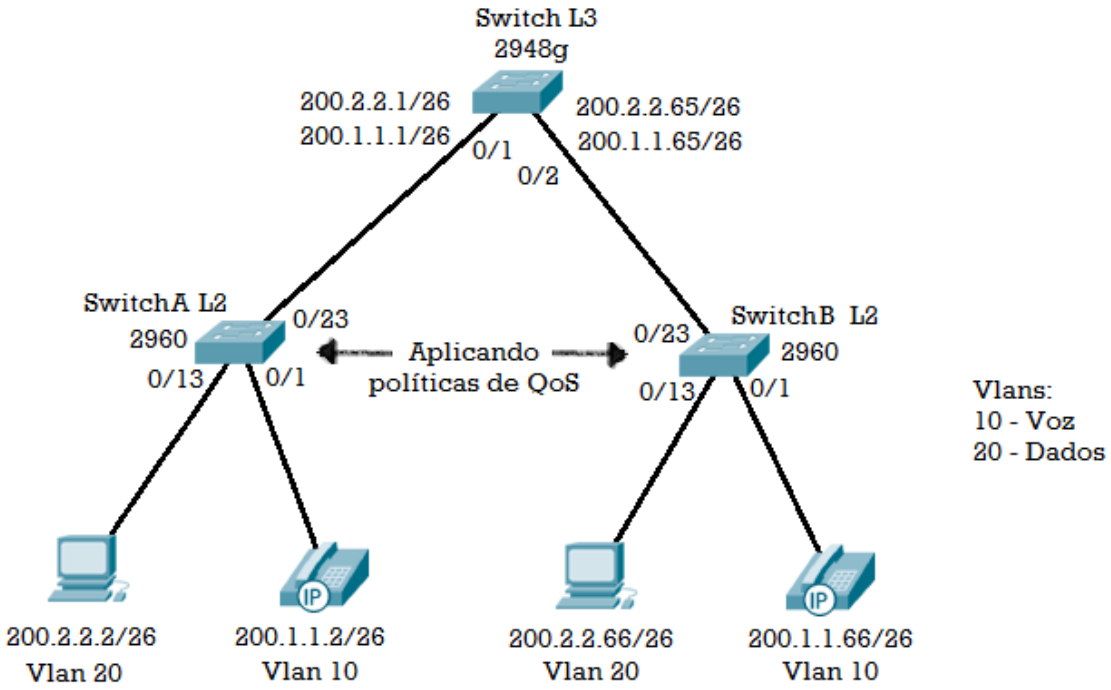


Figura 39 - Cenário 5 de QoS

Fonte: autoria própria

Para gerar tráfego na rede foram executados os mesmos comandos especificados no cenário 3 de QoS no Jperf de cada máquina.

Como no cenário 4, as configurações aplicadas nos *switches* A e B, para a configuração de QoS estão apresentadas no Apêndice C e os custos utilizados nas VLANs foram: 5 (*Voice*) para a VLAN 10 de Voz e 0 (*Best Effort*) para a VLAN 2 de Dados.

Da mesma forma dos outros cenários foram gerados pacotes pelo Jperf e ao capturar as informações pelo Wireshark (em bps), os resultados estão apresentados na Figura 40 (Dados) e Figura 41 na (Voz).

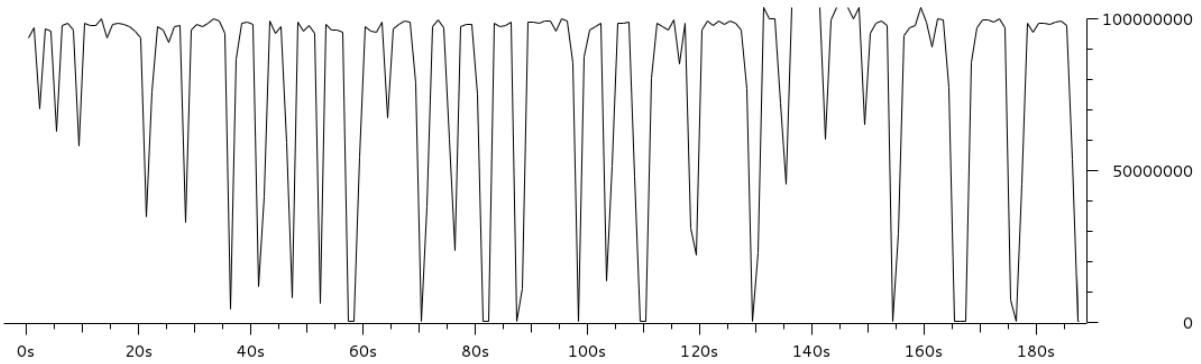


Figura 40 - Gráfico do servidor de Dados (Cenário 5 QoS)

Fonte: autoria própria

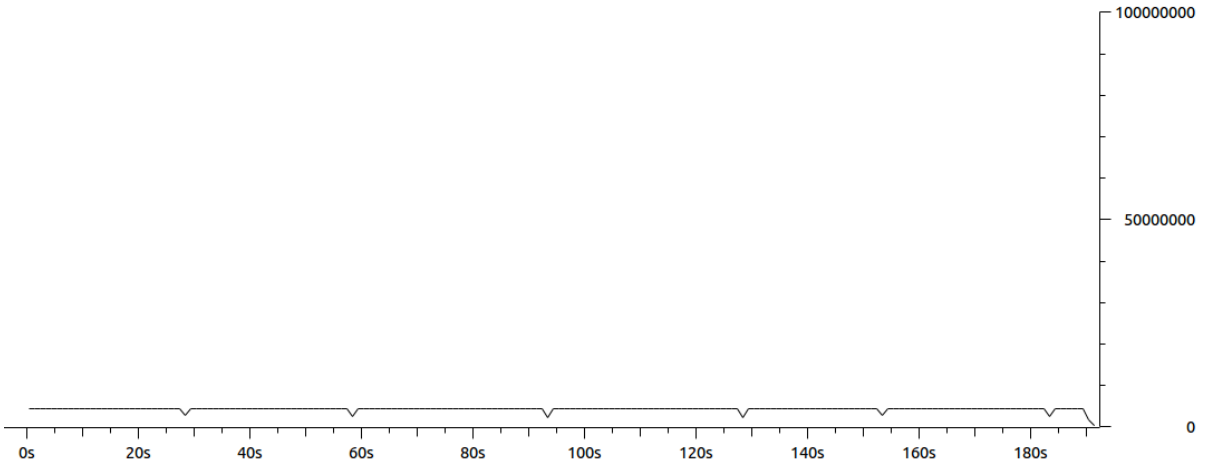


Figura 41 - Gráfico do servidor de Voz (Cenário 5 QoS)

Fonte: autoria própria

Conforme a, pode-se verificar que com a aplicação de custos de QoS nas VLANs (Voz e Dados), não há quedas drásticas na taxa de transmissão, permanecendo estável, em torno de 4 Mbps. Tornando assim viável a transmissão de serviços VoIP.

Outra demonstração de que o tráfego está ocorrendo de forma viável para a comunicação do serviço de voz, seria a Figura 42, que é a representação da taxa de transmissão utilizada pela máquina cliente. Nela é possível verificar que a média da taxa de transmissão está em 3,77 Mbps.

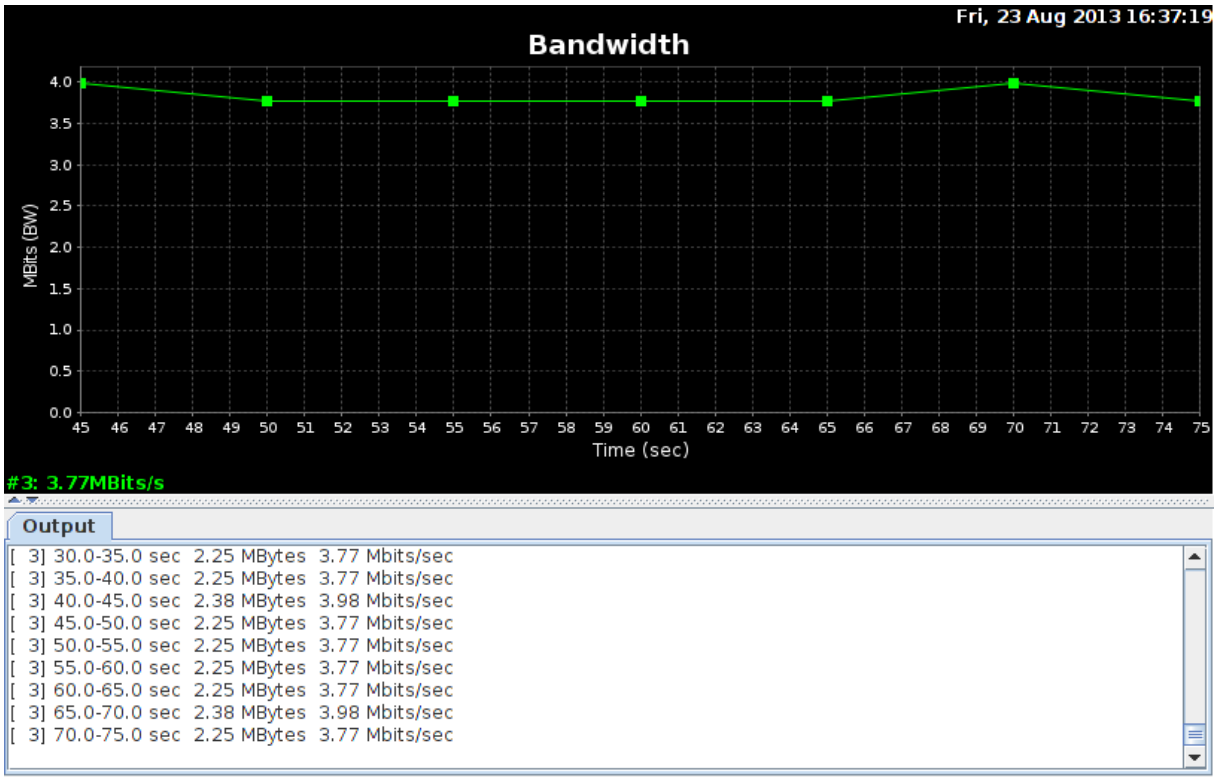


Figura 42 - Gráfico cliente de Voz (Cenário 5 QoS)

Fonte: autoria própria

3.2 TESTES DE SEGURANÇA

Para demonstrar a importância de questões de segurança em redes de computadores, foi necessário quatro cenários de teste. Os dois primeiros cenários representam a segurança de invasores e ataques externos e os dois últimos cenários contemplam a segurança interna da rede, ou seja, invasores e ataques dentro da própria rede local (*insiders*).

3.2.1 Primeiro Cenário de Segurança

O primeiro cenário de segurança (Figura 43) representa uma rede local ligada diretamente a Internet.

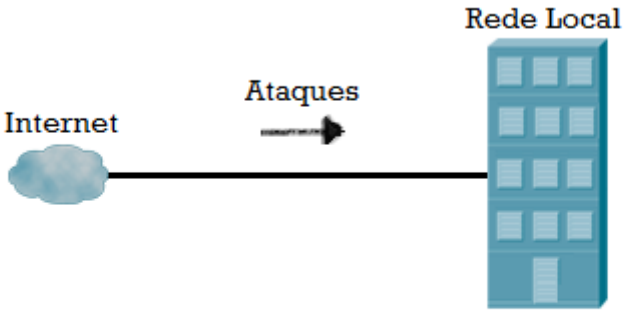


Figura 43 - Cenário 1 de segurança

Fonte: autoria própria

Para a configuração desse cenário foi necessário à utilização do *software* GNS3. A rede implementada, com seus equipamentos e divisões de IPs está representada na Figura 44, onde a rede interna é a configuração apresentada no quinto cenário de QoS (Figura 39) e a rede externa representa o computador invasor.

Figura 44 - Configuração da rede sem segurança externa

Fonte: autoria própria

Na rede interna representada pela nuvem, as configuração de rede foram as mesmas utilizados no cenário 5 dos testes de QoS que estão nos Apêndices A, B e C.

Tanto o roteador interno quando o roteador de borda, que faz a ligação da rede interna com a rede externa, têm as configurações realizadas no Apêndice D.

Após todos os equipamentos configurados, foi utilizado o Nmap instalado da maquina do invasor, ou seja, de um computador na rede externa, para fazer a varredura (*scanner*) das possíveis vulnerabilidades. Nele foi apresentado um mapa de todos os *hosts* existentes na rede (Figura 45), os status de cada porta de todos os *hosts* (Figura 46) e até outras informações como, o sistema operacional em que esta rodando cada máquina (Figura 47).

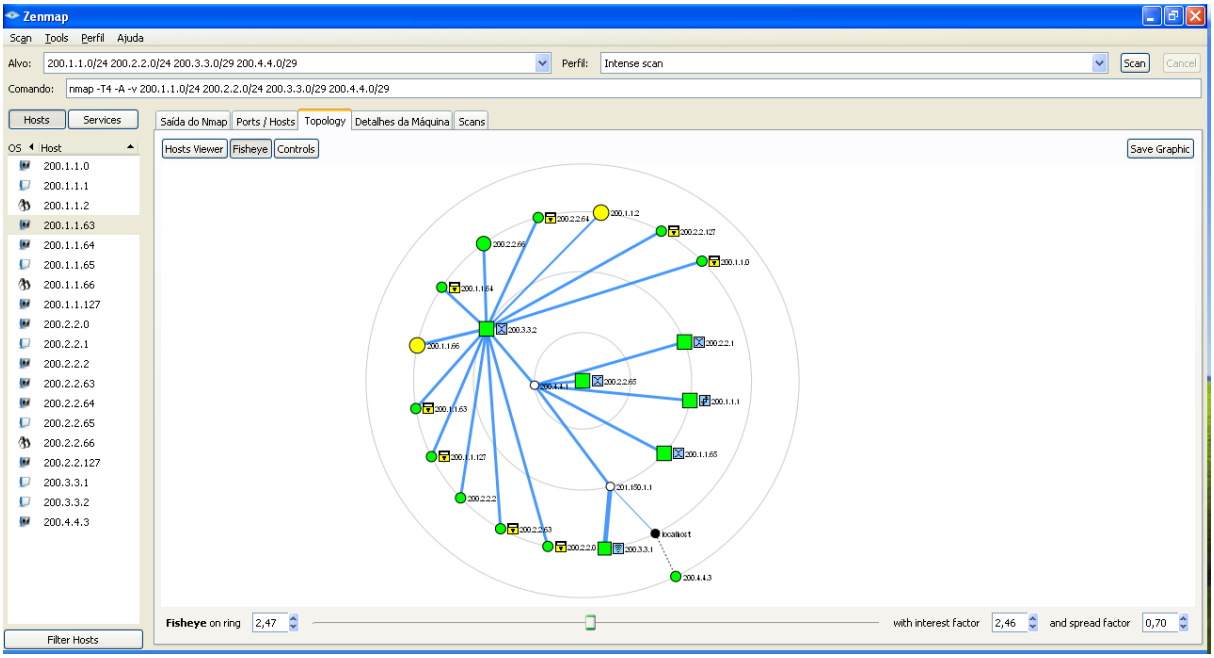


Figura 45 - Mapa de *hosts* (sem segurança externa)

Fonte: autoria própria

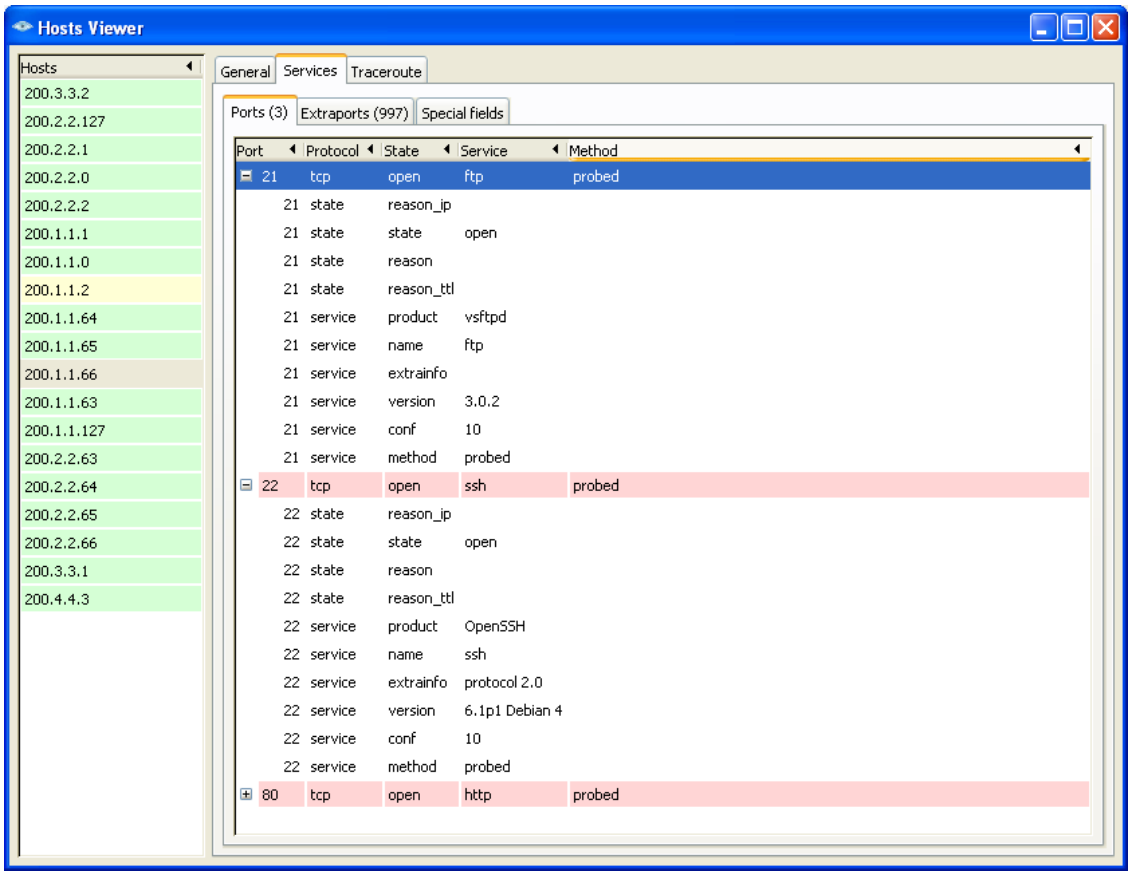


Figura 46 - Status das portas (sem segurança externa)

Fonte: autoria própria

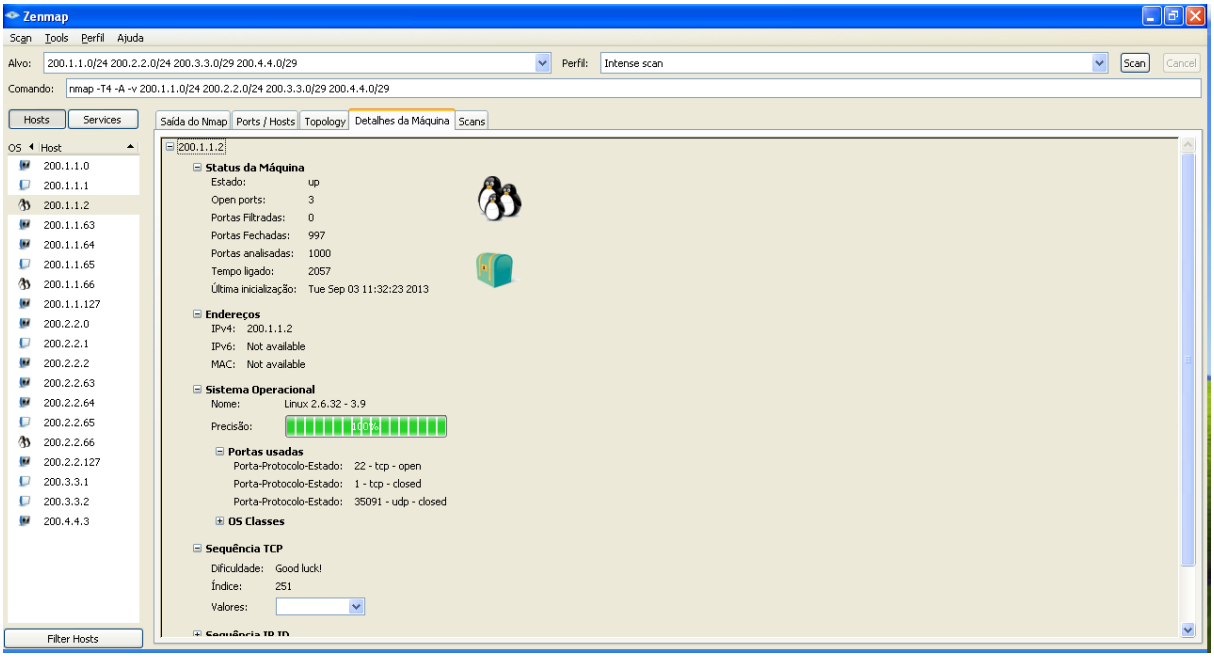
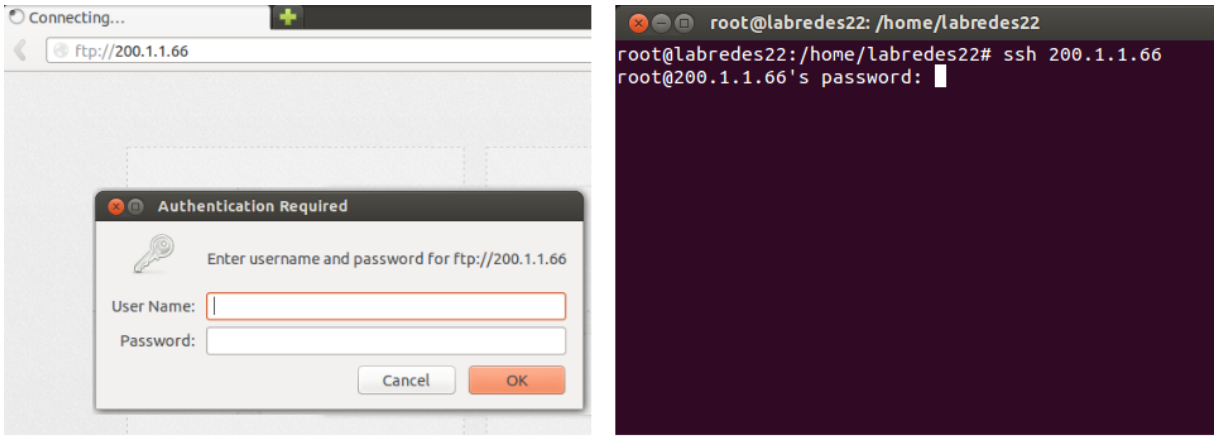


Figura 47 - Informações da máquina (sem segurança externa)

Fonte: autoria própria

Com esta configuração sem segurança, também fica possível acessar de fora da rede conexões de FTP (Figura 48 A) e SSH (Figura 48 B). Fazendo assim, com que a rede interna fique mais vulnerável a ataques externos.



(A) (B)

Figura 48 - Conexões FTP e SSH (sem segurança externa)

Fonte: autoria própria

A Figura 48 mostra tentativas de conexões feitas pelo computador localizado na rede externa utilizando os protocolos FTP e SSH. Como atualmente existem diversos tipos de ferramentas de ataque por força bruta e como a máquina remota tem acesso direto ao servidor interno, é possível que, em uma configuração de senha fraca, um invasor possa ter acesso aos serviços que seriam disponibilizados apenas para os usuários internos.

3.2.2 Segundo Cenário de Segurança

O segundo cenário de segurança (Figura 49) representa uma rede local ligada a Internet por meio de um *firewall*.

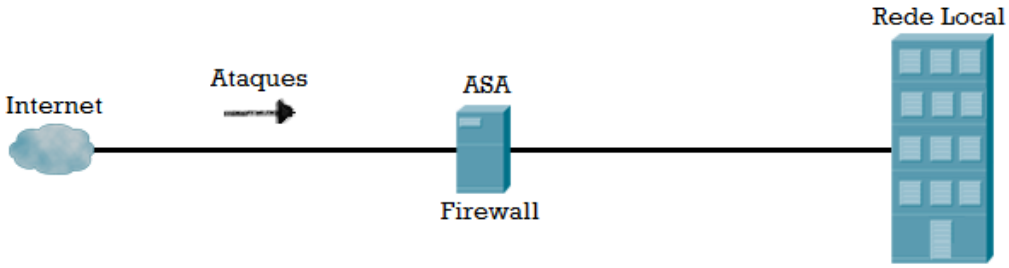


Figura 49 - Cenário 2 de segurança

Fonte: autoria própria

Para a configuração desse cenário também foi necessário à utilização do *software* GNS3. A rede implementada, com seus equipamentos e divisões de IPs, está representada na Figura 50, onde a rede interna é a configuração apresentada no quinto cenário de QoS (Figura 39), o invasor representa um computador que tenta acesso externo, e a rede de gerencia foi configurada somente para possibilitar a utilização do ASDM, a interface gráfica do ASA disponibilizada pela Cisco.

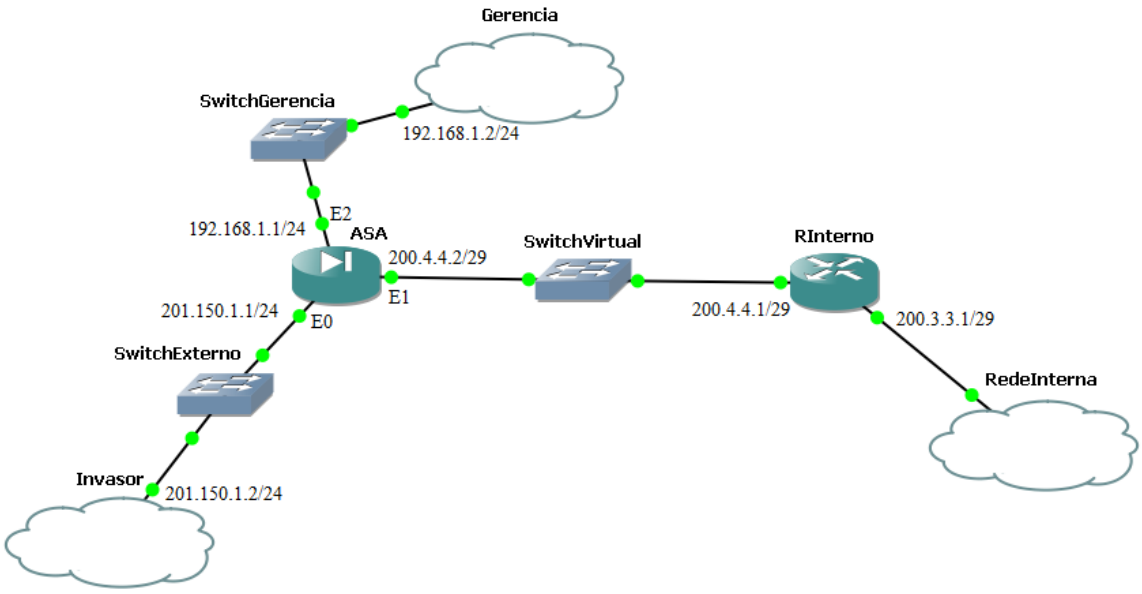


Figura 50 - Configuração da rede com segurança externa

Fonte: autoria própria

Tanto para o roteador interno quanto para o resto da rede interna representada pela nuvem, as configuração de rede foram as mesmas utilizados no cenário 5 dos testes de QoS que estão nos Apêndices A, B e C.

O ASA faz a ligação tanto da rede interna, quanto da rede do invasor e ainda da rede de gerência. Para que essa comunicação seja feita com segurança, as configurações do Apêndice E foram realizadas no ASA. Os *security levels*, que vão dos mais inseguros 0 até os mais seguros 100, foram utilizados no *firewall* da seguinte forma: 0 para a interface de comunicação externa, 100 para a interface de comunicação interna e 60 para a interface de gerencia. Esses níveis de segurança foram escolhidos porque a interface da rede interna pode ter acesso à rede externa e a de gerencia normalmente, porem o contrário não é verdadeiro, pois os *security levels* são menores. O mesmo acontece rede de gerencia, em que ela recebe informações tanto da rede interna tanto do ASA, porem não recebe informações da rede externa.

Caso fosse disponibilizado o acesso a servidores, como por exemplo, HTTP ou FTP, a rede de gerência também poderia ser uma área de DMZ (*DeMilitarized Zone*), considerada uma zona desmilitarizada, ou seja, uma região de interligação entre a rede interna e externa. Nesta área os servidores que serão disponibilizados para os usuários externos não estão em contato direto com a rede interna. Isto indica que, se um usuário externo conseguir invadir algum serviço disponibilizado nesta área, ele não conseguirá acessar os serviços da rede interna, por causa do *security level* menor que esta área possui (60). Um *security level* menor não consegue acessar uma área indicada com um *security level* maior (100).

Após todos os equipamentos configurados, foi utilizado novamente o Nmap instalado na máquina do invasor, ou seja, da rede externa, para fazer um *scanner* das possíveis vulnerabilidades. Com o *firewall*, o invasor não conseguiu visualizar o mapa dos *hosts* existentes na rede interna (Figura 51) e sim um único host que representa o ASA.

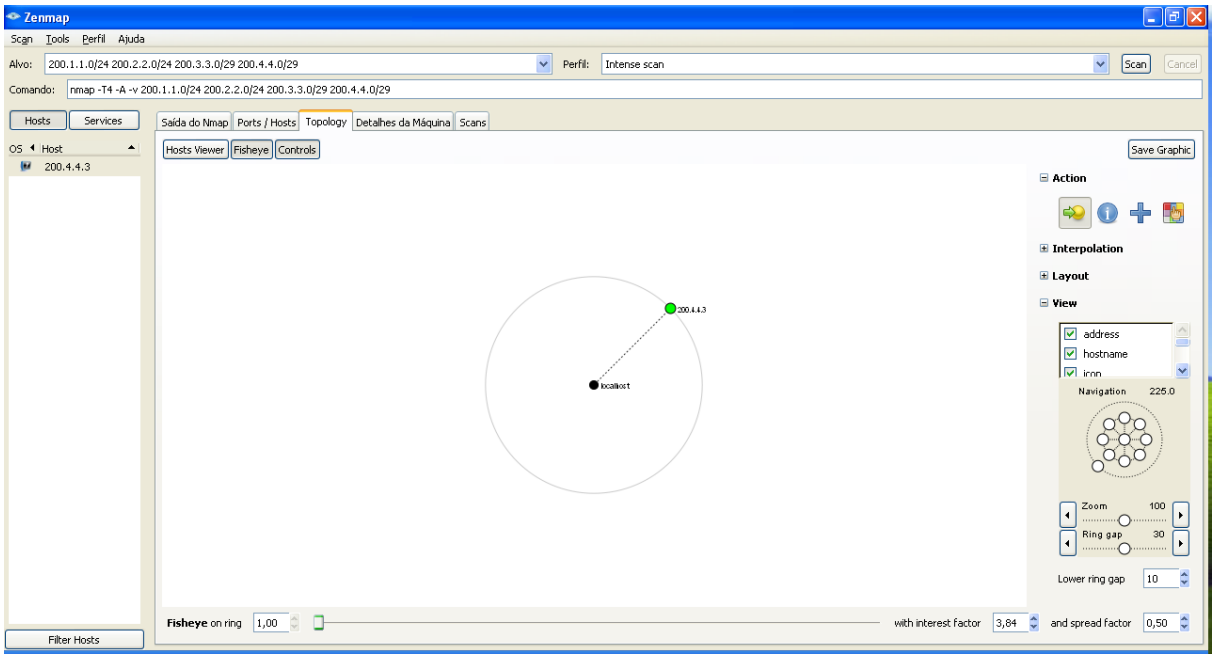


Figura 51 - Mapa de *hosts* (com segurança externa)

Fonte: autoria própria

O ASDM permite que o gerente da rede configure o ASA, mas também possibilita que o administrador veja, por exemplo, uma tentativa de invasão em tempo real. O primeiro gráfico da Figura 52 apresenta a grande quantidade de pacotes enviados pela interface de *outside* (rede externa) e o segundo gráfico mostra que nenhum pacote esta conseguindo sair pela interface *inside* (rede interna).

Figura 52 - Gráfico do ASDM

Fonte: autoria própria

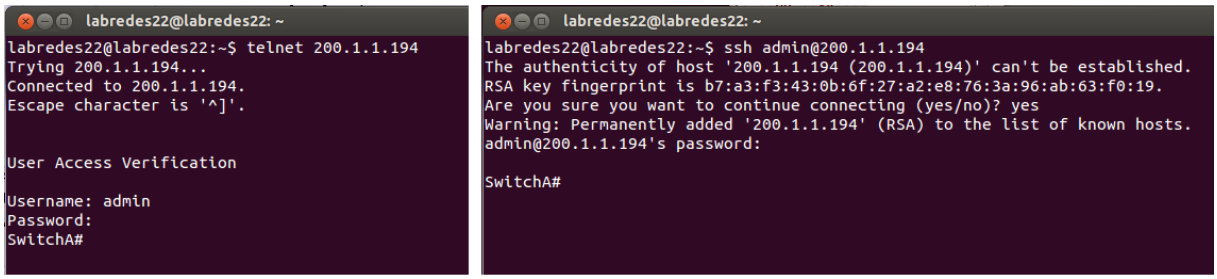
Como as máquinas internas não podem ser encontradas por um invasor externo, também não é possível acessar os serviços desmobilizados para os usuários internos, como por exemplo, FTP e SSH, fazendo com que a rede interna fique mais segura contra ataques externos.

3.2.3 Terceiro Cenário de Segurança

Os testes do terceiro cenário de segurança foram feitos com base na rede configurada no segundo cenário de segurança, porém com a criação de uma VLAN 30 de gerência, em que foi habilitado o acesso do switch por SSH e Telnet. As configurações estão apresentadas no Apêndice F.

A habilitação destes serviços pode acarretar em um ponto vulnerável de invasão, em que uma pessoa mal intencionada, de dentro da rede, tem acesso a todas as configurações do *switch*, tanto pelo Telnet (Figura 53 A), quanto pelo SSH (Figura 53 B). Porém o acesso via Telnet é mais inseguro que o SSH, por não ter seus dados criptografados antes de serem enviados à rede, como é apresentado na Figura 54 A, em que o Wireshark capturou os pacotes

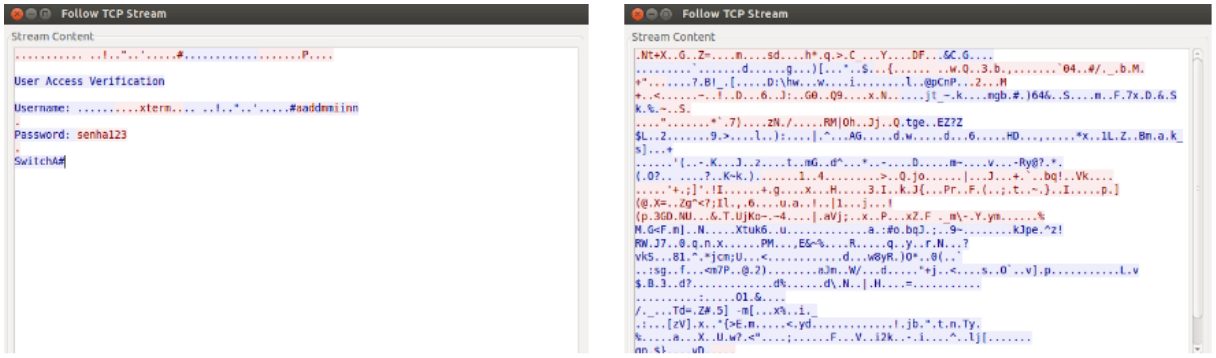
e indicou até mesmo a senha para acesso ao *switch*. Já o protocolo SSH, o Wireshark conseguiu somente capturar as informações criptografadas (Figura 54 B).



(A) (B)

Figura 53 - Acesso SSH e Telnet sem segurança

Fonte: autoria própria



(A) (B)

Figura 54 - Wireshark do Telnet e SSH sem segurança

Fonte: autoria própria

Há também a possibilidade ser colocado um equipamento DHCP invasor conectado em qualquer ponto da rede e quando uma máquina solicita IP automaticamente, ao invés do IP da rede ser enviado para o *host*, o DHCP envia um IP que não dará acesso a rede, fazendo com que a máquina não possa se conectar na rede. Com a Figura 55, do Wireshark é possível verificar os pacotes de DHCP capturados pela máquina.

```
188 59.5884550 0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0xf6558667
189 59.5919890 192.168.1.1      255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0xf6558667
190 59.5924850 0.0.0.0          255.255.255.255    DHCP    359 DHCP Request  - Transaction ID 0xf6558667
191 59.5972060 192.168.1.1      255.255.255.255    DHCP    349 DHCP ACK      - Transaction ID 0xf6558667
```

Figura 55 - Pacotes DHCP

Fonte: autoria própria

3.2.4 Quarto Cenário de Segurança

Como foi visto no cenário anterior, mesmo com a criação da VLAN 30 e utilização do protocolo SSH ao invés do Telnet, a rede ainda continua com falhas de segurança. Algumas políticas que podem ser utilizadas neste cenário para aumentar a segurança seriam a criação de listas de acessos (ACLs) bloqueando acessos à VLAN 30 e a implementação do *port security* em todas as portas dos *switches* camada 2. Para isso foram feitas as configurações do Apêndice G.

Com a configuração da lista de acesso um *host* de outra VLAN, como por exemplo a VLAN 20 (dados), não consegue acesso SSH a VLAN 30 de gerencia, conforme a Figura 56.

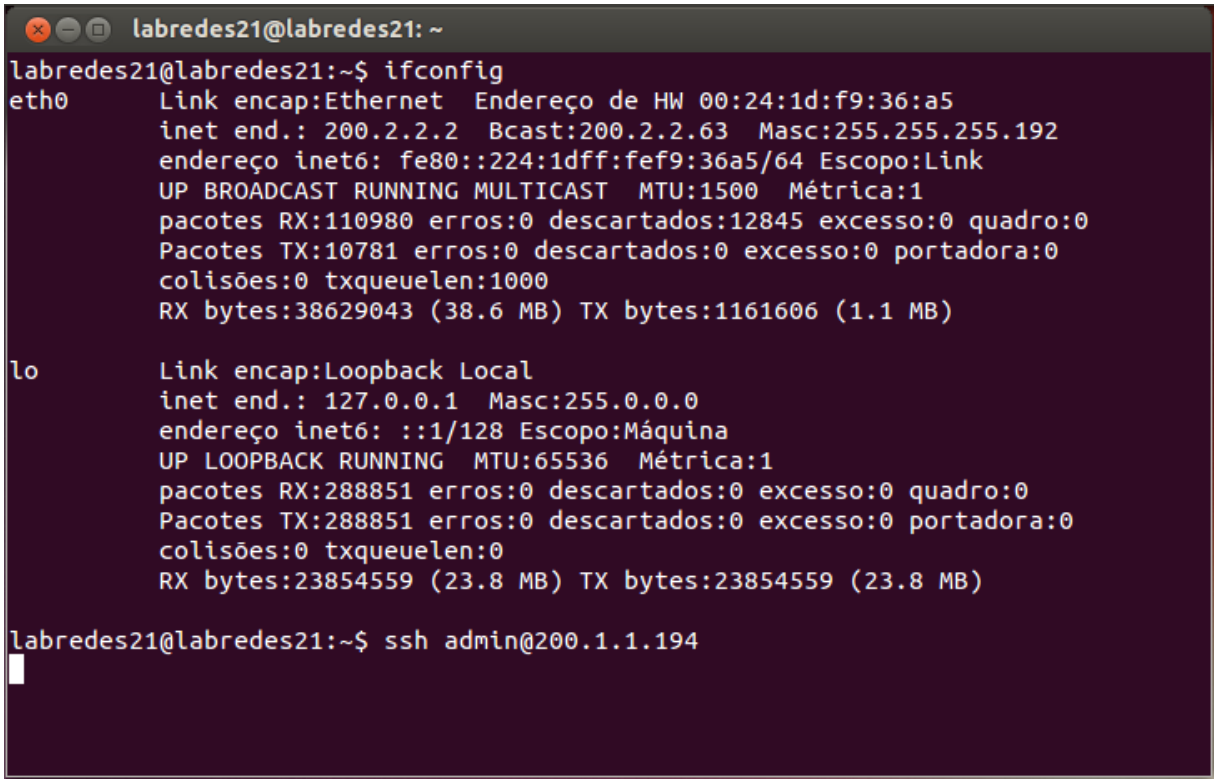


Figura 56 - SSH com lista de acesso

Fonte: autoria própria

Conforme a Figura 57, não foi possível conectar outra maquina com um *Mac address* diferente em uma porta em que foi implementado o *port security* e também o *switch* é informado de que houve uma violação na segurança e o *Mac address* que tentou se conectar

na rede (Figura 58). Assim não é possível colocar um servidor DHCP em uma porta que tenha configurado o *port security.*

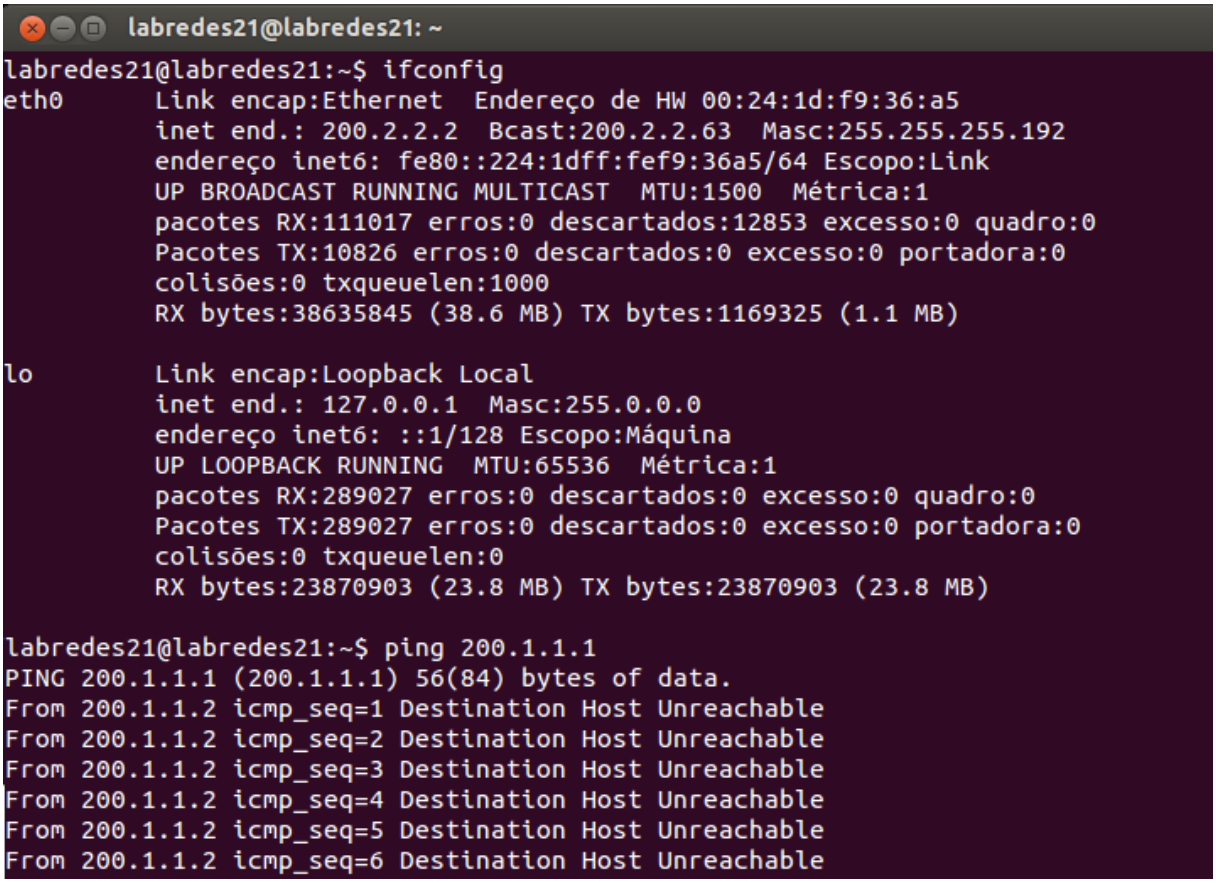


Figura 57 - Teste com *port security*

Fonte: autoria própria

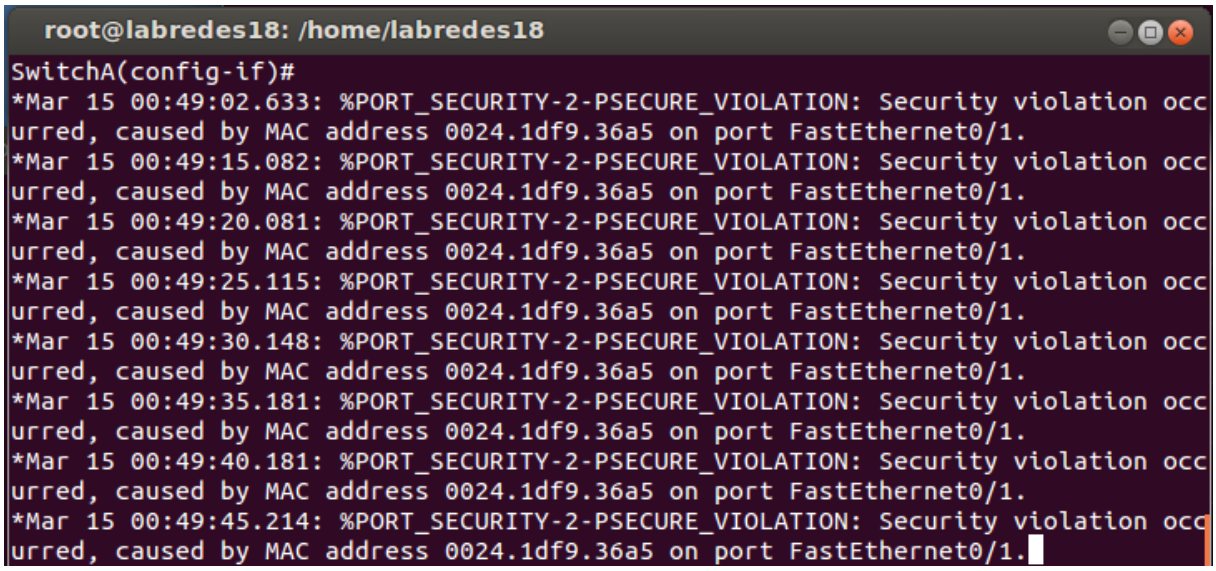


Figura 58 - *Port Security* no *Switch*

Fonte: autoria própria

3.3 TESTES DE GERENCIAMENTO

Para avaliar os ganhos de se ter empregado um *software* de gerenciamento, foi necessário somente um cenário de testes.

O cenário de gerenciamento foi feito com base na rede configurada no quarto cenário de segurança. O gerenciamento feito pelo *software* Cacti, que englobou somente os equipamentos da rede interna, ou seja, o Roteador interno, o *swicth* camada 3, o SwitchA e o SwitchB.

Para poder extrair dados do tráfego na rede, teve de ser executado, da mesma forma que o cenário 5 de QoS, os comandos do Jperf para gerar tráfego na rede:

- ✓ Servidor de Dados: iperf -s -P 10 -i 5 -p 4005 -f m
- ✓ Servidor de Voz: iperf -s -i 5 -p 5001 -f m
- ✓ Cliente de Dados: iperf -c 200.2.2.66 -P 10 -i 5 -p 4005 -f m -t 190
- ✓ Cliente de Voz: iperf -c 200.1.1.66 -i 5 -p 5001 -f m -t 190

Após o cadastro dos equipamentos e as configurações serem feitas no Cacti, foi possível obter alguns gráficos, tanto da quantidade de troca de mensagens SNMP de cada interface, como da temperatura e a quantidade de CPU utilizada de cada equipamento. Esses gráficos podem ser modificados para serem visualizados em varias escalas, por exemplo, em um dia inteiro, de 12 horas, de 4 horas ou de uma hora.

Os gráficos do roteador interno estão apresentados na Figura 59 e estão na escala de um dia. O gerente da rede pôde analisar quais horários do dia a porta ou o equipamento tem maior utilização ou se teve algum ponto de *stress*. A Figura 60 mostra os gráficos relacionados ao *switch* camada 3, que estão em uma escala de 4 horas, que permite analisar mais a fundo picos específicos caso eles tenham sido ocorridos uma única vez ou sejam contínuos no período. Já Figura 61, mostra os gráficos do SwitchA, que representa os *switches* camada 2, que estão em escala de 12 horas, que permite que o gerente analise quais horários, muitas vezes somente dentro do horário comercial, a porta ou o equipamento tem maior utilização e se não está sobrecarregada.

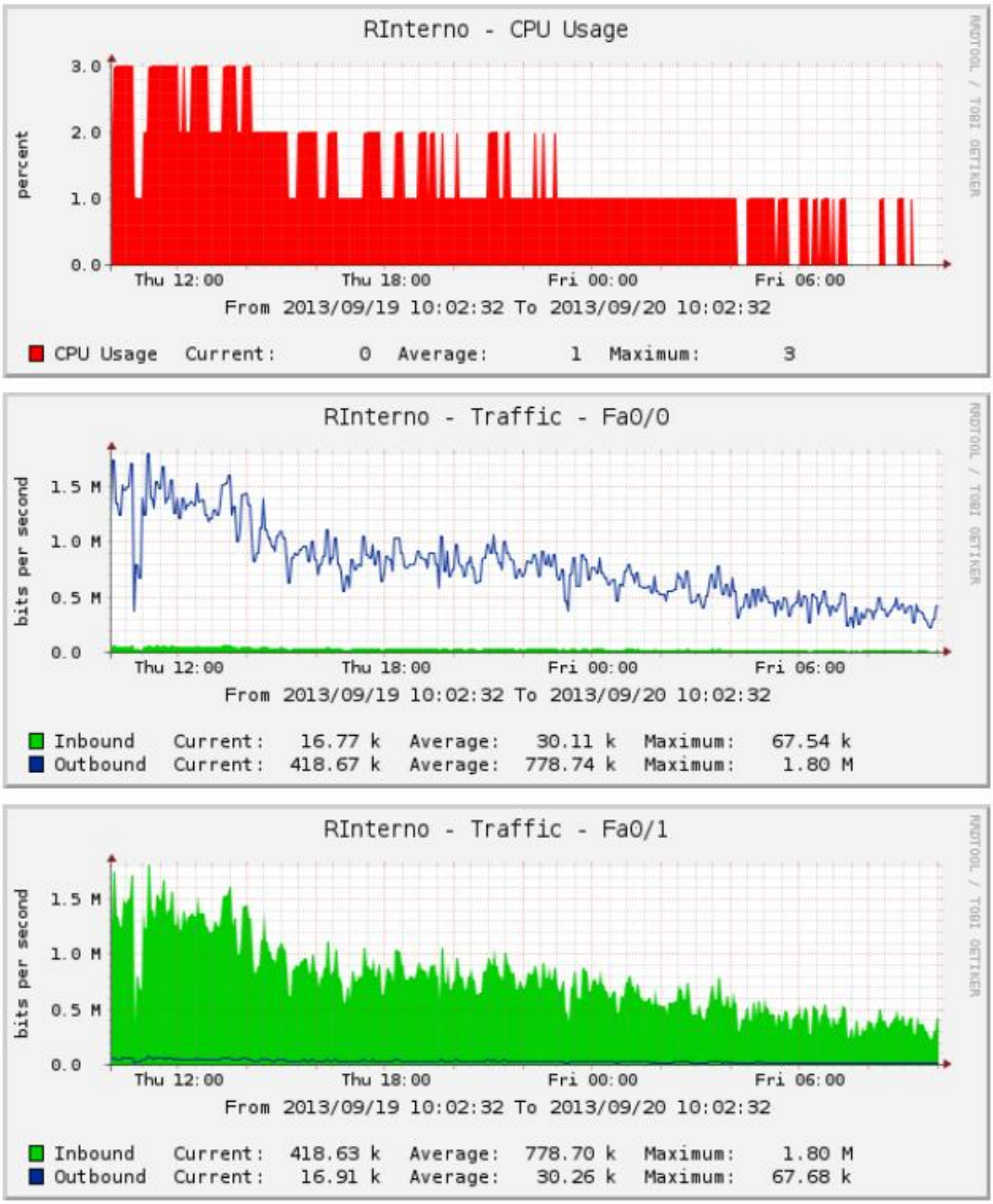


Figura 59 - Gráficos RInterno (24horas)

Fonte: autoria própria

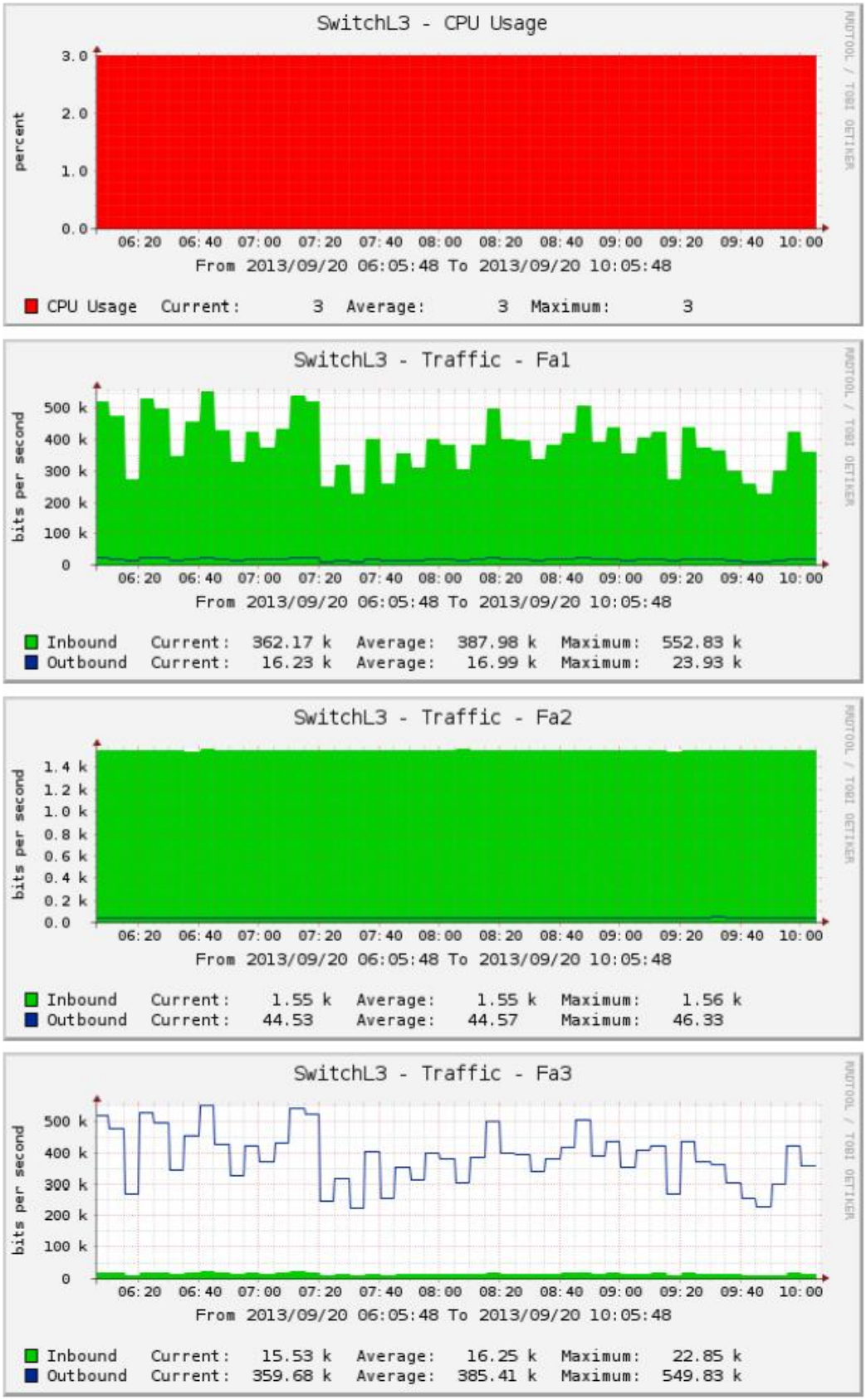


Figura 60 - Gráficos SwitchL3 (4horas)

Fonte: autoria própria

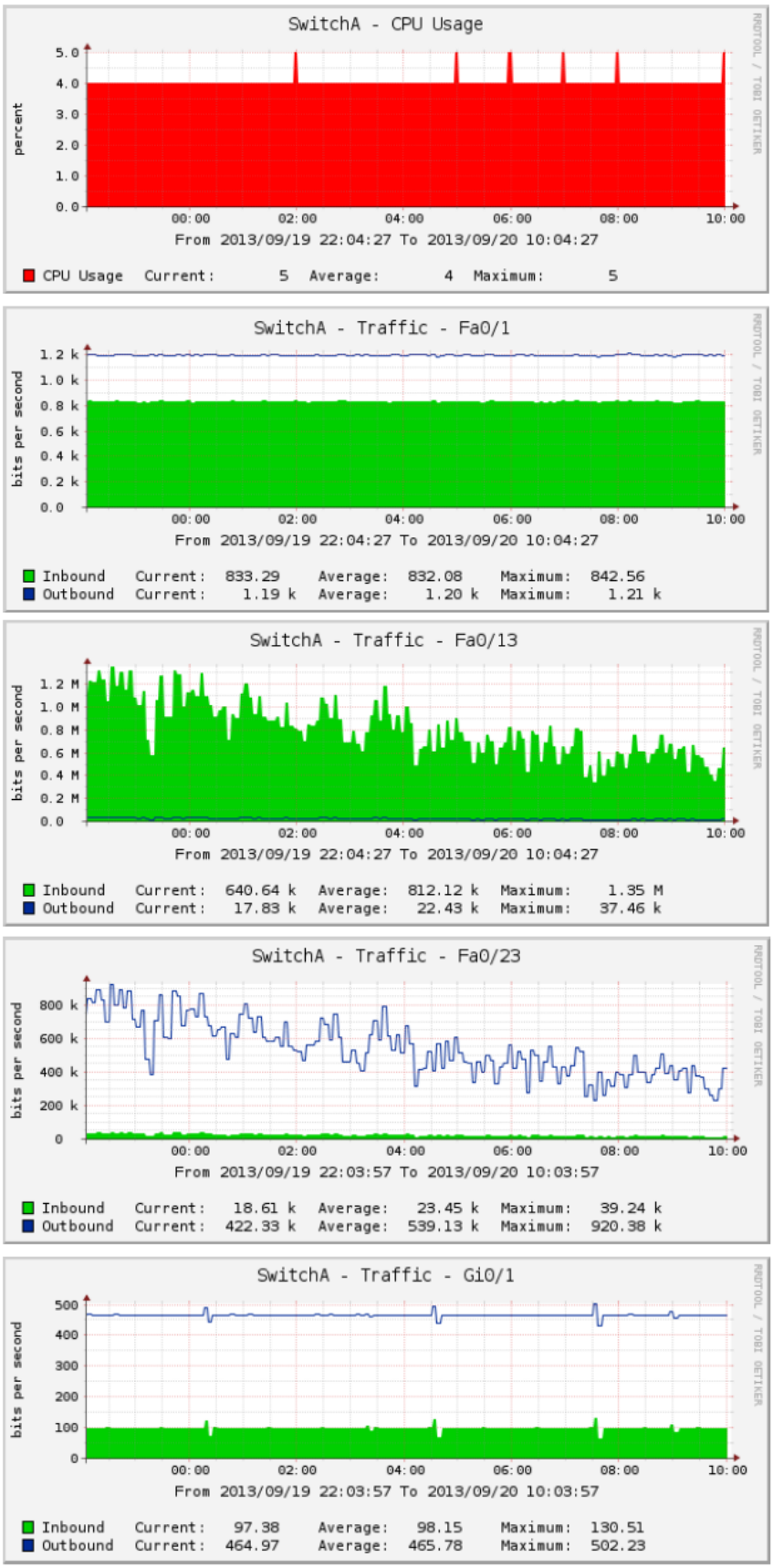


Figura 61 - Gráficos SwitchA (12horas)

Fonte: autoria própria

As Figura 59 (A), Figura 60 (A) e Figura 61 (A) mostram os gráficos de utilização da CPU dos equipamentos, determinando assim a temperatura que o equipamento se encontra. Caso o gráfico mostre que o equipamento está perto da sua capacidade máxima, o gerente de rede deve tomar alguma precaução para evitar que o equipamento tenha uma pane e pare de funcionar, afetando assim a rede como um todo. O mesmo pode acontecer com as interfaces, que estão representadas nos gráficos das Figura 59 (B e C), Figura 60 (B, C e D) e Figura 61 (B, C, D e E), caso o administrador de rede perceba que uma interface esta sendo utilizada de forma anormal, ele deve analisar se não esta ocorrendo algum erro na rede ou se alguma pessoa mal intencionada não esta sobrecarregando o trafego para afetar a rede com um possível ataque de negação de serviço (DoS).

4 CONCLUSÕES E TRABALHOS FUTUROS

Com a finalização dos estudos de casos pôde-se verificar a importância desses três pilares na infraestrutura de redes: qualidade de serviço (QoS), segurança e gerenciamento, trabalhados juntos em uma rede. Assim se a rede somente tiver o suporte a segurança, os testes feitos com QoS mostram que poderá ser inviável a implementação de um sistema que utilize VoIP, porque a rede não irá atender os requisitos básicos para o funcionamento desta tecnologia. Caso haja uma sobrecarga nos equipamentos de redes, tanto por um ataque de negação de serviços (DoS), se o administrador de redes não tiver o auxílio de um *software* de gerenciamento, ele só ira descobrir a falha quando o *hardware* parar de funcionar. Isto também ocorre caso a rede só tenha suporte à QoS, Além do equipamento poder ter problemas, é possível que alguns ataques possam ocorrer a esta rede, como mostram os cenários de segurança.

Com a conclusão do objetivo da pesquisa, que era implementar e fazer a análise de uma infraestrutura de redes que contemplasse segurança, qualidade de serviços e gerenciamento, foi possível colocar em prática conceitos, muitas vezes vistos somente de forma teórica, sem a utilização de equipamentos reais de redes. No desenvolvimento do trabalho, foi possível obter um conhecimento abrangente na área de redes de computadores e telecomunicações.

A conclusão da pesquisa possibilita trabalhos futuros, em que pode-se estudar separadamente e de forma aprofundada cada uma das áreas abordadas, segurança, QoS e gerenciamento. Como *Firewall* ASA foi utilizado com as configurações básicas, pode-se também fazer um estudo mais aprofundado sobre os conceitos de segurança em firewall, as listas de controle de acesso (ACLs) e o controle das conexões feito por este equipamento. A implementação de utilização do *software* de gerenciamento Cacti também pode ser assunto para trabalhos futuros, fazendo uma abordagem mais específica das características do gerenciamento de redes.

REFERÊNCIAS

BERTHOLDO L. M. **Implementando Segurança e Controle em Redes de Computadores.** 1997. Lume Repositório Digital Universidade Federal do Rio Grande do Sul. Disponível em: < http://www.lume.ufrgs.br/handle/10183/9009> Acessado em: 03/05/2012.

BIRKNER, M. H. **Projeto de Interconexão de Redes – Cisco Internetwork Design – CID**. São Paulo: Pearson Education do Brasil, 2003.

BLACK, T. L. **Comparação de Ferramentas de Gerenciamento de Redes.** 2008. Lume Repositório Digital Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf?sequence=1> Acessado em: 03/05/2012.

BRUNA.; VOGT E. M. G.; MENDES A. S. **QoS - Qualidade de Serviço em TCP/IP.** 2002. Disponível em: <http://www.micropic.com.br/paginadecliente/noronha/Informatica/REDES/qos%20-%20qualidade%20de%20servi%C3%A7o%20em%20tcp-ip.pdf> Acessado em: 03/05/2012.

Cacti®: The Complete RRDTool-based Graphing Solution. Disponível em: <www.cacti.net/> Acessado em: 26/09/2013.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br/> Acessado em: 09/07/2013.

Cisco Systems, Inc. Disponível em: < http://www.cisco.com/en/US/products/ > Acessado em: 07/05/2012.

COLCHER, S.; GOMES, A. T. A.; SILVA, A. O.; FILHO, G. L. S.; SOARES, L. F. G. **VoIP: Voz sobre IP.** 4ª Reimpressão. Rio de Janeiro: Elsevier, 2005.

COMER, D. E. **Interligação de Redes com TCP/IP: volume 1 princípios, protocolos e arquitetura.** 5ª Ed. Rio de Janeiro: Elsevier, 2006.

COMER, D. E. **Redes de Computadores e Internet.** 4ª Ed. Porto Alegre: Bookman, 2007.

CORREIA, M. F. **Gerência de Redes.** União Educacional de Minas Gerais, 2004. Disponível em: <http://www.si.lopesgazzani.com.br/TFC/monografias/MONOGRAFIA%2013011062.pdf> Acessado em: 06/05/2012.

CRONKHITE, C.; MCCULLOUGH, J. **Hackers, acesso negado.** Rio de Janeiro: Campus, 2001.

FARROW, R. **VLANs: virtually insecure?** Network Magazine Mar 2003, Vol. 18 Issue 3, p 62.

FEIT, S.M. **SNMP: a guide to network management.** New York: McGraw-Hill,Inc, 1995.

FILIPPETTI, M. A. **CCNA 4.1 – Guia Completo de Estudo.** Florianópolis: Visual Books, 2008.

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 3ª Ed. Porto Alegre: Bookman, 2006.

FROOM, R. **Implementing Cisco Switched Networks (SWITCH): Foundation Learning Guide.** Indianapolis: Cisco Press, 2010.

GNS3: Graphical Network Simulator. Disponível em: <http://www.gns3.net/> Acessado em: 26/09/2013.

GONZAGA, F. B.; SALLES, R. M. **Proportional Differentiated Services based on a Single Composite Metric.** 2007. LaReS Laboratório de Redes de Computadores e Sistemas Distribuídos. Disponível em: <http://www.bcc.unifal-mg.edu.br/lares/files/artigos/> Acessado em: 07/05/2012.

GUIMARÃES, M. V. A. F. **Gerenciamento e Monitoração de Redes TCP/IP.** Universidade Federal Ouro Preto, 1997. Disponível em: <http://www.oocities.org/siliconvalley/vista/5635/cap4.html> Acessado em: 10/06/2013.

HARFF, S. **Requisitos e Proposta para Implantação de um Servidor VoIP.** 2008. Lume Repositório Digital Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15984/000695302.pdf?sequence=1> Acessado em: 25/06/2013.

HEIN, M.; GRIFFITHS, D. **SNMP Versions 1 & 2 Simple Network Management Protocol Theory and Practice.** London: International Thomson Computer Press, 1995.

Iperf: The TCP/UDP Bandwidth Measurement Tool. Disponível em: <http://iperf.fr/> Acessado em: 25/09/2013.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: uma nova abordagem.** São Paulo: Addison Wesley, 2003.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: uma abordagem top-down.** 3ª Ed. São Paulo: Pearson Addison Wesley, 2006.

MORIMOTO, C. E. **Redes: guia prático.** Porto Alegre: Sul Editores, 2008.

MOURA, J. M. **Gerência de Sistemas Baseada em Redes Ativas.** ACSO – Núcleo de Arquitetura de Computadores e Sistemas Operacionais, 2003. Disponível em: <http://www.acso.uneb.br/marcosimoes/TrabalhosOrientados/MOURA2003.pdf> Acessado em: 06/05/2012.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec Editora, 2007.

Nmap: Free Security Scanner For Network Exploration & Hacking. Disponível em: <http://nmap.org/> Acessado em: 26/09/2013.

ODOM, W. **Cisco CCNA: guia de certificação do exame**. 3ª Ed. Rio de Janeiro: Alta Books, 2003.

SCHWEITZE, C. M. et al. **Tecnologias de redes sem fio: Wpans, wlans e wmans – desafios de segurança, vulnerabilidades e soluções.** 7º Simpósio de Segurança em Informática, 2005. Disponível em: <http://www.linorg.cirp.usp.br/SSI/SSI2005/Microcursos/MC04.pdf> Acessado em: 09/07/2013.

SCRIMGER, R.; LASALLE, P.; PARIHAR, M.; GUPTA, M. **TCP/IP a Bíblia.** 6ª Reimpressão. Rio de Janeiro: Elsevier, 2002.

SEACORD, R. C.; HOUSEHOLDER A. D**. A structured approach to classifying security Vulnerabilities**. Tech. Rep. CMU/SEI-2005-TN-003, CMU/SEI, Jan 2005. Disponível em: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1479&context=sei> Acessado em: 09/07/2013.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S**. Redes de Computadores das LANs, MANs e WANs às Redes ATM.** 2ª Ed. Rio de Janeiro: Campus, 1995.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas.** 2ª Ed. Rio de Janeiro: Elsevier, 2005.

SYSTEMS INC, Cisco. **Quality of Service Design Overview.** Disponível em: <http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html>. Acessado em: 24/09/2013.

TANENBAUM, A. S. **Redes de Computadores**. 4ª Ed. Rio de Janeiro: Elsevier, 2003.

TSAUR, W.; HORNG, S. **Establishing Secure Ethernet LANs Using Intelligent Switching Hubs in Internet Environments.** The Computer Journal,1998;41:125 - 133.

VEGESNA, S. **IP Quality of Service.** Indianapolis: Cisco Press, 2001.

WANG, Z. **Internet QoS: architectures and mechanisms for quality of service.** San Francisco: Morgan Kaufmann Pubblishers, 2001.

WATKINS, M.; WALLACE, K. **CCNA Security Official Exam Certification Guide.** Indianapolis: Cisco Press, 2008.

Wireshark: Go Deep. Disponível em: <http://www.wireshark.org/> Acessado em: 25/09/2013.

APÊNDICES

Apêndice A

SwitchA:

```
SwitchA#configure terminal
SwitchA(config)#vtp mode server
SwitchA(config)#vlan 10
SwitchA(config-vlan)#name voz
SwitchA(config-vlan)#vlan 20
SwitchA(config-vlan)#name dados
SwitchA(config-vlan)#exit
SwitchA(config)#interface range fastEthernet0/1-12
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range fastEthernet0/13-22
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 20
SwitchA(config-if-range)#exit
SwitchA(config)#interface fastEthernet 0/23
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk all vlan 10, 20
SwitchA(config-if)#end
SwitchA#wr
```

SwitchB:

```
SwitchB#configure terminal
SwitchB(config)#vtp mode server
SwitchB(config)#vlan 10
SwitchB(config-vlan)#name voz
SwitchB(config-vlan)#vlan 20
SwitchB(config-vlan)#name dados
SwitchB(config-vlan)#exit
SwitchB(config)#interface range fastEthernet0/1-12
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 10
SwitchB(config-if-range)#exit
SwitchB(config)#interface range fastEthernet0/13-22
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 20
SwitchB(config-if-range)#exit
SwitchB(config)#interface fastEthernet 0/23
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk all vlan 10, 20
SwitchB(config-if)#end
SwitchB#wr
```

Apêndice B

Switch camada 3:

```
Switch2948G #configure terminal
Switch2948G(config)#interface fastEthernet 1
Switch2948G(config-if)#no shutdown
Switch2948G(config-if)#exit
Switch2948G(config)#interface fastEthernet 1.10
Switch2948G(config-subif)#encapsulation dot1Q 10
Switch2948G(config-subif)#ip address 200.1.1.1 255.255.255.192
Switch2948G(config-subif)#exit
Switch2948G(config)#interface fastEthernet 1.20
Switch2948G(config-subif)#encapsulation dot1Q 20
Switch2948G(config-subif)#ip address 200.2.2.1 255.255.255.192
Switch2948G(config-subif)#exit
Switch2948G(config)#interface fastEthernet 2
Switch2948G(config-if)#no shutdown
Switch2948G(config-if)#exit
Switch2948G(config)#interface fastEthernet 2.10
Switch2948G(config-subif)#encapsulation dot1Q 10
Switch2948G(config-subif)#ip address 200.1.1.65 255.255.255.192
Switch2948G(config-subif)#exit
Switch2948G(config)#interface fastEthernet 2.20
Switch2948G(config-subif)#encapsulation dot1Q 20
Switch2948G(config-subif)#ip address 200.2.2.65 255.255.255.192
Switch2948G(config-subif)#exit
Switch2948G(config)# exit
Switch2948G#wr
```

Apêndice C

SwitchA:

```
SwitchA#configure terminal
SwitchA(config)#mls qos
SwitchA(config)#interface range fastEthernet 0/1-12
SwitchA(config-if-range)#mls qos
SwitchA(config-if-range)#mls qos cos 5
SwitchA(config-if-range)#mls qos trust cos
SwitchA(config-if-range)#exit
SwitchA(config)#interface range fastEthernet 0/13-22
SwitchA(config-if-range)#mls qos
SwitchA(config-if-range)#mls qos cos 0
SwitchA(config-if-range)#mls qos trust cos
SwitchA(config-if-range)#exit
SwitchA(config)#interface fastEthernet 0/23
SwitchA(config-if)#mls qos
SwitchA(config-if)#mls qos trust cos
SwitchA(config)#end
SwitchA#wr
```

SwitchB:

```
SwitchB#configure terminal
SwitchB(config)#mls qos
SwitchB(config)#interface range fastEthernet 0/1-12
SwitchB(config-if-range)#mls qos
SwitchB(config-if-range)#mls qos cos 5
SwitchB(config-if-range)#mls qos trust cos
SwitchB(config-if-range)#exit
SwitchB(config)#interface range fastEthernet 0/13-22
SwitchB(config-if-range)#mls qos
SwitchB(config-if-range)#mls qos cos 0
SwitchB(config-if-range)#mls qos trust cos
SwitchB(config-if-range)#exit
SwitchB(config)#interface fastEthernet 0/23
SwitchB(config-if)#mls qos
SwitchB(config-if)#mls qos trust cos
SwitchB(config)#end
SwitchB#wr
```

Apêndice D

RInterno:

```
RInterno#configure terminal
RInterno(config)#interface fastEthernet0/0
RInterno(config-if)# ip address 200.4.4.1 255.255.255.248
RInterno(config-if)#no shutdown
RInterno(config-if)#exit
RInterno(config)#interface range fastEthernet0/1
RInterno(config-if)# ip address 200.4.4.1 255.255.255.248
RInterno(config-if)#no shutdown
RInterno(config-if)#exit
RInterno(config)#ip route 0.0.0.0 0.0.0.0 200.4.4.2
RInterno(config)#ip route 200.1.1.0 255.255.255.0 200.3.3.2
RInterno(config)#ip route 200.2.2.0 255.255.255.0 200.3.3.2
RInterno(config)#ip route 201.150.1.0 255.255.255.0 200.4.4.2
RInterno(config)#end
RInterno#wr
```

RBorda:

```
RBorda#configure terminal
RBorda(config)#interface fastEthernet0/0
RBorda(config-if)# ip address 200.4.4.2 255.255.255.248
RBorda(config-if)#no shutdown
RBorda(config-if)#exit
RBorda(config)#interface range fastEthernet0/1
RBorda(config-if)# ip address 201.150.1.1 255.255.255.0
RBorda(config-if)#no shutdown
RBorda(config-if)#exit
RBorda(config)#ip route 0.0.0.0 0.0.0.0 201.150.1.2
RBorda(config)#ip route 200.1.1.0 255.255.255.0 200.4.4.1
RBorda(config)#ip route 200.2.2.0 255.255.255.0 200.4.4.1
RBorda(config)#ip route 200.3.3.0 255.255.255.0 200.4.4.1
RBorda(config)#end
RBorda#wr
```

Switch camada 3:

```
Switch2948G# configure terminal
Switch2948G(config)#interface fastEthernet 3
Switch2948G(config-if)#ip address 200.3.3.2 255.255.255.252
Switch2948G(config-if)# no shutdown
Switch2948G(config-if)#exit
Switch2948G(config)#interface fastEthernet 3
Switch2948G(config)#ip route 0.0.0.0 0.0.0.0 200.3.3.1
Switch2948G(config)#end
Switch2948G#wr
```

Apêndice E

ASA:

```
ASA# configure terminal
ASA(config)# interface ethernet 0/0
ASA(config-if)# security-level 0
ASA(config-if)# nameif outside
ASA(config-if)# ip address 201.150.1.1 255.255.255.0
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# interface ethernet 0/1
ASA(config-if)# security-level 100
ASA(config-if)# nameif inside
ASA(config-if)# ip address 200.4.4.2 255.255.255.248
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# interface ethernet 0/2
ASA(config-if)# security-level 60
ASA(config-if)# nameif gerencia
ASA(config-if)# ip address 192.168.1.1 255.255.255.0
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# username admin password senha123 privilege 15
ASA(config)# http 192.168.1.2 255.255.255.255 gerencia
ASA(config)# route inside 200.1.1.0 255.255.255.0 200.4.4.1
ASA(config)# route inside 200.2.2.0 255.255.255.0 200.4.4.1
ASA(config)# route inside 200.3.3.0 255.255.255.0 200.4.4.1
ASA(config)# route outside 0.0.0.0 0.0.0.0 201.150.1.2
ASA(config)# end
ASA# wr
```

Apêndice F

Criação Vlan 30 (SwitchA e SwitchB):

```
Switch#configure terminal
Switch(config)#vtp mode server
Switch(config)#vlan 30
Switch(config-vlan)#name gerencia
Switch(config-vlan)#exit
Switch(config)#interface range gigabitEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk all vlan all
Switch(config-if)#end
Switch#wr
```

Criação Vlan 30 (Switch camada 3):

```
Switch2948G(config)#interface fastEthernet 1.30
Switch2948G(config-subif)#encapsulation dot1Q 30
Switch2948G(config-subif)#ip address 200.1.1.193 255.255.255.192
Switch2948G(config-subif)#exit
Switch2948G(config)#interface fastEthernet 2.30
Switch2948G(config-subif)#encapsulation dot1Q 30
Switch2948G(config-subif)#ip address 200.2.2.193 255.255.255.192
Switch2948G(config-subif)#exit
```

Telnet (SwitchA e SwitchB):

```
Switch#configure terminal
Switch(config)#username admin privilege 15 password senha123
Switch(config)#line vty 0 4
Switch(config-line)#login local
Switch(config-line)#end
Switch#wr
```

SSH (SwitchA e SwitchB):

```
Switch#configure terminal
Switch(config)#ip domain-name labredes.dainf.ct.utfpr.edu.br
Switch(config)#crypto key generate rsa
Switch(config)#ip ssh time-out 60
Switch(config)#line vty 0 4
Switch(config-line)#transport input ssh
Switch(config-line)#login local
Switch(config-line)#end
Switch#wr
```

Apêndice G

ACLS (SwitchA e SwitchB):

```
Switch#configure terminal
Switch(config)#access-list 100 deny ip 200.1.1.0 0.0.0.63 200.1.1.192 0.0.0.63
Switch(config)#access-list 100 deny ip 200.2.2.0 0.0.0.63 200.1.1.192 0.0.0.63
Switch(config)# access-list 100 deny ip 200.1.1.0 0.0.0.63 200.2.2.192 0.0.0.63
Switch(config)# access-list 100 deny ip 200.2.2.0 0.0.0.63 200.2.2.192 0.0.0.63
Switch(config)#access-list 100 permit ip any any
Switch(config)#interface range fastEthernet 0/1-22
Switch(config-if-range)#ip access-group 100 in
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/1-22
Switch(config-if-range)#ip access-group 100 in
Switch(config-if-range)#end
Switch#wr
```

SwitchA:

```
SwitchA#configure terminal
SwitchA(config)#interface fastEthernet 0/1
SwitchA(config-if)#switchport port-security
SwitchA(config-if)#switchport port-security mac-address 00:1F:D0:E4:E8:82
SwitchA(config-if)#switchport port-security maximum 1
SwitchA(config-if)#switchport port-security violation restrict
SwitchA(config-if)#exit
SwitchA(config)#interface fastEthernet 0/13
SwitchA(config-if)#switchport port-security
SwitchA(config-if)#switchport port-security mac-address 00:24:1D:F9:36:A5
SwitchA(config-if)#switchport port-security maximum 1
SwitchA(config-if)#switchport port-security violation restrict
SwitchA(config-if)#end
SwitchA#wr
```

SwitchB:

```
SwitchB#configure terminal
SwitchB(config)#interface fastEthernet 0/1
SwitchB(config-if)#switchport port-security
SwitchB(config-if)#switchport port-security mac-address 00:F9:D4:E0:E2:81
SwitchB(config-if)#switchport port-security maximum 1
SwitchB(config-if)#switchport port-security violation restrict
SwitchB(config-if)#exit
SwitchB(config)#interface fastEthernet 0/13
SwitchB(config-if)#switchport port-security
SwitchB(config-if)#switchport port-security mac-address 00:D5:B3:26:A1:E1
SwitchB(config-if)#switchport port-security maximum 1
SwitchB(config-if)#switchport port-security violation restrict
SwitchB(config-if)#end
SwitchB#wr
```