CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
ULBRA
COMUNIDADE EVANGÉLICA LUTERANA "SÃO PAULO"
Recredenciado pela Portaria Ministerial nº 3.607 - D.O.U. nº 202 de 20/10/2005

Neuziron Aguiar dos Santos

MELHORIAS EM LANS ATRAVÉS DE GERÊNCIA DE REDES E QoS: proposta de melhoria para estrutura atual do CEULP/ULBRA

Palmas - TO

2013

Neuziron Aguiar dos Santos

MELHORIAS EM LANS ATRAVÉS DE GERÊNCIA DE REDES E QoS: proposta de melhoria para estrutura atual do CEULP/ULBRA

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.Sc. Madianita Bogo Marioti.

Palmas - TO

2013

Neuziron Aguiar dos Santos

MELHORIAS EM LANS ATRAVÉS DE GERÊNCIA DE REDES E QoS: proposta de melhoria para estrutura atual do CEULP/ULBRA

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.Sc. Madianita Bogo Marioti.

Aprovada em: Junho de 2013.

BANCA EXAMINADORA

_____

Prof. M.Sc. Madianita Bogo Marioti

Centro Universitário Luterano de Palmas

_____

Prof. M.Sc. Fernando Luiz de Oliveira

Centro Universitário Luterano de Palmas

_____

Prof. M.Sc. Edeilson Milhomem da Silva

Centro Universitário Luterano de Palmas

Palmas - TO

2013

DEDICATÓRIA

Dedico este trabalho à minha Mãe, ao meu Pai e aos meus irmãos por todo o apoio, carinho, confiança e compreensão.

AGRADECIMENTOS

Agradeço a Deus por me conceder forças para superar os obstáculos e alcançar com êxito essa graduação.

À minha Mãe, pelo incentivo e apoio nos momentos de angústia durante as madrugadas, por ter me dado suporte e por me amparar ao longo dessa longa caminhada. Obrigado, minha velhinha, por tudo o que fez por mim, por nossa família e pelo nosso lar.

Ao meu Pai, que sempre me ensinou bons valores e a lutar por aquilo que acreditamos. Obrigado por me ensinar que o trabalho dignifica o homem e que grandes conquistas são alcançadas depois de atravessar longos caminhos.

Agradeço a minha orientadora Madianita Bogo Marioti, que me apoiou, cobrou e incentivou desde a disciplina de estágio.
Também sou grato aos professores Fernando Luiz de Oliveira, Fabiano Fagundes, Jackson Gomes de Souza, Parcilene Fernandes de Brito, Michael Schuenck dos Santos e Edeilson Milhomem da Silva pela dedicação, incentivo e por me prepararem para o mercado de trabalho e por contribuírem para o meu enriquecimento pessoal e profissional.

Aos meus amigos Paulo Henrique de Sousa e Rafael Gonçalves Barreira que iniciaram e concluíram comigo essa jornada. Valeu, nobres guerreiros de corujões e trabalhos, fico muito feliz em chegar ao final do curso e confraternizar essa vitória com vocês.

À Monik Helen Gomes pela amizade, carinho, paciência e por fazer parte dessa conquista.

Às minhas amigas comunicativas e sempre sorridentes Eva Bandeira e Patrícia Oliveira Vera que juntas auxiliaram na revisão de alguns trechos deste trabalho.

Aos amigos do trabalho Ernandes Rodrigues da Silva, José Neto Luz Carneiro e Urias Cruz da Cunha pelos ensinamentos, apoio, disposição, amparo e compreensão desde o período do estágio.

Enfim, é isso. Obrigado a todos que contribuíram direta ou indiretamente para essa conquista!

RESUMO

Os avanços tecnológicos, juntamente com a disponibilização da internet 2.0 proporcionaram uma maior interação entre usuários e as aplicações, e, consequentemente o uso massificado da internet passou a demandar a maior parte dos recursos de rede, prejudicando a produtividade nas organizações. Para assegurar que os serviços essenciais funcionem de maneira eficaz, ações gerenciais devem ser tomadas: uma opção, nem sempre eficiente, pode ser a disponibilização de links com maior largura de banda; Outra forma, menos onerosa financeiramente, poderá ser alcançada com a implantação de técnicas de priorização de tráfego e de gerência de redes, com enfoque no monitoramento do consumo dos insumos de internet. O objetivo deste trabalho é mostrar o processo de comunicação das ferramentas de gerência que atuam como facilitadoras no cotidiano dos administradores de redes. Além disso, em um cenário proposto, foi aplicado método de priorização de tráfego e a utilização de ferramentas de gerência na rede do CEULP/ULBRA. Neste sentido, serão apresentados os conceitos envolvidos e os testes realizados dentro do ambiente simulado da instituição.

PALAVRAS-CHAVE: gerência de redes, ferramentas de gerência, QoS(*Quality of service*).

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

QoS	(*Quality of Services*)
SNMP	(*Simple Network Management Protocol*)
MIB	(*Management information base*)
TCP	(*Transmission Control Protocol*)
UDP	(*User Datagram Protocol*)
LAN	(*Local Area Network*)
WAN	(Wide Area Network)
SLAs	(*Services Level Agreements*)
ISO	(*International Organization Standardization*)
SO	(Sistemas Operacionais)
IETF	(*Internet Engineering Task Force)*
ICMP	(*Internet Control Message Protocol)*

SUMÁRIO

1 INTRODUÇÃO

A evolução dos recursos de *hardware* e, consequentemente, o aumento da utilização das Tecnologias de informações e comunicação (TICs) dentro das corporações, tem aumentado o tráfego nas redes das empresas. Esse aumento do tráfego não pode afetar a qualidade dos serviços disponibilizados, para isso, precisam de uma rede estável e funcional.

Gerenciar as redes sem a ajuda de ferramentas de gerência fica mais difícil e as redes das organizações se tornam cada vez mais vulneráveis a lentidão e quedas provocadas por tráfego não produtivo. Atualmente, existem diversas ferramentas que realizam o gerenciamento de redes. Essas ferramentas são projetadas e desenvolvidas a partir de protocolos de comunicação e gerência desenvolvidos para esse fim.

A expansão da internet 2.0, que proporciona maior interação entre usuários e aplicações, geram grande volume de tráfego nas redes das corporações. Realizar o bloqueio dessas páginas nem sempre é possível, um exemplo disso são instituições de ensino, onde não pode haver bloqueio de acesso ao conhecimento. Páginas como Vimeo e Youtube, que possuem canais de conhecimento, devem ser liberadas para pesquisa, o que gera uma grande demanda no link das instituições.

Para assegurar que os serviços essenciais funcionem de maneira eficaz é necessário adquirir links com maior largura de banda. Uma forma de minimizar esse problema é a implantação de ferramentas de QoS, com a qual os administradores da rede poderão analisar informações do tráfego da rede e dar prioridade aos serviços que são mais relevantes para a corporação.

O CEULP/ULBRA é uma instituição de ensino com estrutura de rede de porte médio, que possui uma alta demanda por informações disponibilizadas na Internet e uma grande quantidade de acessos à rede local, o que gera um tráfego excessivo. Essa rede se torna excessivamente lenta em determinados horários e datas. Nesse contexto, pensou-se em realizar um levantamento da estrutura da rede atual do CEULP/ULBRA para entender o tráfego existente, e realizar a e propor soluções que melhorem o desempenho da rede.

Nesse contexto, o objetivo deste trabalho é conhecer e simular em ambiente virtual a rede LAN do CEULP/ULBRA para propor melhorias usando ferramentas de gerência de redes e QoS.

2 REFERENCIAL TEÓRICO

Nessa seção serão apresentados os fundamentos teóricos que servirão de base para compreensão e execução deste trabalho. São apresentados mecanismos e conceitos de gerência de redes e QoS (*Quality of Services*) e ferramentas de gerencia de rede e QoS.

2.1. Gerência de redes

Uma rede consiste em um apanhado de *hardwares* e *softwares* que interagem entre si, sejam eles comutadores, roteadores, computadores e qualquer outro dispositivo que faça parte dos componentes físicos de uma rede. Esse aglomerado de equipamentos quando configurados e interligados formam uma rede que, com o passar do tempo ou por acidente, podem apresentar falhas que podem não ser facilmente detectadas pelo administrador da rede. Algumas dessas falhas de *hardware* podem ser percebidas quando o equipamento ainda está funcionando, por exemplo, um roteador que apresenta taxa alta de perda de pacotes pode ser substituído antes de paralisar totalmente a rede.

No contexto de gerência de redes de médio e grande porte, um administrador não consegue fazer a gestão de todos os computadores de uma empresa *in loco*, sendo importante o uso de ferramentas que auxiliem na gerência da rede de sua organização. Segundo Tanenbaum (2011, p. 386), essas ferramentas de gerência auxiliam o gerente na análise de erros e o alerta sobre falhas como:

- **Detecção de falha em uma placa de interface em um hospedeiro, comutador ou roteador –** Utilizando mecanismos de gerência eficaz, é possível que um equipamento de rede indique que uma de suas interfaces não está funcionando. Além disso, se o administrador realizar um monitoramento eficaz e contínuo da rede ainda é possível verificar a perda de pacotes de uma interface e substituí-la antes que o serviço fique indisponível aos usuários.

- **Monitoração de hospedeiro –** Constantemente o administrador da rede pode averiguar se os *hosts estão* ativos e operacionais, possibilitando correções antes mesmo de reclamações por parte dos usuários.

- **Monitoração do tráfego para auxiliar o oferecimento de recursos –** A partir do monitoramento da rede o administrador pode verificar padrões de tráfego entre origem e destino e realizar uma comutação de servidores em segmentos de LAN e fazer com que o fluxo de dados que passa por várias LAN's seja reduzido de maneira relevante. Realizando assim o melhoramento no desempenho sem aquisição de novos recursos de rede. O monitoramento do tráfego, também, pode mostrar que um segmento ou enlace de rede, seja ele LAN ou WAN, esteja sobrecarregado e que haja a real necessidade de aumentar sua capacidade.

- **Detecção de mudanças rápidas em tabelas de roteamento –** Mudanças frequentes em tabelas de roteamento e alternância de rotas podem revelar problemas físicos ou de configuração do roteador. Se essas mudanças forem detectadas a tempo, o problema pode ser solucionado antes que da rede ficar inoperante.

- **Monitoramento de SLAs –** Com o surgimento dos Acordos de níveis de serviços (SLAs) que são contratos e definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor de rede em relação a essas medidas, o interesse em monitorar o tráfego cresceu consideravelmente nos últimos anos (LARSEN, 1997, P.85). Entre os principais SLAs estão alta disponibilidade de serviços, latência, vazão e requisitos para notificação de ocorrência de serviços interrompidos. Os parâmetros citados acimas são verificados para assegurar e cobrar que as operadoras forneçam o serviço e velocidade estipuladas em contrato.

- **Detecção de intrusos –** É fundamental ter implementado em uma rede mecanismos que assegure a integridade da rede para evitar entrada de dados

de fonte suspeita ou mesmo quando é destinado dados á rede. A detecção de intrusos pode ser realizada através de monitoramento de *firewall* onde pode-se verificar ataques do tipo *port scan* ou *ip spoofing* , onde um ataque é realizado de um *host* externo que se passa por uma máquina da rede.

Assim, as falhas podem ser físicas, e ocorrer em equipamentos, ou lógicas, e ocorrer via programas e acessos à rede. Essas falhas podem ocorrer em diversos cenários provocando falhas e até mesmo a inoperância da rede. Como podem ser vários os tipos de problemas em uma rede, também, devem existir diversas formas de gerenciá-la. KUROSE (2007, p. 573) afirma que a *International Organization Standardization* (ISO) criou um modelo de gerenciamento de rede dividido em cinco áreas:

- **Gerenciamento de desempenho –** O gerenciamento do desempenho de uma rede consiste na monitoração das atividades da rede e no controle dos recursos através de ajustes e trocas, com o objetivo principal de quantificar, medir, informar, analisar e controlar o desempenho (por exemplo, utilização e vazão) de diferentes componentes da rede. Os dispositivos podem ser roteadores, enlaces, servidores, hosts etc. Para realizar a gerência de desempenho o administrador deve monitorar os recursos ou dispositivos que, em seu conhecimento, podem apresentar gargalos. Inicialmente o numero de dispositivos gerenciados a fim de se mensurar o desempenho pode ser um quantitativo pequeno, pois é melhor e mais fácil abstrair e realizar a leitura de níveis de desempenho da rede. As informações abstraídas pelo gerenciamento de desempenho podem auxiliar o administrador de rede proceder no planejamento, manutenção e manutenção da rede que gerencia Em sua obra SPECIALSKI (2002, online), afirma que as informações abstraídas podem ser utilizadas para reconhecer pontos onde há a ocorrência de gargalos, de modo á evitar que cause problemas para os usuários da rede. Através da analise de desempenho é possível realizar a troca de tabela de roteamento para melhorar o desempenho e até mesmo á longo prazo mostrar a necessidade de expansão dos circuitos que provém o acesso á internet.

- **Gerenciamento de falhas –** O principal objetivo de se gerenciar as falhas é registrar, detectar e reagir às condições de falhas na rede. Não existe uma

separação bem definida entre a gerência de desempenho e gerência de falhas (KUROSE, ROSS, 2007, P. 574). Pode-se considerar como gerenciamento de falhas a detecção e correção de falhas em dispositivos na rede como roteadores, hosts, enlaces e hospedeiros ou em *hardware* e *software* de roteadores. Por outro lado, o gerenciamento de desempenho realiza uma abordagem em longo prazo que verifica, principalmente, o comportamento da rede em face de demandas variáveis de tráfego e falhas casuais na rede que prejudiquem o seu desempenho. No entanto, para ser ter controle sobre a rede como um todo, é fundamental realizar o gerenciamento de cada componente essencial para, assim, poder corrigi-la e restabelecer a comunicação. Segundo SPECIALSKI (2002, online), são pontos importantes da gerência de falhas: apontar o componente exato onde a falha ocorreu; isolar o resto da rede da falha, de tal forma que ela continue a funcionar sem interferências; reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou; reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

  - A duração, impacto, e prejuízos advindos da falha podem ser minimizados e até mesmo eliminados pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um grau de “tolerância à falhas”

- **Gerenciamento de configuração –** Segundo Oliveira (2002, online), a gerência de configuração visa conhecer e controlar o estado do complexo formado pelas redes de uma instituição, o que inclui conhecer os dispositivos e a inter-relação dos mesmos. Na área de gerências de rede existem diversas definições como a de SPECIALSKI (2002, online):

> “O gerenciamento de configuração está relacionado com a inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado com as tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e do status dos componentes durante a operação da rede.”

  - Com o gerenciamento de configuração é possível que o administrador saiba informações sobre todos os dispositivos existentes em sua rede e suas configurações de *hardware* e *software*. As informações que podem ser gerenciadas podem ser quantidade de memória,

capacidade de armazenamento, versões de *softwares*, volume de entrada e saída de informações do banco de dados. Um caso onde se pode realizar gerência de configuração com eficiência é em servidores de alto desempenho que hospedam máquinas virtuais. As informações dessas máquinas virtuais que podem oferecer diferentes serviços como roteador, servidor de proxy, ou outros serviços devem ser apresentados e gerenciados.

- **Gerenciamento de contabilização –** O principal objetivo do gerenciamento de contabilização é permitir que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede, evitando que usuários da rede monopolizem os recursos, através dos privilégios atribuídos a si (KUROSE, ROSS, 2007, P. 574). Nesse contexto, é fundamental implantar quotas de utilização, cobrança por utilização e alocação de acesso privilegiado a recursos. O gerenciamento de contabilização, também, prevê que os usuários sejam assistidos a fim de assegurar a qualidade e o desempenho dos serviços disponibilizados em rede e, ainda, conhecer atividades com detalhes suficientes para se planejar o crescimento da rede.

- **Gerenciamento de segurança** – SPECIALSKI (2002, online) diz que o gerenciamento da segurança: “provê facilidades para proteger recursos da rede e informações dos usuários. Estas facilidades devem estar disponíveis apenas para usuários autorizados”, ou seja, o objetivo principal do gerenciamento de segurança é controlar, a partir de uma politica predefinida, os acessos aos recursos de uma rede. São politicas adotadas no gerenciamento de segurança: gerar, distribuir e armazenas chaves de criptografia de dados; realizar manutenção e distribuir senhas e informações de controle de acesso; liberar acesso à rede, ou parte dela, realizando monitoramento e controle de acesso às informações obtidas; e por fim, coletar, armazenar e examinar registros de auditoria e logs de segurança SPECIALSKI (2002, online). Logo, o gerenciamento de segurança tem por objetivo assegurar que os dados que trafegam pela rede cheguem ao seu destino com segurança, mantendo a confidencialidade das informações.

Para realizar a gerência nas cinco áreas apresentadas, de maneira prática e eficaz, é necessário o auxilio de ferramentas de gerência de redes, sendo que estas são criadas seguindo uma infraestrutura de gerenciamento. Essa infraestrutura de gerenciamento, bem como seu funcionamento, é apresentada na seção seguinte.

2.1.1. A infraestrutura de gerenciamento de rede

Podem ser encontradas várias definições de gerência de redes, como a de SAYDAM[1] (1996, apud KUROSE, ROSS, 2007, P. 575):

> "Gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de *hardware*, *software* e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável."

Realizar o monitoramento dos recursos de rede em uma organização exige que o administrador da rede realize coleta de informações dos dispositivos que estão sendo gerenciados. Uma ferramenta de gerência de rede é composta por três elementos:

- **Gerente –** O gerente consulta e obtém resposta atualizada dos objetos gerenciados (servidores, roteadores, *switchs, etc.*) e pode gravar informações para gerenciar os objetos;
- **Agente -** O agente recebe e executa as requisições realizadas pelo gerente, e quando configurado realiza notificações de falhas e/ou erros ocorridos no objeto gerenciado;
- **Objeto gerenciado -** O objeto gerenciado são todos os dispositivos que podem ser gerenciados tais como servidores, roteadores, *switchs, softwares,* etc*.*

A figura 1 mostra o funcionamento dos três elementos no processo de gerenciamento de objetos, sendo que a entidade gerenciadora é uma aplicação capaz de realizar a leitura da informação; o dispositivo gerenciado que é um *hardware* ou *software* que faz parte de uma rede gerenciada; e o agente é o responsável por realizar a comunicação entre entidade gerenciadora e os dispositivos gerenciados.

[1] SAYDAM, D. **Direito privado**. New York: SynOptics Communications, Inc, 1993.

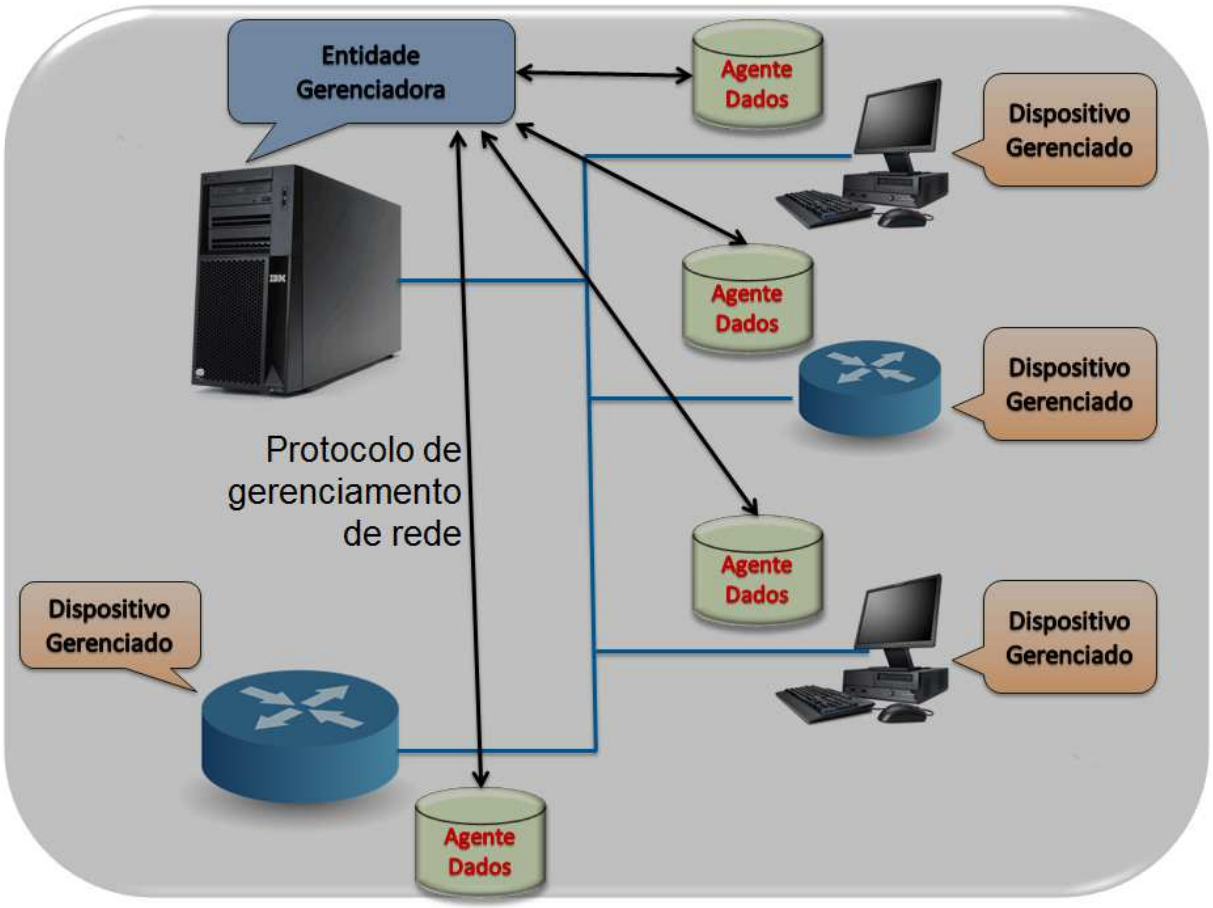

Figura 1- Principais componentes de uma arquitetura de gerenciamento de rede.
Fonte: KUROSE, ROSS, 2007, P. 576.

O administrador de rede, através de uma aplicação, realiza o controle e a coleta de informações dos dispositivos gerenciados. O objetivo principal da entidade gerenciadora é possibilitar que administrador interaja com os dispositivos gerenciáveis da rede realizando leitura e escrita nos dispositivos da rede.

Em uma rede, os dispositivos são os objetos gerenciados e alguns exemplos são roteadores, comutadores, modens, hosts, *softwares* de banco de dados etc. As informações desses dispositivos e *softwares* são armazenadas em uma base de dados de gerenciamento denominada *Management information base* (MIB).

A figura 1 apresenta, ainda, o protocolo de gerenciamento, que coordena a comunicação entre entidade gerenciadora e os objetos gerenciados. Através de parâmetros de comunicação, o protocolo de gerenciamento permite que a entidade gerenciadora consulte o estado de um dispositivo de rede e execute ações sobre o mesmo usando os agentes (KUROSE, ROSS, 2007, P. 576).

Vários padrões de gerenciamento de rede foram desenvolvidos desde o princípio da gerência de redes no início da década de 80, porém, entre os protocolos criados podem-se destacar dois que amadureceram e foram implementados, o SNMP(*Simple network management protocol*) e o OSI CMISE/CMIP (*common management service element/common management information protocol*) (KUROSE, ROSS, 2007, P. 576). No presente trabalho será apresentado o funcionamento do protocolo SNMP, pois é o protocolo utilizado na maior parte das ferramentas de gerência de rede atualmente. O protocolo SNMP é descrito na seção seguinte.

2.1.2. Protocolo SNMP

Apesar do que sua sigla sugere, Protocolo Simples de Gerência de Rede, o SNMP deixou de ser um protocolo simples e apresenta uma estrutura de gerenciamento avançada, possibilitando que ferramentas de gerência realizem um gerenciamento avançado dos equipamentos que fornecem suporte ao protocolo. O SNMP é utilizado para realizar o transporte de informações do objeto gerenciado para a entidade gerenciadora.

ABREU E PIRES (2003, online) afirmam que “o protocolo SNMP (*Simple Network Management Protocol*) foi desenvolvido para permitir que dispositivos de rede que utilizam o protocolo IP (*Internet Protocol*) possam ser gerenciados remotamente, através de um conjunto de “simples” operações. Essas operações são realizadas da entidade gerenciadora sob o objeto gerenciado.

Segundo Zeltserman (1999), os elementos gerenciados possuem um agente SNMP e uma base de dados denominada MIB (*Management Information Base*). O agente, através do protocolo de comunicação, é responsável por transmitir as informações armazenadas na MIB, Essas informações refletem a configuração e o comportamento dos elementos gerenciados e pode ser acessada em tempo real. Por exemplo, acessando-se dados da MIB pode-se obter a quantidade de *bytes* trafegados em uma interface em um determinado momento.

O SNMP possui poucos comandos, que são baseados em leitura e gravação de informações nas entidades gerenciadas. A estrutura de leitura e gravação é realizada por duas operações: uma que permite a escrita/alteração de informações dos objetos (SET) e a outra que realiza a leitura/coleta de informações dos objetos (GET) (PINHEIRO, 2006. online). Além das operações padrão de leitura e escrita

(GET e SET), o SNMP possui outro operador denominado TRAP que é utilizado para informar à entidade gerenciadora a ocorrência de eventos tais como quedas de energia, reinicialização, falhas de conexão e etc.

Em seu escopo de operação o protocolo SNMP trabalha como "*Manager"* e "*Agent",* de forma que a entidade gerenciadora comunica-se com o objeto gerenciado utilizando o protocolo SNMP. A figura 2 mostra o envio de TRAP e a comunicação entre entidade gerenciadora NMS (*Network Management System*) e objeto gerenciado.

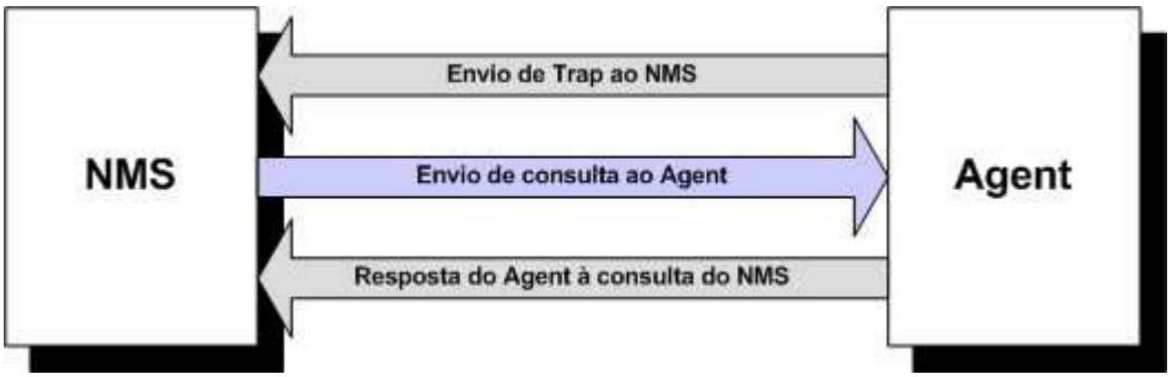

Figura 2- Relacionamento entre NMS e Agent
Fonte: ABREU, PIRES, 2003. Online

Como pode ser observado na figura 2: a entidade gerenciadora envia uma mensagem solicitando informações sobre o dispositivo gerenciado; o dispositivo, através do agente, responde as solicitações enviando para a entidade gerenciadora as informações como resposta à solicitação.

Existem três versões do protocolo SNMP que possuem a mesma concepção básica de comunicação entre entidade gerenciadora e objeto gerenciado, porém, existem algumas diferenças das funcionalidades entre as versões, a segurança é um delas. Algumas das funcionalidades e diferenças entre as versões serão apresentadas e comentadas na seção seguinte.

2.1.2.1. Versões do SNMP

Desde a criação da primeira versão do SNMP no ano de 1980, já foram lançadas outras duas versões, o SNMPv2 e SNMPv3. As versões foram lançadas com o

objetivo de corrigir erros e agregar funcionalidades e operações em relação às versões anteriores. As operações presentes em cada versão são:

- **SNMPv1** - O SNMPv1 é definido como “um protocolo simples de gerência de redes que é usado no gerenciamento entre estações de gerenciamento e agentes dos elementos de redes (CASE et al, 1990, p. 5). Por ter sido criado e implementado em pouco tempo, o SNMPv1 não possui critérios de segurança em seu escopo. Em seu trabalho, ABREU E PIRES(2003, online) afirma que o SNMPv1 baseia-se em “*community strings*”, que nada mais são que simples “*passwords*”, “*strings*” em formato texto aberto, que permitem que qualquer ferramenta de gerência que conheça esta *string* obtenha acesso aos dados do dispositivo gerenciado. SZTAJNBERG(1996, online), afirma que o SNMPv1 possui as seguintes operações:
    - **GetRequest** – comando utilizado para obter valores de uma variável de um objeto gerenciado;
    - **SetRequest** – define um novo valor de uma variável ou de uma lista de variáveis a partir de um OID passado como parâmetro. Novamente, uma resposta do tipo GetResponse chega à entidade gerenciadora com os valores correntes das variáveis em questão;
    - **Trap** – resposta ou notificação acionada devido à ocorrência de um evento.

  Para corrigir problemas na segurança e na estrutura das informações dos objetos, foi lançado o SNMPv2.

- A versão 2 do SNMP aborda em seu escopo correções na parte de segurança e inserção de novas operações de consulta às informações dos dispositivos gerenciados como, “*GetBulkRequest”* e *“InformRequest”*. MCCLOGHRIE et al (1996, online) afirma que o SNMPv2 operacionaliza sob um *framework* administrativo que define politicas de autenticação, autorização, controle de acesso e politicas de privacidade.
    - **GetNextRequest** – comando utilizado para obter o valor do próximo atributo, incrementando o OID passado como parâmetro.
    - **GetResponse** – resposta ou confirmação de uma operação de busca de atributos de um objeto.

- **GetBulkRequest** - obtém um bloco de respostas a partir de um identificador de objeto. O GetBulkRequest elimina uma das grandes limitações do SNMPv1 que é obter grandes blocos de dados a partir do OID de um objeto. Nas versões anteriores para obter informações de todas as interfaces de um *switch* era necessário realizar várias requisições de GetRequest. A operação GetBulkRequest realiza essa consulta em apenas uma requisição, trazendo para a entidade gerenciadora um bloco com informações das interfaces do *switch.*

Em relação à versão 1, o SNMPv2 melhorou muito no que tange a segurança e novas operações. Mesmo com as melhorias agregadas com a versão 2 o protocolo ainda apresenta falhas no que tange à segurança e a confirmação no recebimento de mensagens e ou notificações que alertam possíveis falhas no objeto gerenciado. As dificuldades enfrentadas na versão 2 somente é corrigida na versão 3 do SNMP.

- O SNMPv3 foi criado em 1999 por BLUMENTHAL e MUNDY et al (1999, online), onde os autores afirmam que o SNMPv3 é derivado e construído sobre as versões do SNMPv1 e SNMPv2, incrementando diretivas de segurança para: autenticação de gerentes autorizados; criptografia na troca de mensagens entre gerente e agentes, evitando a leitura por interceptação das mensagens por terceiros; e controle de acesso por configuração de perfis de agentes, oferecendo diferentes níveis de acesso ás informações da MIB. Além dos mecanismos de segurança o SNMPv3 também possui um nova operação:
  - **InformRequest** – ao receber uma mensagem ou notificação, retorna ao agente uma mensagem informando que recebeu a informação. Assim, se tem a certeza que o problema do equipamento é reconhecido pela entidade gerenciadora.

A tabela 1 apresenta uma relação entre as operações existentes em cada versão do SNMP. Essas operações foram explicadas anteriormente.

Tabela 1- Operações em diferentes versões do SNMP

SNMPv1	SNMPv2C	SNMPv3
GetRequest	GetRequest	GetRequest
SetRequest	SetRequest	SetRequest
Trap	Trap	Trap
	GetNextRequest	GetNextRequest
	GetResponse	GetResponse
	GetBulkRequest	GetBulkRequest
		InformRequest

Fonte: COUTO, 2012. Online.

A grande mudança que ocorre no SNMPv3 está vinculada ao seu modelo de acesso, o qual deixa de tratar o modelo de gerente e agente e passa a tratá-los como entidades SNMP. Cada entidade consiste de um motor SNMP e uma ou mais aplicações SNMP. Segundo Harrington, et al (2002, online), neste novo padrão, ilustrado na figura 3, o motor do SNMPv3 é composto por quatro peças: o *dispatcher*, o subsistema de processamento de mensagens, o subsistema de segurança, e do subsistema de controle de acesso.

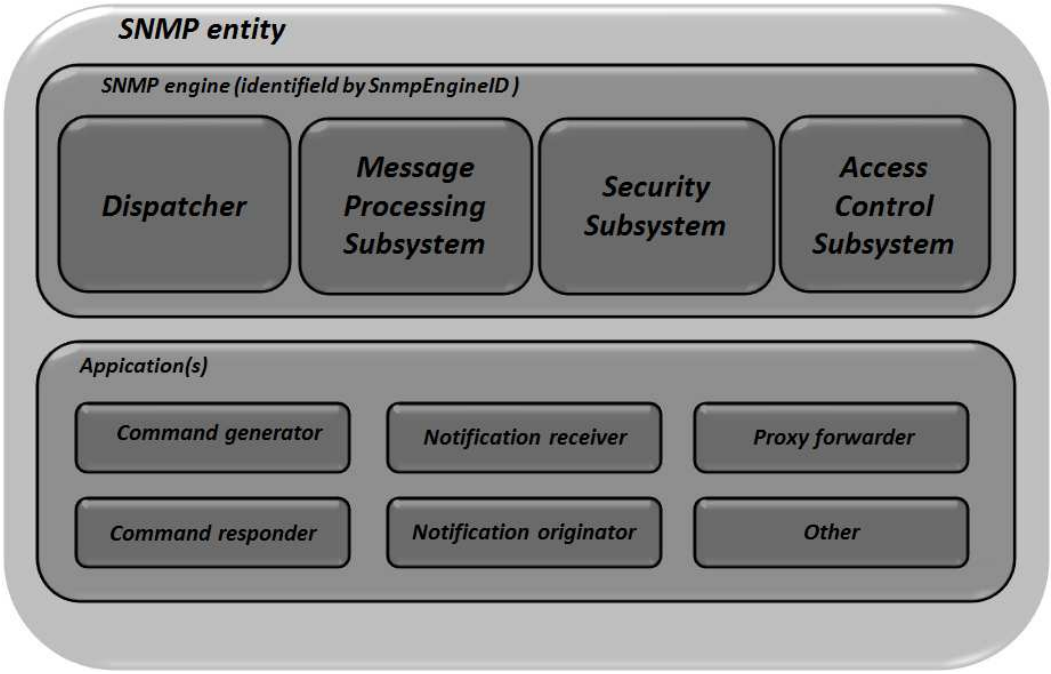

Figura 3 - Representação dos elementos das entidades no SNMPv3

Fonte: HARRINGTON, et al, 2002. Online.

Como mostra a figura 3, as entidades possuem um motor de busca que agrega funções de envio e recebimento de mensagens, autenticação de usuários, criptografia das mensagens enviadas e recebidas, e controle ás informações dos objetos gerenciados.

Muitas ferramentas permitem que o administrador trabalhe com as três versões do protocolo, permitindo que uma única ferramenta de gerência realize o gerenciamento de equipamentos que utilize qualquer versão do protocolo.

A seção seguinte aborda os conceitos e o funcionamento da MIB, local em que as informações do dispositivo, sistema e *softwares* são armazenadas para leitura utilizando o protocolo SNMP.

2.1.3. MIB

MIB (*Management Information Base*) é o nome conceitual para a informação de gerenciamento, incluindo os objetos gerenciados e seus parâmetros, operações e notificações que podem ser utilizadas para monitorar o status do equipamento. Pode-se também considerar as informações para a configuração do sistema como também pertencentes à MIB (MENEZES, SILVA, 1998. Online). As informações da MIB, consultadas ou gravadas pelo SNMP, refletem a situação atual do equipamento, podendo o gerente ser alertado caso algum parâmetro de objeto alcançar limites críticos ou mesmo não responder requisições do gerente.

Segundo PERKINS [2](1997 apud , MENEZES, SILVA, 1998. Online), as MIB's possuem tratamento e modelagem de informação de gerenciamento, normalmente, baseada em objetos. Essa abstração permite a modelagem de objetos que representarão a realidade de um acontecimento. Uma instância individual de um objeto gerenciado é uma variável da MIB.

Criada para atender as necessidades de gerência a MIB possui duas versões. A versão 1 foi utilizada até o lançamento da versão 2 do protocolo SNMP. O protocolo SNMPv2 já opera sobre o novo modelo organizacional dos objetos. A tabela 2 apresenta os objetos existentes no padrão internet da MIB versão I.

Tabela 2 - Número e descrição de objetos MIB - I

Grupo	Objetos para	Qtd. de Objetos
system	Informações básicas do sistema	3

[2] PERKINS, D. **Direito privado**. New York: SynOptics Communications, Inc, 1993.

interfaces	Interfaces de rede	22
at	Tradução de endereço	3
ip	*Software* de protocolo IP	33
icmp	Protocolo de estatíst. Para controle interno de mensagens	26
tcp	*Software* de protocolo TCP	17
udp	*Software* de protocolo UDP	4
egp	*Software* de protocolo EGP	6

Fonte: SZTAJNBERG, 1996. Online.

Como pode ser verificado na tabela 2, em sua raiz, que analogamente funciona como uma unidade de disco, a MIB possui 8 pastas, aqui denominados grupos. Cada grupo possui sub-grupos e assim sucessivamente até que se cheguem aos nós, local onde é armazenado informações dos objetos.

Tabela 3 - Número e descrição de objetos MIB-II

Grupo	Objetos para	Qtd	OID
system	Informações básicas do sistema	7	1.3.6.1.2.1.1
interfaces	Interfaces de rede	23	1.3.6.1.2.1.2
at	Tradução de endereço	3	1.3.6.1.2.1.3
ip	*Software* de protocolo IP	38	1.3.6.1.2.1.4
icmp	Protocolo de estatíst. Para controle interno de mensagens	26	1.3.6.1.2.1.5
tcp	*Software* de protocolo TCP	19	1.3.6.1.2.1.6
udp	*Software* de protocolo UDP	7	1.3.6.1.2.1.7
egp	*Software* de protocolo EGP	18	1.3.6.1.2.1.8
snmp	Aplicações SNMP	30	1.3.6.1.2.1.9

Fonte: SZTAJNBERG, 1996. Online.

A versão 2 da MIB apresenta maior quantidade de grupos e, consequentemente, de objetos para gerenciamento dos ativos de rede, que são apresentados na tabela 3. Atualmente, utiliza-se em equipamentos gerenciados o padrão da MIB-II.

Por existir um número grande de objetos é necessário que o administrador utilize uma ferramenta de gerência que auxilie na leitura as informações dos objetos gerenciados. As informações são gerenciadas a partir de um computador que utiliza um *software* de gerenciamento de ativos de rede. A próxima seção apresenta conceitos e operações que podem ser realizadas a partir de ferramentas de gerencia.

2.1.4. Ferramentas

A estrutura básica utilizada pela maioria das ferramentas de gerência de rede constitui em uma estação de gerenciamento, o agente, a base de informações gerenciáveis (MIB) e o protocolo de gerenciamento no caso o SNMP. Existem diversas ferramentas de gerência, tais como CACIC, CACTI, ZABBIX, AKER, etc. Para realizar a gerência e o controle dos ativos de rede virtualizados neste trabalho, será utilizado o gerenciador de redes ZABBIX.

O ZABBIX é uma ferramenta gratuita que realiza o gerenciamento de rede e é utilizada principalmente no monitoramento de dispositivos de rede no âmbito de gerenciar o volume informações que trafega nos equipamentos da rede, recursos de *hardwares* (discos rígidos, memória, processador, etc.), versões e *softwares* instalados e em execução, etc. A ferramenta ainda possui diversas diretivas de controle de usuários, gerenciamento de ativos de rede e etc. O ZABBIX também realiza o monitoramento do fluxo de entrada e saída de informações de aplicações tais como o MySQL. Por ser uma ferramenta de grande eficácia e fácil instalação e gerenciamento de ativos, será uma das ferramentas utilizadas para realizar este trabalho.

Uma das principais dificuldades de se gerenciar uma rede não está vinculada ao funcionamento físico e sim á gestão do controle de usuários e o uso de insumos da rede pelos mesmos. Visando a priorização de serviços ou aplicações que utilizam o protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*) [3] e necessitam de maior tráfego, criou-se sobre o protocolo TCP/IP mecanismos que realizam a priorização de dados de aplicações visando garantir uma qualidade satisfatória as redes corporativas. Para caracterizar um mecanismo que possibilita garantir qualidade de serviços, a seção seguinte aborda os conceitos e o funcionamento de QoS (*Quality of Services*).

2.2. QoS(*Quality of Serviços*)

Criado com o intuito de melhorar os serviços que utilizam a comunicação em redes TCP/IP, o QoS(*Quality of Serviços*) vem assegurar que a rede tenha requisitos mínimos de qualidade nos serviços definidos como prioritários. TANENBAUM (2011, p.253) afirma que QoS é a necessidade de manter parâmetros mínimos para entrega

[3] *Transmission Control Protocol / Internet Protocol* (TCP/IP): protocolo criado para realizar a comunicação de computadores. É usado como protocolo primário da rede e na internet para o envio e recebimento de mensagens.

e uso de um serviço por uma aplicação, diferenciando o tipo de tráfego das diferentes aplicações existente em uma rede.

Com a evolução das tecnologias de TI e o aumento na largura de banda, dificilmente se pensa no uso de QoS para assegurar o desempenho satisfatório de serviços importantes que utilizam a rede como canal de comunicação. Porém, com essa evolução das tecnologias e conexões mais velozes, percebe-se também o consumo cada vez maior de aplicações que utilizam grandes fatias dos *links* de internet. Por isso, quando o tráfego começa a aumentar, é importante buscar mecanismos que assegurem que os serviços mais importantes para as organizações possuam níveis aceitáveis de desempenho em horários que a rede apresenta níveis críticos de tráfego.

A implantação de QoS em uma rede é feita com o intuito de assegurar a satisfação dos usuários que utilizam serviços ou transmitem dados que demandam requisitos mínimos para seu funcionamento. Isso porque com o uso de QoS é possível reduzir a perda e reenvio de pacotes “preferenciais”, otimizando, assim, o consumo de banda. Vale ressaltar que implantar QoS em uma rede não assegura resolver seus problemas com o tráfego, porém pode prevenir e minimizar os problemas relacionados á quantidade de tráfego da rede, permitindo que aplicações tipos específicos de tráfegos tenha maior prioridade na rede.

A seção a seguinte apresenta conceitos acerca dos dois tipos de serviços de QoS existentes. De modo conciso, são apresentadas as principais características e seu funcionamento.

2.2.1. Serviços de QoS

Os diferentes tipos de serviços existentes na internet possuem requisitos mínimos exigidos pelas aplicações para serem executados com qualidade. Para garantir que as aplicações executem esses serviços sem gerar problemas ou insatisfação ao usuário, o IETF(Internet Engineering Task Force) criou o mecanismo de priorização de serviços. Segundo DAVIDSON, et al(2008, p.183), para classificar a priorização de serviços o QoS é dividido em Serviços diferenciados e serviços integrados.

2.2.1.1. Serviços Integrados

Criado para trabalhar em aplicações *unicast* e *multicast*, o serviço integrado é tipicamente utilizado para assegurar que um fluxo em específico de aplicações ou um grupo de tráfego receba um nível de tráfego apropriado ao longo de todo o caminho a ser percorrido na rede antes de realizar o envio do tráfego (DAVIDSON, et al, 2008, p.183).

Esse mecanismo é assegurado através do protocolo RSVP(*ReSerVation Protocol*), que realiza as reservas de banda para o envio dos pacotes, e é destinado á aplicações em tempo real onde a qualidade está ligada diretamente a inexistência congestionamento e perda de pacotes nos roteadores. Caso a largura de banda não seja suficiente para atender a aplicação, o protocolo informa a falha.

O QoS baseado em serviços integrados é mais simples de operacionalizar e de ser implementado.

2.2.1.2. Serviços Diferenciados

Nos serviços diferenciados, a diferenciação dos pacotes é realizada conforme a prioridade atribuída ao pacote, onde estes são agrupados e enviados conforme sua prioridade. O objetivo dos serviços diferenciados pode ser facilmente entendido quando comparado com um serviço oferecido por companhias aéreas. A diferenciação entre as classes executivas e econômicas, em que a classe executiva possui maior conforto e melhor atendimento que a classe econômica. O mesmo ocorre com a classificação de prioridades nos serviços de rede.

O QoS baseado em serviços diferenciados é tipicamente utilizado em grandes redes para classificar o nível apropriado de QoS no fluxo específico de aplicações ou grupo de tráfego que uma corporação ou indivíduo demanda. Os serviços diferenciados atribuem seu nível de prioridade em um campo específico no pacote a fim de assinalar a prioridade do serviço sem depender ou verificar os protocolos de sinalização em cada salto ou mesmo no fluxo. A prioridade é definida no campo tipo de serviço ToS (type of service) do cabeçalho do protocolo IPv4 ou no campo classe de tráfego TC (traffic of class) do protocolo IPv6 (DAVIDSON, et al, 2008, p.194), . Como apresenta a figura 4.

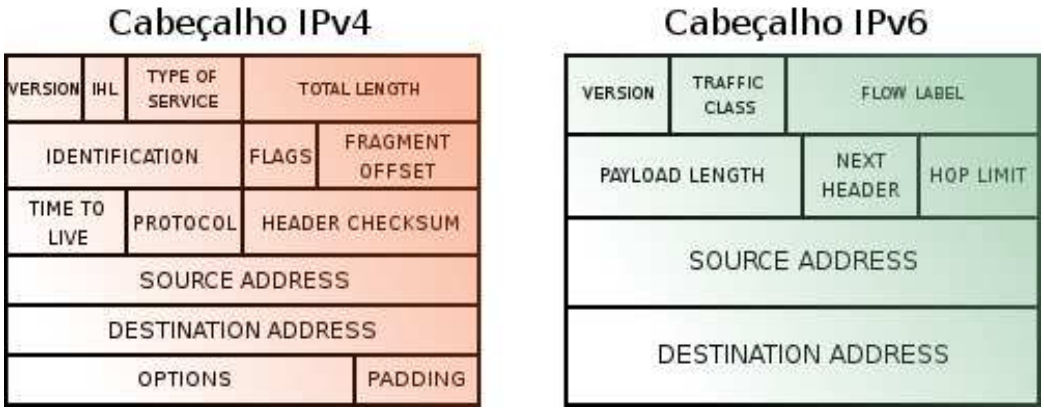

Figura 4 - Campo *Type of Service* ipv4 e *Traffic class* ipv6.

Fonte: adaptado de DAVIDSON, et al, 2008, p.194.

O campo ToS ou ToC possui 8 bits que permitem classificar os serviços com 8(0-7) tipos diferentes de prioridades de serviços. Os principais serviços e prioridades a eles relacionados são apresentados na tabela 4.

Tabela 4 - Prioridades dos serviços

Tipo de serviço	Propósito
Rotina	Setar a precedência de rotina (0)
Prioridade	Setar a precedência de prioridade (1)
Imediato	Setar a precedência de imediato(2)
Flash	Setar a precedência de flash(3)
Flash-overrride	Setar a precedência de flash-override(4)
Crítico	Setar a precedência de critico(5)
Internet	Setar a precedência de internet(6)
Rede	Setar a precedência de rede(7)

Fonte: DAVIDSON, et al, 2008, p.195.

Nesse modelo de priorização de serviços os níveis 6 e 7(internet e rede)não são utilizados para categorização de serviços. O agrupamento de pacotes é realizado conforme nível de prioridade semelhantes e utiliza algoritmo de ordenamento de FIFO (*First In First Out*), primeiro a chegar primeiro a sair.

Para garantir que os pacotes trafeguem até o destino com a mesma prioridade definida na origem, o IETF criou um padrão que é implementado pelas operadoras de internet, em que padronizou conjuntos de comportamentos dos roteadores para serem empregados aos pacotes prioritários. Estes comportamentos são distinguidos como “comportamentos agregados por nó (PHB – Per Hop Behavior). Existem dois tipos de encaminhamentos de pacotes baseados em PHB, o encaminhamento expresso e o encaminhamento assegurado (TANENBAUM, 2011. p. 265).

O tratamento que cada pacote receberá vai depender da definição do campo TS. É importante que na rede local esses níveis de prioridades sejam definidos de maneiras distintas, para que não gere uma fila única, provocando um gargalo na fila de pacotes regulares, como mostra a figura 5.

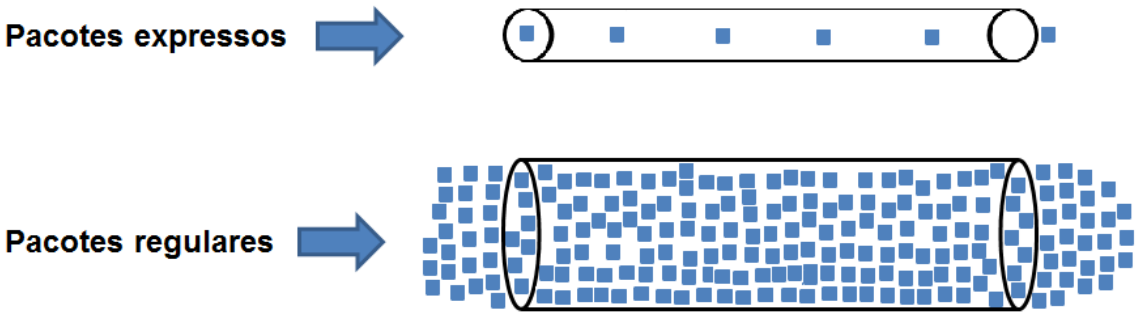

Figura 5 - Fluxo de pacotes por prioridades

Fonte: Adaptado de TANENBAUM, 2011. p. 265.

O funcionamento ideal é existir diversas prioridades, de forma que o tráfego gerado ingresse em uma das filas existentes no roteador. Essas filas são esvaziadas conforme o nível de prioridade, logo, as filas com maiores prioridades utilizam os insumos de banda até esvaziar, em seguida as filas com prioridades menores realizam o envio de seus pacotes.

Um exemplo que mostra a importância de QoS é na ocorrência de filas de pacotes no roteador: caso a fila esteja cheia e o roteador não tenha implementado o mecanismo de QoS, ocorre o descarte de pacotes de maneira aleatória, podendo ser descartado pacotes de aplicações relevantes; em um roteador que possui o mecanismo de QoS, quando a fila está cheia e ocorre a exclusão de pacotes, o descarte dos pacotes ocorre de maneira inteligente, sendo descartados inicialmente os pacotes com menor prioridade, de aplicações menos relevantes.

Como os serviços diferenciados propiciam a discriminação de serviços progressiva na Internet, sem precisar de estados por fluxo e de sinalização a cada

salto, de forma que não é necessário realizar uma reserva de QoS em cada fluxo, será o mecanismo adotado para a realização desse projeto.

Existe parâmetros que auxiliam a mensurar a classificação adequada de cada fluxo dos serviços de aplicações existentes na rede. É importante realizar a verificação desses parâmetros para se certificar que a rede está funcionando adequadamente e viabilizar a definição de prioridades para se implantar o QoS. A seção seguinte apresenta os parâmetros utilizados para classificar os serviços existentes na rede.

2.2.2. Parâmetros de QoS

Garantir QoS em uma rede significa assegurar garantias de transmissão e fluxo prioritário para determinados tipos de dados que trafegam por ela. Segundo TANENBAUM (2011, p. 254), a garantia de transmissão no encaminhamento expresso de pacotes é realizada através da junção de alguns dos parâmetros a seguir:

- Atraso – é o tempo necessário para um pacote ser transmitido do emissor, passando por todos os nodes do caminho, até ser entregue ao receptor. Quanto maior o tempo necessário para realizar esse percurso, maiores os problemas, e dados causados ás aplicações, comprometendo a eficiência e qualidade no serviço que utiliza o protocolo TCP/IP. Algumas aplicações sensíveis á atrasos exigem o cumprimento de níveis máximos de retardo para jitter funcionar adequadamente (vídeo e áudio, por exemplo).
- Jitter – ou variação do atraso end-to-end ocorre quando uma há uma variação muito grande na entrega dos pacotes, ocorrendo assim variações acentuadas de retardo ao entregar os pacotes. A ocorrência acentuada do jitter provoca uma recepção não regular dos pacotes, provocando erros e atrasos (delay) á aplicação que espera o recebimento dos pacotes.
- Largura de banda – é a taxa de transmissão ou vazão máxima de dados sustentada entre dois pontos finais. A largura de banda é baseada na conexão com menor capacidade de transmissão, seja uma das pontas ou nos roteadores existentes no caminho. A largura de banda também pode ser limitada pela quantidade de fluxos que compartilham a utilização de determinados componentes da rede.

- Perda de pacotes – uma das propriedades utilizadas para mensurar a confiabilidade de uma rede é a perda ou erro na entrega de pacotes nos sistemas de transmissão. Nas definições do protocolo TCP/IP é considerado que menos de 0,2% da perda de pacotes está vinculada á falhas físicas. Uma maneira de assegurar e expressar a confiabilidade de uma rede é realizar o roteamento. Porém isso pode provocar atrasos na entrega dos pacotes, alterar a ordem de entrega ou ocorrer a exclusão do pacote na ocorrência de filas cheias em um dos roteadores da rede.

A seção a seguinte apresenta a metodologia para o desenvolvimento do projeto. De modo conciso, são apresentadas as principais atividades e materiais já produzidos e que ainda serão utilizados.

3 MATERIAIS E MÉTODOS

Nessa seção são apresentadas as ferramentas e a metodologia que foram utilizadas para o projeto e execução deste trabalho, que consistiu em conhecer e simular em ambiente virtual a rede LAN do CEULP/ULBRA para propor melhorias usando ferramentas de gerência de redes e QoS.

3.1. Materiais

Para a realização do trabalho foram criados dois ambientes virtuais: o primeiro simula o ambiente de rede atual do CEULP/ULBRA; o segundo é constituído pelo ambiente proposto, que acrescenta ao primeiro o uso da ferramenta de gerenciamento de rede Zabbix e a priorização de tráfego utilizando QoS, visando a melhoria da rede.

Para a criação dos ambientes virtuais, foi utilizado um computador desktop da marca Itautec, modelo Infoway ST 4272, com processador core I7-2600k, com 3.40GHz e 8 GB de memória RAM. O sistema operacional instalado no desktop é o Windows 7 Professional de 64 Bits, na máquina virtual que simula a rede administrativa foi utilizado o Debian 6.0, o Windows XP professional na máquina que simula a rede acadêmica e o Windows Server 2008 *enterprise edition* na máquina virtual que simula os servidores do portal.

Os softwares utilizados para a criação do ambiente virtual e realização de testes, foram:

- Virtualbox: ferramenta de virtualização de sistemas operacionais, usada para a criação dos dois ambientes virtuais. Foi escolhido por possuir, entre outras características, o fácil gerenciamento das máquinas criadas, bem como apresenta a funcionalidade exportar uma máquina virtual já existente. Não houve estudo prévio comparativo com outras ferramentas de virtualização para a definição de uso do VirtualBox;
- Zabbix: gerenciador de dispositivos e ativos de rede, utilizado para monitorar as máquinas virtuais que simulam o ambiente do CEULP/ULBRA no ambiente proposto. Essa ferramenta foi escolhida por possuir a

personalização de perfis de usuários para gerência, por ser uma ferramenta com gerência WEB, por realizar controle de inventário e gerar relatórios e, principalmente, por ser uma ferramenta grátis. Porém, é importante ressaltar que não foi realizado um estudo comparativo com outras ferramentas de gerência para a definição do uso do Zabbix como ferramenta de gerência

- QoS: priorização de tráfego e controle de *bandwidth* utilizando o algoritmo de ordenação de tráfego HTB (*Hierarchical Token Bucket*). O HTB foi inserido no Kernel a partir da versão 2.4.20 e implementa uma fila com suporte a várias classes para controle de tráfego (STALO, 2009, P.247);
- SqStat: ferramenta de monitoramento de conexões, usado para monitorar em tempo real as conexões existentes na rede ou em um host específico. Foi utilizada para realizar o monitoramento dos tipos e o volume de tráfego das redes acadêmica e administrativa. Foi definida pela fácil interpretação dos dados apresentados na interface WEB e por exibir os links de onde são baixados os arquivos, bem como o nome dos arquivos baixados e as taxas de transferências;
- SARG: ferramenta que possibilita interpretar os logs do Squid.. Esta foi utilizada para realizar um mapeamento do volume e do tipo de tráfego da rede do CEULP/ULBRA. Existem outras ferramentas no mercado que atendem a mesma demanda, porém, o SARG foi definido por ser uma ferramenta já utilizada pelo administrador da rede do CEULP.
- IfTop: monitor de conexões em tempo real com filtros e ordenação por interfaces. Foi utilizada para leituras das conexões em tempo real , onde as leituras foram ordenadas por classificação e por utilização (*top ranking*). Foi escolhida por apresentar as conexões com maior exatidão se comparada com outras ferramentas e ainda por ser uma ferramenta gratuita. A instalação e uso da ferramenta é realizada de maneira simples e não requer qualquer configuração especial ;
- Iperf: gerador de tráfego para ambientes Windows e Linux, usado para simular e realizar os testes de tráfego. A ferramenta realiza a injeção de tráfego na rede para simular o volume de tráfego do ambiente real.

A descrição dos softwares utilizados, enfocando as suas principais características e funcionalidades serão apresentadas nas subseções seguintes. O VirtualBox não será apresentando por ser uma ferramenta genérica e não apresenta uma caraterística em particular que justifique a sua apresentação neste trabalho.

3.1.1. Zabbix

Criado em 2001 por Alexei Vladishev e mantido atualizado pela empresa Zabbix SAI, o Zabbix é uma ferramenta gratuita utilizada para realizar o gerenciamento e acompanhar o desempenho de ativos de rede (ZABBIX, 2013, ONLINE). Com a gerência centralizada WEB, essa ferramenta de gerência de rede possui em seu portfólio de funcionalidades as seguintes características:

- Auto-descoberta de dispositivos de rede;
- Autenticação segura de usuário;
- Permissões flexíveis de usuário;
- Monitoramento de volume de entrada e saída de informações das aplicações e de banco de dados;
- Monitoramento distribuído com a administração centralizada via WEB;
- Aplicação servidor compatível com os sistemas operacionais Linux, Solaris, HP-UX, AIX, BSD Livre, Open BSD, Mac OS X;
- Coleta de informações utilizando apenas o serviço de SNMP;
- Aplicação cliente de alta performance compatível com Linux, Solaris, HP-UX, AIX, BSD Livre, Open BSD, OS X, Tru64/OSF1, NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista e Windows 7;
- Gerar diversos relatórios (Softwares instalados, consumo de banda por host, disponibilidade de equipamento etc.).

. O Zabbix também consegue realizar a coleta de informações utilizando serviços de web e e-mail, pela checagem simples de envio e recebimento de respostas.

O servidor Zabbix (Zabbix server) é responsável por coletar e receber as informações e notificações dos dispositivos gerenciados, e é o principal elemento para o gerenciamento da rede (ZABBIX, 2013, ONLINE). Este é o responsável por

coletar as informações via SNMP como informações de disponibilidade, usabilidade e integridade do equipamento, coletadas pelo agente em um dispositivo gerenciado. Após o recebimento, a aplicação processa as informações e armazena no banco de dados, possibilitando ao gerente extrair relatórios e acompanhar toda a gerência da rede pela aplicação WEB.

3.1.2. SqStat

Desenvolvida em PHP, a ferramenta SqStat é um *script* que acessa os logs do *Squid* e, em tempo real, gera um relatório das conexões existentes dos *hosts* da rede (SAMORUKOV, 2006, ONLINE). Essa ferramenta permite que o administrador realize uma análise do tráfego da rede para detectar o alto consumo de banda por um host especifico, bem como saber o tipo de tráfego, a origem e o destino.

A figura 6 apresenta a interface do SqStat em execução e apresenta informações dos acessos existentes no momento da analise do tráfego.

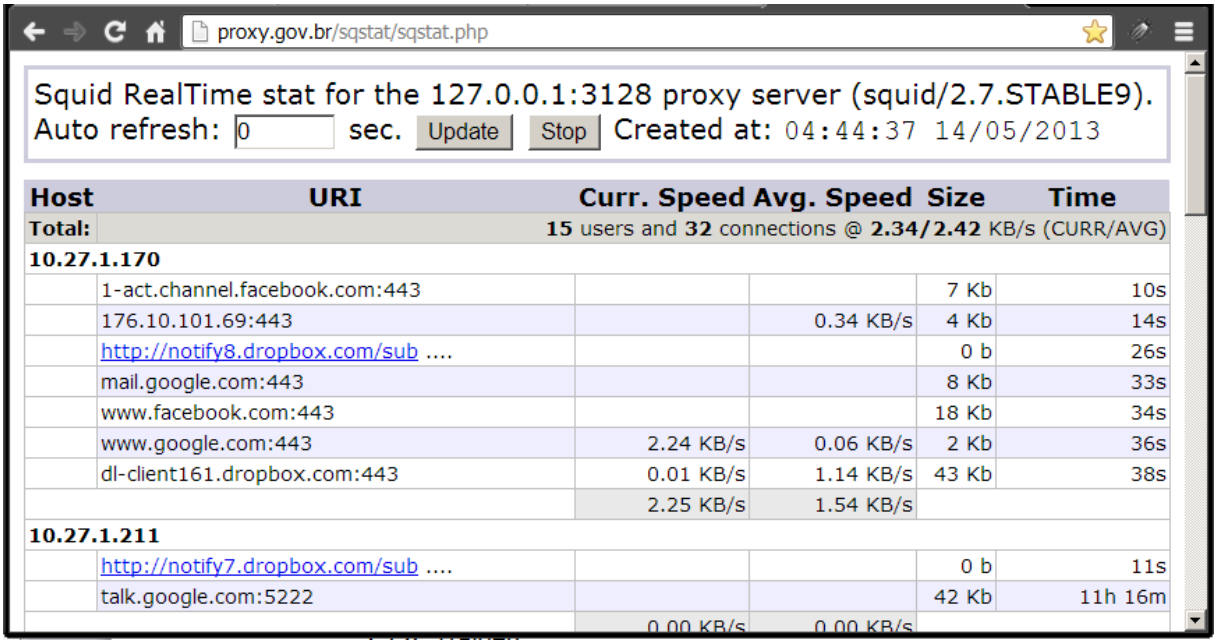

Figura 6: Tela do SqStat no monitoramento de conexões

A figura 6 apresenta os resultados disponibilizados pelo SqStat no monitoramento das conexões de rede em execução. A imagem traz uma série de informações que auxiliam o gerente a visualizar as conexões: o host que fez a requisição, o destino da requisição, o uso de banda por aplicação, a média de banda por aplicação, o tempo que a conexão está em vigência e a quantidade de bits consumidos por cada aplicação. Ao final do relatório de conexões vigente de cada

host, o SqStat apresenta a soma do consumo de todas as aplicações, bem como a média de velocidade das aplicações.

3.1.3. SARG

O SARG é uma fermenta de interpretação de *logs* do Squid que consulta os *logs* do Squid e apresenta essas informações em uma página WEB (SAMORUKOV, 2007, ONLINE). Entre os relatórios apresentadas estão o volume de tráfego de um determinado host e as páginas acessadas pelo mesmo.

A figura 7 mostra a interface do SARG na apresentação do relatório de páginas mais acessadas, ordenadas pela quantidade de bytes trafegados na rede.

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO	
www.previdenciasocial.gov.br	73	465,656	26.55%	58.85%	41.15%	00:00:12	12,639	21.49%	
www.mte.gov.br	71	429,031	24.46%	56.22%	43.78%	00:00:17	17,195	29.24%	
www.sindilojas-sp.org.br	6	321,048	18.30%	100.00%	0.00%	00:00:02	2,242	3.81%	
www.barreiro.com.br	65	196,028	11.18%	100.00%	0.00%	00:00:08	8,024	13.65%	
www.sescon.org.br	42	185,319	10.57%	100.00%	0.00%	00:00:03	3,309	5.63%	
www.eaa.org.br	10	44,011	2.51%	53.34%	46.66%	00:00:05	5,236	8.90%	
humortadela1.uol.com.br	20	24,342	1.73%	100.00%	0.00%	00:00:03	3,030	5.15%	NEGADO
fiscosoft.bighost.com.br	15	24,342	1.39%	100.00%	0.00%	00:00:03	3,157	5.37%	NEGADO
www40.dataprev.gov.br	4	20,021	1.14%	92.25%	7.75%	00:00:01	1,158	1.97%	
humortadela.uol.com.br	13	19,968	1.14%	100.00%	0.00%	00:00:00	107	0.18%	NEGADO
www.dataprev.gov.br	14	8,755	0.50%	100.00%	0.00%	00:00:00	302	0.51%	
graphics.hotmail.com	5	7,572	0.43%	100.00%	0.00%	00:00:01	1,110	1.89%	NEGADO
www14.bancobrasil.com.br:443	1	1,484	0.08%	100.00%	0.00%	00:00:00	2	0.00%	NEGADO
www.fiscosoft.com.br	2	438	0.02%	0.00%	100.00%	00:00:01	1,290	2.19%	
TOTAL	**341**	**1,753,993**	**2.91%**	**77.08%**	**22.92%**	**00:00:58**	**58,801**	**0.38%**	
MÉDIA	**1,783**	**2,413,167**				**00:10:25**	**625,066**	**4.00%**	

Figura 7: Interface do SARG

As informações, apresentadas pela ferramenta, são importantes para que o gerente possa analisar o tráfego da rede e verifique quais as páginas mais acessadas, os usuários que mais consomem banda, o volume total consumido pelos *hosts* da rede, a quantidade de *hosts* que acessaram, a média de tráfego por *host* etc.

A atualização das informações apresentadas se dá a partir de um intervalo de tempo configurado na instalação da ferramenta. Por padrão, essas informações são atualizadas a cada 24 horas, ou seja, o SARG consulta e abstrai as informações da base de logs do Squid uma vez por dia. Essa consulta diária se dá pelo tamanho da base de dados do Squid que, dependendo do tamanho da rede, pode ficar muito grande, o que pode provocar lentidão no funcionamento do proxy, o que não é interessante.

3.1.4. IfTop

O IfTop é uma solução de código livre utilizada para o monitoramento de tráfego de rede (WARREM, 2009, ONLINE). Ao contrário de outras ferramentas que analisam dados históricos em curto espaço temporal, o IfTop realiza um monitoramento em tempo real.

No mercado existem diversas soluções semelhantes ao IfTop, tais como Iptop e Htop. O diferencial do IfTop é a fácil criação de sintaxes de filtros e a eficiência na apresentação das informações. A Figura 8: Visualização de conexões no IfTopexibe o resultado apresentado pelo IfTop após a execução do comando "*iftop -i eth1*". O comando citado executa uma instância do programa IfTop que exibe apenas as conexões requisitadas a partir da interface eth1.

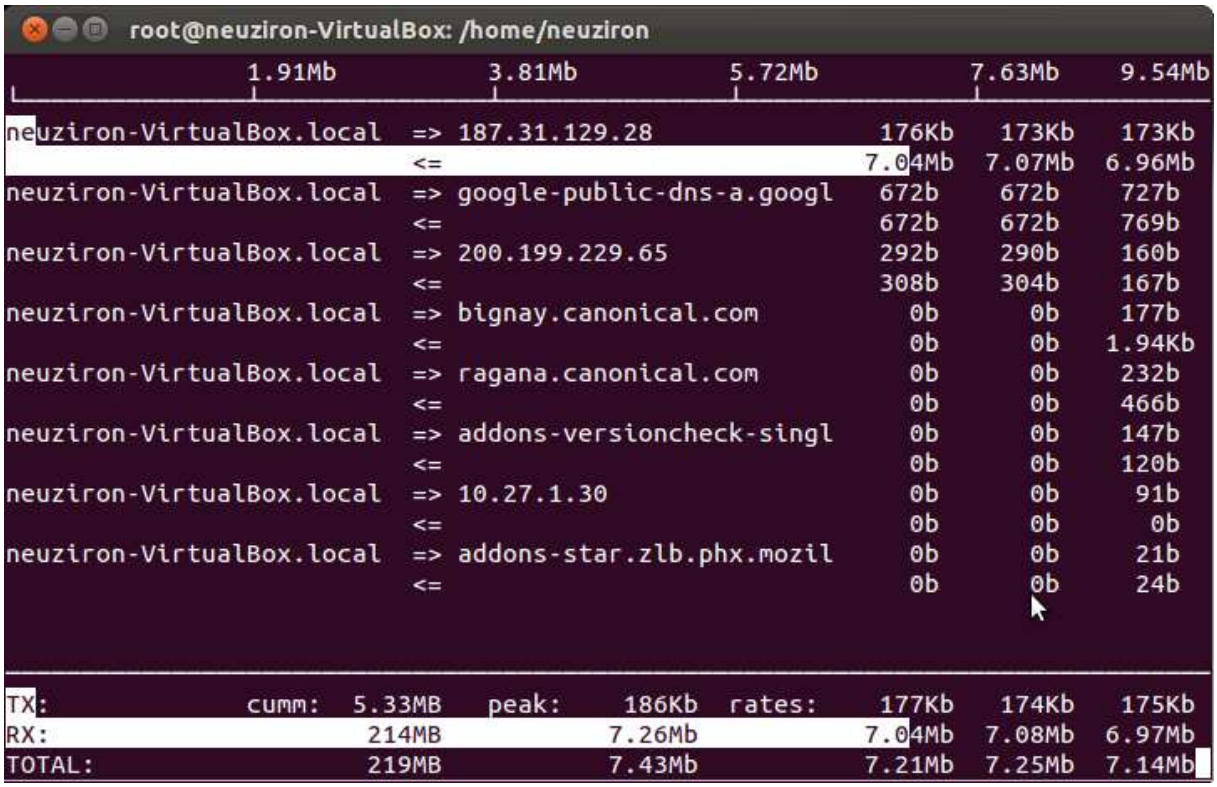

Figura 8: Visualização de conexões no IfTop

A Figura 8: Visualização de conexões no IfTop exibe as conexões em execução, informações de taxas de transferências, origem e destino dos pacotes, total de dados trafegados em cada uma das conexões, a soma de todos os dados enviados e recebidos etc. Como o comando foi executado em um host comum, a imagem mostra apenas as requisições do host "*neuziron-VirtualBox.local*". As setas "=>" e "<=" correspondem às requisições de *Upload* e *Download* respectivamente. .

O IfTop não armazena em uma base de dados as informações das conexões, por isso é necessária a utilização do SARG na apresentação dos dados históricos, pois ele coleta o *log* do Squid e armazena em uma base de dados, podendo ser usado para verificações de dados históricos.

3.1.5. Iperf

O Iperf é uma ferramenta gratuita que foi desenvolvida para gerar tráfego de rede e auxiliar gerentes e administradores na realização de testes sobre as redes de computadores. Isto porque ela possibilita realizar a injeção de dados na rede para simular o tráfego TCP e UDP entre 2 hosts de uma rede (SOURCEFORGE.NET, 2008, ONLINE). No caso, vale ressaltar que os testes são baseados em parâmetros configurados e, ao final, são apresentados relatórios contendo largura de banda utilizada, atraso, *jitter* e perda de pacotes.

Desenvolvida em C++ pela DAST (*Distributed Applications Support Team*) e pelo NLANR (*National Laboratory for Applied Network Research*), o Iperf não possui interface gráfica e é executado exclusivamente por terminal (SOURCEFORGE, 2013, ONLINE).

Para a realização dos testes básicos utilizando o Iperf, é necessário configurá-lo no host que vai ser testado como servidor através do parâmetro "*iperf -s*", onde o "-s" indica que o host será o servidor. Em seguida, o host cliente é configurado através do parâmetro "*iperf –c <IP>*", onde o parâmetro "-c" indica que o host será o cliente e realizará requisições para o IP do servidor.

Dessa forma, com os conceitos apresentados na revisão de literatura, as ferramentas e materiais descritos acima, se torna possível entender os conceitos e realizar a implementação da gerência de redes do CEULP/ULBRA, bem como apresentar resultados e relatórios que podem ser comparados para apresentar melhorias que se espera ao finalizar este trabalho. Na próxima seção será abordada a metodologia seguida para o desenvolvimento deste trabalho.

3.2. Metodologia

A primeira etapa deste trabalho constituiu nos estudos dos conceitos envolvidos e na elaboração do referencial teórico acerca do tema proposto. Para isso, os principais materiais estudados foram livros, dissertações, normas e artigos científicos.

Considerando que o objetivo do trabalho é propor melhorias usando ferramentas de gerência de redes e QoS, os conteúdos abordados na primeira etapa foram:

- Gerência de redes: principais conceitos acerca de gerência de rede e os mecanismos de gerência existentes;
- Ferramentas de gerência: estrutura básica das ferramentas, tipos de gerenciamento e tipos de ativos que podem ser gerenciados;
- Protocolo de comunicação de gerência: funcionamento e mecanismo de comunicação do protocolo de gerência de SNMP;
- QoS (Qualidade de serviços): principais conceitos e funcionamento de priorização de tráfego em redes de computadores.

A partir do estudo realizado acerca dos conceitos envolvidos, foi possível vislumbrar o uso de gerência de redes e da implementação de QoS para oferecer melhoria na rede do CEULP/ULBRA. Utilizar uma ferramenta de Gerência de Redes é interessante para auxiliar o gerente da rede no monitoramento dos dispositivos (ex. tempo de atividade, arquitetura de *hardware* etc), do consumo da banda, do tráfego da rede local etc.. Já utilizar ferramenta de QoS é interessante para priorizar o tráfego de forma que os serviços que demandam maior urgência são priorizados quando requeridos em paralelo a solicitações menos relevantes.

A próxima etapa consistiu na realização do levantamento de informações sobre a rede atual do CEULP/ULBRA, para que fosse possível criar os cenários. Para isso, foram feitas entrevistas estruturadas com os responsáveis pela rede do portal e pelas redes administrativa e acadêmica. O formulário que os responsáveis preencheram estão no APÊNDICE A deste documento.

Na entrevista realizada com o coordenador das redes Acadêmica e Administrativa, Israel Andrade Pinheiro, foram obtidas as seguintes informações:

- Quantidade de dispositivos das redes acadêmica e administrativa;
- Informações sobre os servidores de rede;
- Regras e configurações dos servidores de firewall;
- Regras e configurações do proxy;
- Softwares instalados nos ambientes Administrativo e Acadêmico;

- Informações relativas a volume e tipo de tráfego, que foram obtidas utilizando o interpretador de logs do Squid (SARG) e a ferramenta de monitoramento de conexões SqStat.

Além das informações cedidas na entrevista, foi fornecido os arquivos de configuração do Squid3 dos servidores de firewall das redes administrativa e acadêmica. Os arquivos fornecidos serão utilizados para na criação das máquinas virtuais que simularão os servidores de firewall e proxy das respectivas redes.

Para obter informações do portal, foi realizada entrevista com o Prof. M.Sc Jackson Gomes de Souza, responsável pelo portal. Na entrevista foram coletadas informações sobre:

- Volume de tráfego;
- Tipos de tráfego;
- Períodos e horários de picos;
- Médias de tráfego de acesso à internet.

As informações repassadas pelo prof. Jackson foram levantadas utilizando o *Google Analytics*, desenvolvido pela Google e respondem as perguntas do APENDICÊ B deste documento.

Após a fase de estudos e compreensão do ambiente e das possibilidades de oferecer melhoria à rede, definiu-se que para a execução do trabalho seriam criados dois cenários distintos:

- Cenário 1: criado para simular o ambiente de rede atual do CEULP. Esse cenário constitui em um ambiente virtual composto por máquinas virtuais que simulam as redes administrativa, acadêmica, do portal, servidores de firewall e servidor de gateway das redes administrativa acadêmica;
- Cenário 2: simula o ambiente proposto e foi criado para demonstrar a sugestão da nova configuração a ser implantada e verificar a possível melhora do comportamento da rede após a mudança. Além de adicionar as ferramentas de gerência de redes e de QoS, definidas nesse trabalho, foram realizadas modificações no arquivo de

configuração do proxy. As alterações no arquivo, bem como as melhorias alcançadas serão apresentas nos resultados deste trabalho.

A partir dessas informações foi possível desenhar a topologia da rede atual do CEULP e projetar os cenários para a realização dos testes.

Foi definido que o Cenário 1 seria composto por sete máquinas virtuais que simulam:

- Roteador da operadora;
- Servidor gateway das redes administrativa e acadêmica;
- Servidor de firewall da rede acadêmica;
- Servidor de firewall da rede administrativa;
- Rede administrativa;
- Rede acadêmica;
- Servidores do Portal.

A infraestrutura de máquinas virtuais criadas no Cenário 1 reflete o cenário implantado na instituição. Para configurar os serviços e as interfaces de rede dos servidores de firewall, proxy e gateway das redes administrativa e acadêmica foram inseridos os arquivos de configuração importados dos servidores do ambiente real.

Após a criação do Cenário 1, foi possível iniciar a fase de testes, para verificar o comportamento da rede atual.

Primeiro, definiu-se que os parâmetros obtidos e avaliados durante os testes seriam:

- Taxa de transferência (*Throughput*) das redes administrativa, acadêmica e portal simultaneamente: esse parâmetro é utilizado verificar a vazão dos dados em um canal de comunicação. Os valores desse parâmetro foram obtidos a partir da analise dos resultados dos testes do Iperf;
- Latência na conexão das redes administrativa, acadêmica e portal simultaneamente: esse parâmetro foi obtido através do envio de pacotes de ICMP (ping);
- Variação do atraso (*Jitter*) das redes administrativa, acadêmica e portal simultaneamente: esse parâmetro é utilizado para verificar a oscilação entre o tempo de entrega dos pacotes. Essa oscilação pode acarretar o

recebimento fora da ordem dos pacotes enviados pelo emissor ao receptor;

- Perda de pacotes.

Para realizar a coleta dos dados os testes foram realizados da seguinte forma:

- O Iperf é inicializado em modo servidor na máquina virtual que simula o roteador da operadora.
- Em seguida o Iperf é inicializado em modo cliente nas máquinas virtuais que simulam as redes: administrativa, acadêmica e portal.
- Em paralelo com a simulação de tráfego foi realizado as requisições de ICMP para obter informações de perda de pacotes, latência e variação de atraso.

Após a realização de testes sobre o Cenário 1, os dados coletados foram armazenados para realizar analise nos resultados finais do trabalho.

A etapa seguinte constituiu na criação e configuração do Cenário 2, que é um clone do Cenário 1, acrescido das ferramentas de gerência e QoS. As regras e configurações de QoS foram definidas a partir do mapeamento do tráfego de rede do CEULP/ULBRA. Após a construção e configuração do Cenário 2, foram repetidos os testes realizados sobre o Cenário 1.

O Cenário 2 foi construído e configurado com o intuito de representar o ambiente proposto para o CEULP/ULBRA, onde as alterações realizadas no ambiente virtual são propostas e sugeridas para ambiente de rede real do CEULP/ULBRA.

Após a criação dos cenários e a captura dos dados, foi feita uma comparação do comportamento dos dois ambientes. Essa comparação foi realiza a partir dos resultados obtidos nos testes sobre os dois cenários, na qual foi feita uma análise das informações e foi elaborada uma tabela comparativa dos resultados.

O resultado deste trabalho é o Cenário 2, que é o ambiente proposto para o CEULP/ULBRA, e a comparação com o ambiente atual para sugerir melhorias para a rede do CEULP. A partir do cenário proposto e das informações apresentadas nos resultados desse projeto, o administrador da rede pode decidir por implantar ou não.

O funcionamento da ferramenta de gerência, as regras de QoS criadas bem como a comparação do comportamento da rede com e sem o uso de gerência de redes e QoS são apresentados na seção seguinte.

4 RESULTADOS E DISCUSSÃO

Esse trabalho foi realizado com objetivo de criar um ambiente virtual que simule a estrutura atual da rede do CEULP/ULBRA, estudar e conhecer essa estrutura, descobrir os pontos negativos e principais problemas, visando propor melhorias que acabem ou amenizem esses problemas, usando ferramenta de gerência de redes e QoS. A proposta de melhoria consiste em apresentar um ambiente virtual que simule a estrutura de rede atual e apresentar o comportamento do tráfego de internet do CEULP/ULBRA após a implantação da ferramenta de gerência e QoS.

Nos ambientes virtuais criados foram realizados testes que avaliam o comportamento da rede que representa o cenário atual, Cenário 1, e o comportamento da rede proposta com uso da ferramenta de gerência e QoS, Cenário 2. A seguir é apresentada uma breve descrição dos cenários criados para a realização desse trabalho:

- **Cenário 1**: é composto por 7 máquinas virtuais criadas para reproduzir o cenário do ambiente real. Nessas máquinas virtuais foram instalados os softwares em produção no ambiente real, acrescentando as ferramentas de coleta de informações do proxy e a ferramenta de simulação de tráfego;

- **Cenário 2**: foi criado a partir do Cenário 1, utilizando a clonagem de máquinas virtuais. Após a clonagem foi instalada e configurada a ferramenta de gerência e as regras de QoS. Nesse ambiente, as configurações foram ajustadas até chegar no ambiente proposto, que é o Cenário 2 apresentado nesse trabalho.

Desta forma, esta seção é direcionada para a apresentação dos dois ambientes virtuais criados (Cenário1 e 2), as configurações realizadas sobre cada um deles, dos resultados dos testes sobre cada cenário e de um comparativo entre os dois cenários:

4.1. Cenário 1

A partir das entrevistas realizadas foi constatado que o CEULP/ULBRA possui aproximadamente 850 *hosts* que estão distribuídos da seguinte forma:

- **Rede acadêmica**: é composta por 290 *desktops,* distribuídos nas salas do complexo de informática, configurados com IPs estáticos. Esses equipamentos ficam disponíveis para os alunos realizarem pesquisas e acessar a internet. Além dos 290 *desktops* dos laboratórios acadêmicos, a rede acadêmica possui aproximadamente 230 notebooks de alunos cadastrados na coordenação dos labins, sendo que esses equipamentos não conectam simultaneamente à internet.
- **Rede administrativa**: é composta por aproximadamente 130 computadores configurados com IPs estáticos. Esses equipamentos ficam ligados e conectados á internet e aos sistemas administrativos durante boa parte do dia e o acesso á esses equipamentos é realizado apenas por funcionários da instituição;
- **Rede do portal**: é constituída por cinco servidores com serviços e páginas publicadas na internet. Alguns servidores do portal estão configurados com IP da rede WAN do CEULP/ULBRA, e os outros estão configurados com IP da rede local do portal. O acesso físico aos equipamentos da rede do portal é restrito aos funcionários do portal. O acesso ás páginas publicadas é realizado pelos docentes, discentes e comunidade geral;
- **Servidores de gateway e firewall das Redes Acadêmica e Administrativa:** são os gateways das redes administrativa e acadêmica. Esses servidores são responsáveis por prover o acesso á internet para as redes administrativa e acadêmica. Nesses servidores estão configuradas as regras de bloqueio e liberação de páginas que os alunos e servidores podem acessar e os serviços de firewall da rede corporativa da instituição.

Como o Cenário 1 foi construído para representar a rede LAN atual do CEULP/ULBRA, as máquinas virtuais foram criadas para simular as três redes e os servidores de firewall e gateway. A Figura 9 apresenta o Cenário 1, que possui 7 máquinas virtuais (VM).

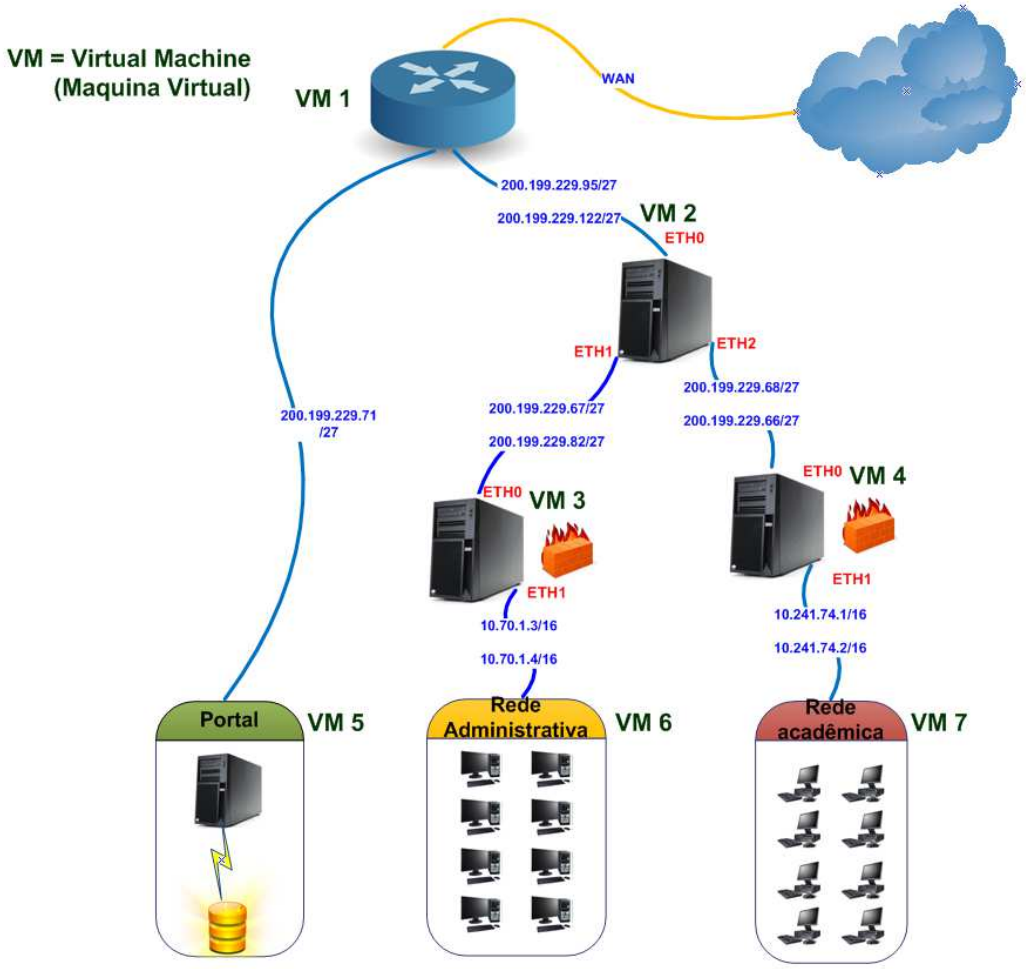

Figura 9: Cenário 1

Como pode ser observado na Figura 9, o Cenário 1 é composto por 7 máquinas virtuais:

- VM1 – simula o roteador da operadora;
- VM2 – simula o servidor de gateway do firewall acadêmico e administrativo;
- VM3 – simula o firewall administrativo;
- VM4 – simula o firewall acadêmico;
- VM5 – simula a rede do portal;
- VM6 – simula a rede administrativa;
- VM7 – simula a rede acadêmica.

Os *softwares* relevantes e os serviços inicializados nas máquinas foram definidos a partir dos estudos e das entrevistas realizadas para conhecer a topologia de rede da instituição. Os *softwares* instalados em cada umas das máquinas foram:

- VM1 – SNMP, SNMPD, Iperf;
- VM2 – SNMP, SNMPD, Iperf, Iftop;
- VM3 – SNMP, SNMPD, Squid 3, IPTABLES, Iperf, SqStat, SARG, Iftop;
- VM4 – SNMP, SNMPD, Squid 3, IPTABLES, Iperf, SqStat, SARG, Iftop;
- VM5 – SNMP, SQL Server, Iperf;
- VM6 – SNMP, Iperf;
- VM7 – SNMP, SNMPD, Iperf;.

A descrição de cada uma das máquinas virtuais, o que esta representa dentro do Cenário 1 e as ferramentas instaladas é apresentada a seguir.

A rede acadêmica, que é constituída por aproximadamente 520 equipamentos, é simulada na máquina virtual 7, com o sistema operacional Linux. Nessa máquina foi instalada a versão 6.0 do Debian, conforme ilustrado Figura 10.

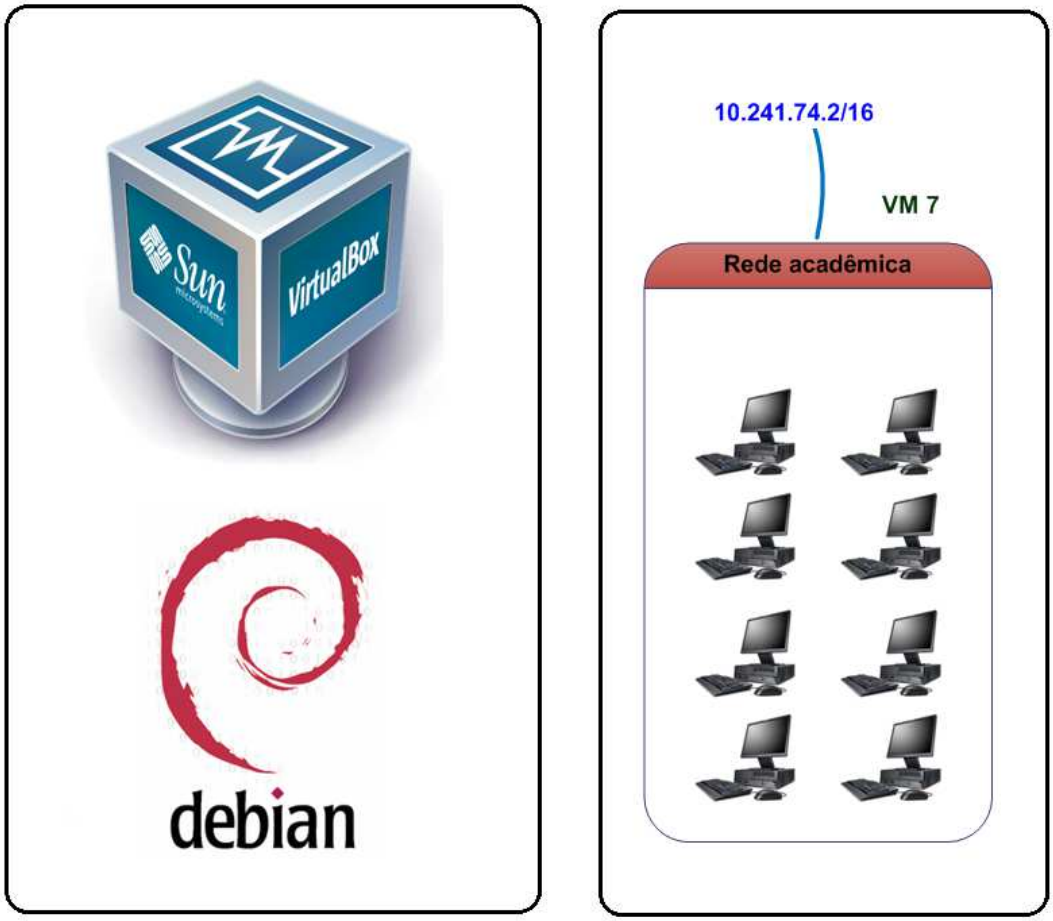

Figura 10: VM7 – Simulação da Rede Acadêmica

Foi instalado na máquina virtual 7 a versão básica do Linux e os pacotes do SNMP e SNMPD para permitir a coleta de informações de MIB da máquina e o pacote do Iperf, utilizado para testar e simular a largura de banda e simular tráfego da rede. A interface de rede foi configurada com o IP 10.241.74.2, máscara de rede 255.255.0.0 e gateway 10.241.74.1 como são ilustrados na Figura 10.

Para simular a rede administrativa, que é composta por aproximadamente 130 computadores, foi criada a máquina virtual 6, que possui a versão *professional* do Windows XP de 32 bits, conforme ilustrado na Figura 11.

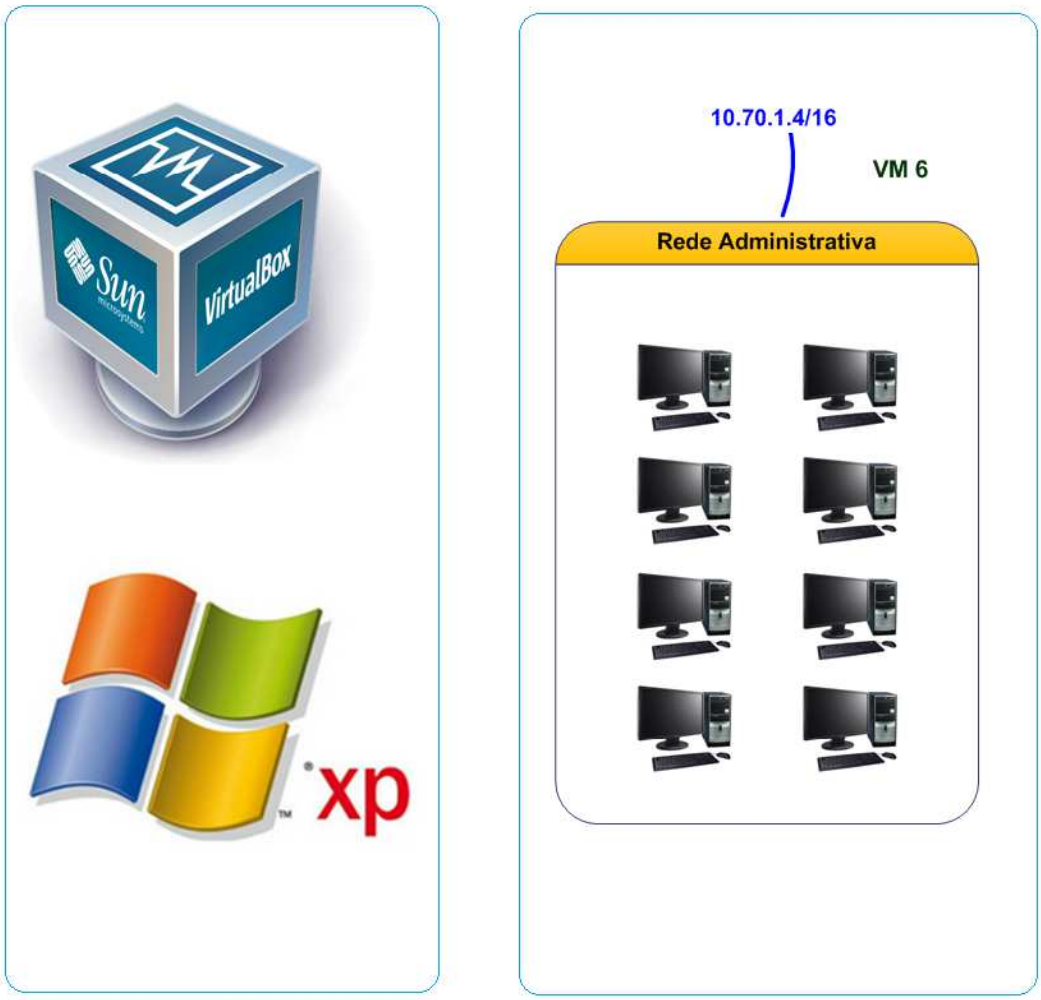

Figura 11: Simulação da rede administrativa

Na máquina virtual 6 o serviço de SNMP foi instalado e configurado para inicializar automaticamente. Juntamente com o serviço de SNMP, foi instalado o programa Iperf para simular o tráfego da rede. A interface de rede foi configurada com o IP 10.70.1.4, máscara de rede 255.255.0.0 e gateway 10.70.1.3 como é ilustrado na Figura 11.

Para realizar a simulação da rede do portal, que é composta por 5 servidores com serviços e páginas publicadas na internet, foi criada a máquina virtual 5. Nela foi instalado o sistema Operacional *Windows Server* 2008 *Enterprise Edition*, como mostra a Figura 12.

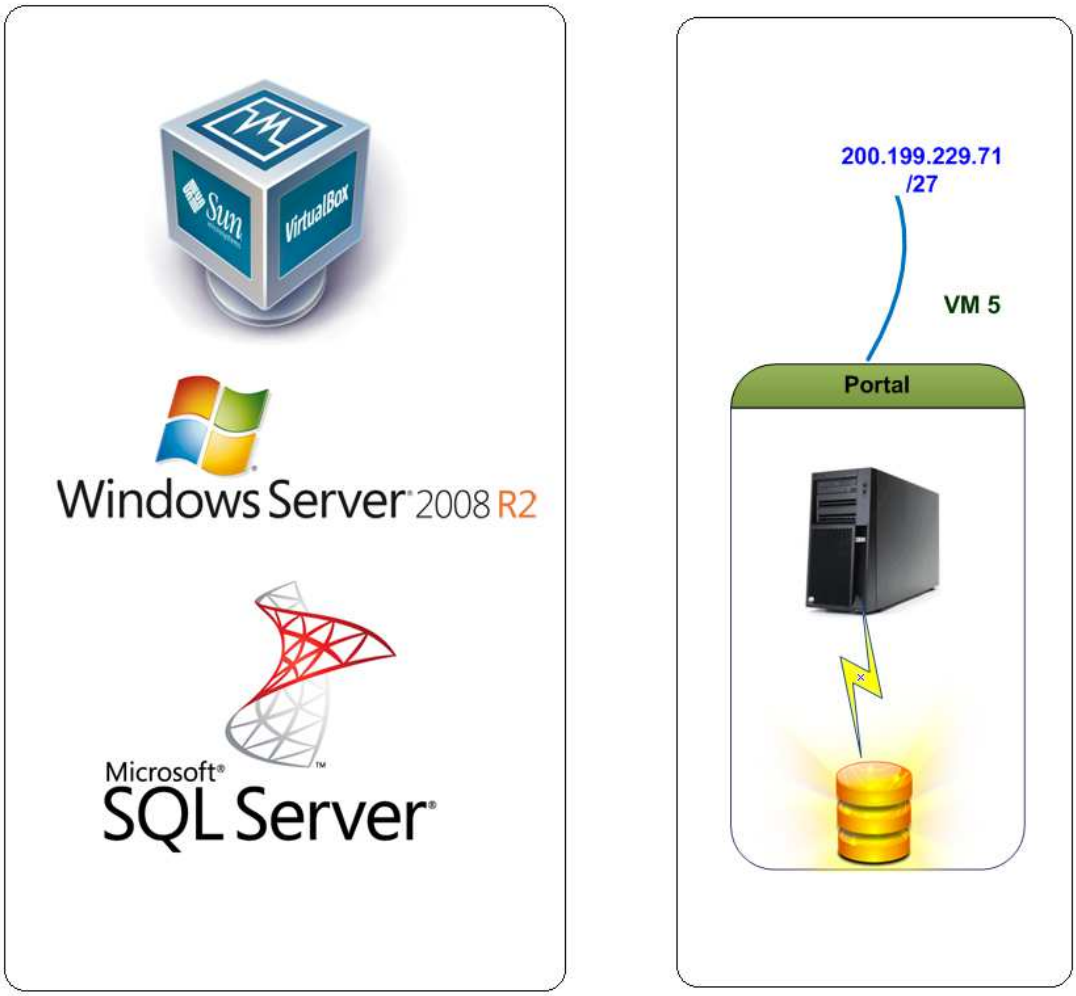

Figura 12: Simulação da rede do portal

Nessa máquina virtual foi instalado e configurado o SQL *Server Enterprise Edition* e o Iperf para realizar a simulação do tráfego de rede do portal. A interface de rede foi configurada com o IP 200.199.229.71, máscara de rede 255.255.255.192 e gateway IP 200.199.229.65 como é ilustrado na Figura 12Figura 10.

O portal do CEULP/ULBRA oferece uma grande quantidade de conteúdo, entre páginas e aplicações, para a comunidade acadêmica e a comunidade externa. O acesso diário às páginas do portal somam aproximadamente 3.200 visitas, sendo que esse número chega á 7.300 nos dias que antecedem a entrega das atividades semipresenciais da intranet.

O tráfego do portal tem um volume aproximado de 280GB mensais, sendo que esse volume é construído por tráfego dos protocolos HTTP e HTTPS. Do valor global de 280GB, o tráfego de saída (upload) é composto por aproximadamente

260GB de informações e 20GB de entrada (download). Esse tráfego é simulado pelo Iperf.

A rede acadêmica simulada da máquina virtual 7, utiliza um servidor, que se localiza no CPD, como gateway. Esse servidor é simulado na máquina virtual 4 com o sistema operacional Linux, utilizando a versão 6.0 do Debian, ilustrada na Figura 13.

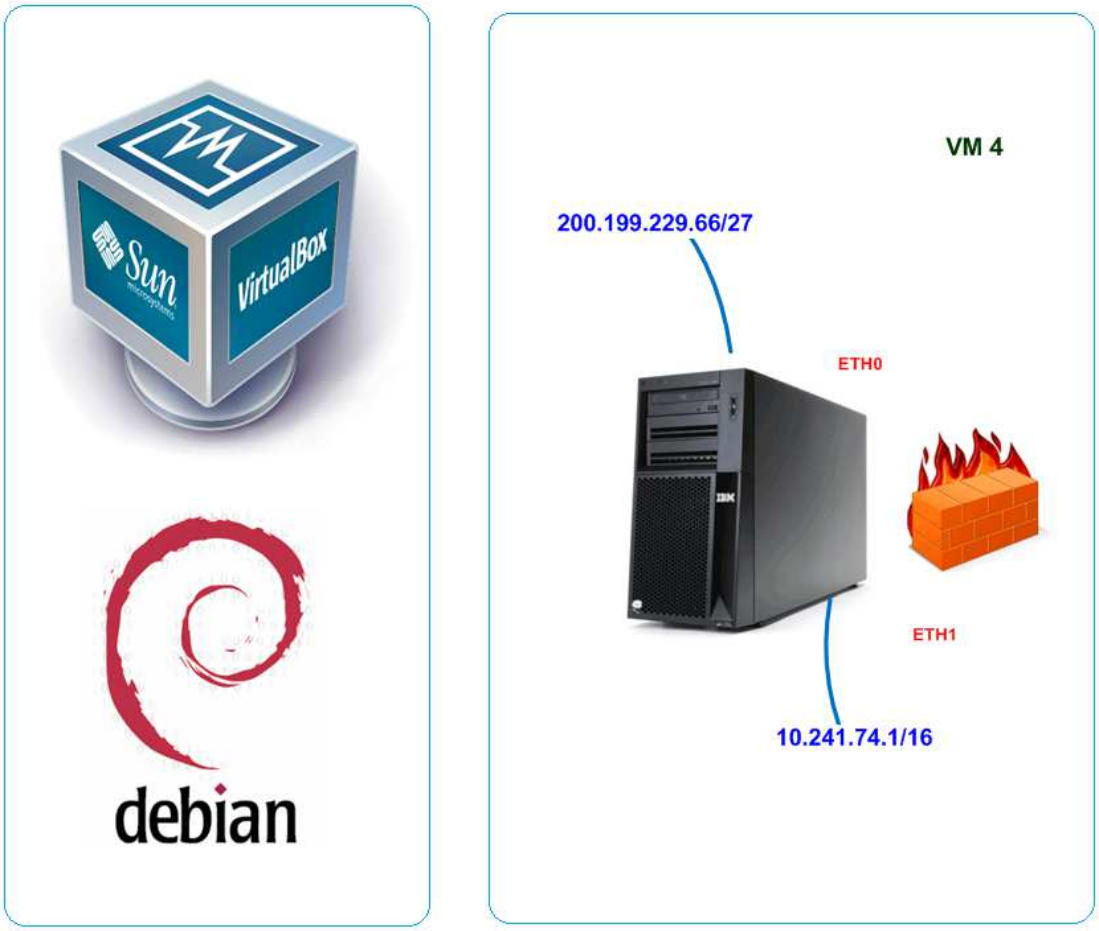

Figura 13: Simulação do servidor de firewall da rede acadêmica

. Na máquina virtual 4 foram instalados os pacotes do SNMP e SNMPD, para fazer a coleta de informações de MIB da máquina e os leitores de *logs* do Squid, SARG e SqStat, utilizados para coletar e analisar as requisições dos hosts que utilizam esse servidor como *gateway*. No servidor, foram configuradas as regras de *firewall,* IPTABLES, e as regras de Proxy, Squid, da rede acadêmica. Como mostra Figura 13, esse servidor possui duas interfaces de rede que estão configuradas para

o acesso à rede local e acesso externo. A interface ETH0 foi configurada com o IP 200.199.229.66, máscara de rede 255.255.255.192 e gateway 200.199.229.68. A interface ETH1 foi configurada com o IP 10.241.74.1 e máscara de rede 255.255.0.0.

A rede administrativa também utiliza um servidor localizado no CPD como gateway. Esse servidor, simulado na máquina virtual 3, tem como sistema operacional a versão 6.0 do Debian, como é ilustrado da Figura 14.

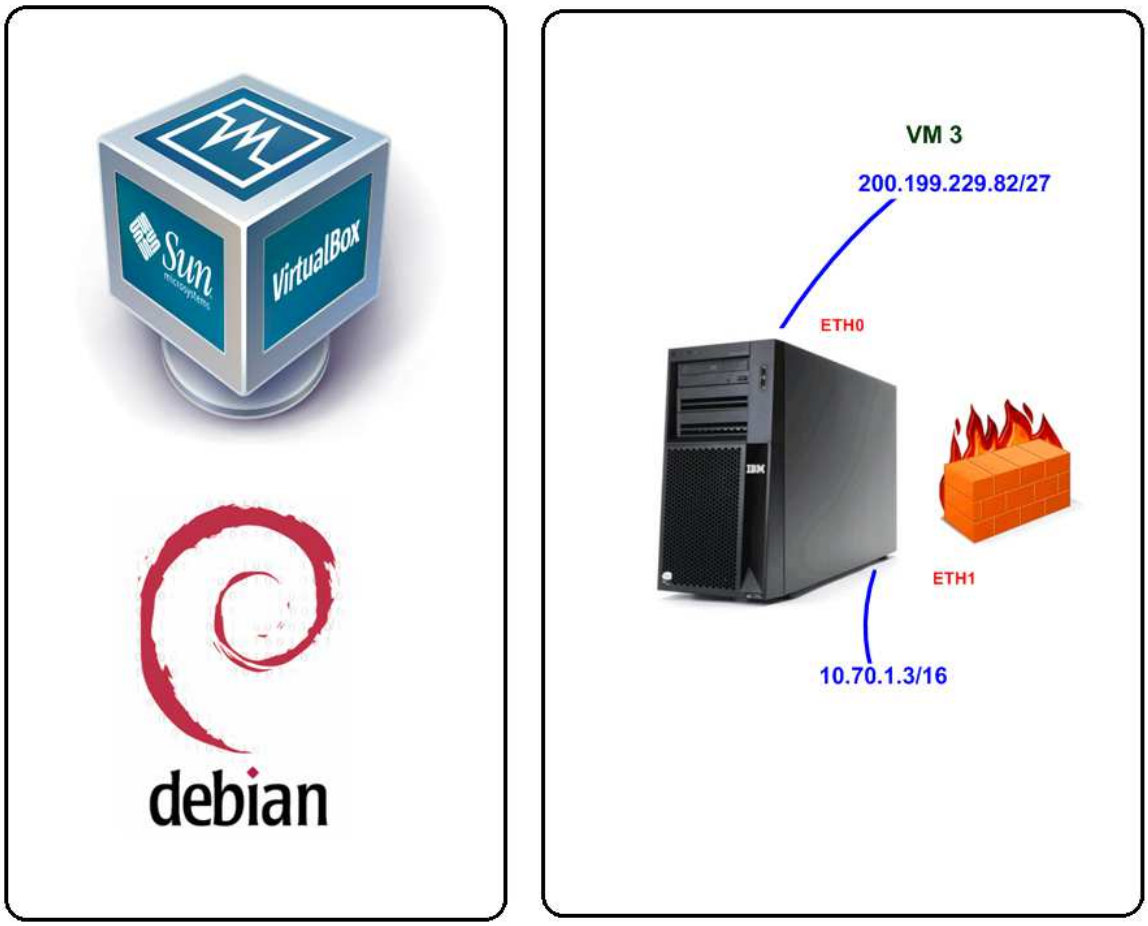

Figura 14: Simulação do servidor de firewall da rede administrativa

Na máquina virtual 3 foram instalados os pacotes do SNMP e SNMPD, para permitir a coleta de informações de MIB da máquina, e os leitores de *logs* do Squid, SARG e SqStat, utilizados para coletar e analisar as requisições dos hosts que utilizam esse servidor como gateway. No servidor foram configuradas as regras de firewall utilizando IPTABLES e as regras de proxy da rede administrativa. Como mostra Figura 14, esse servidor possui duas interfaces de rede que estão configuradas para o acesso à rede local e externo. A interface ETH0 utilizada para acesso externo foi configurada com o IP 200.199.229.82, máscara de rede

255.255.255.192 e gateway 200.199.229.67. A interface ETH1 utilizada para acesso local foi configurada com o IP 10.70.1.3 e máscara de rede 255.255.0.0.

Os firewalls das redes administrativa e acadêmica possuem como gateway de suas redes um servidor Debian, versão 6.0.1, simulado através da máquina virtual 2. No ambiente simulado, esse host está configurado com três interfaces de rede, como mostra a Figura 15.

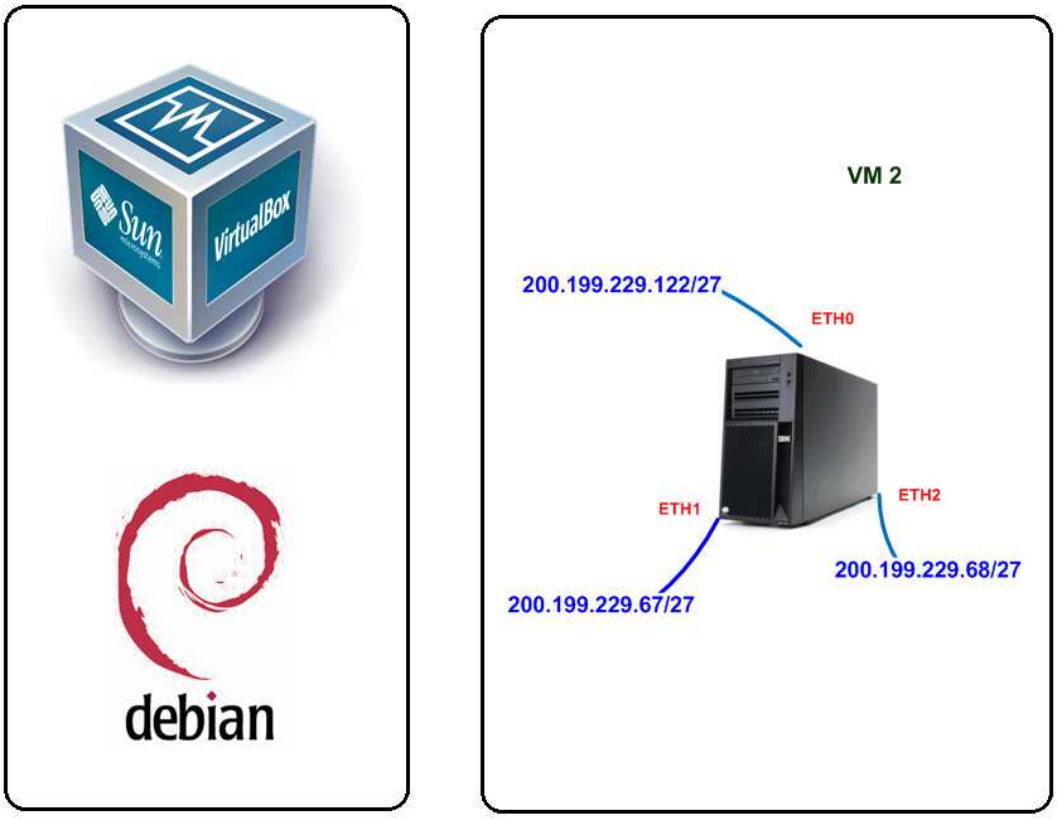

Figura 15: Simulação do gateway das redes acadêmica e administrativa

Nesse servidor a ETH0 foi configurada com o IP 200.199.229.122, máscara de rede 255.255.255.192 e *gateway* 200.199.229.95. A interface ETH1 foi configurada com o IP 200.199.229.67 máscara de rede 255.255.255.192 e é utilizada como gateway do servidor de firewall administrativo. Na interface ETH2 foi configurado o IP 200.199.229.68, máscara de rede 255.255.255.192 e é utilizado como servidor de gateway do servidor de firewall da rede acadêmica. As interfaces ETH1 e ETH2 utilizam a interface ETH0 como *default gateway*.

Para realizar a simulação do roteador da operadora, que disponibiliza o acesso à internet, foi criada a máquina virtual 1, que utiliza a distribuição Linux com a versão 6.0 do Debian, como é apresentado na Figura 16. Nessa máquina virtual foram instalados os pacotes do SNMP e SNMPD, para permitir a coleta de informações de MIB da máquina, e o pacote do Iperf, utilizado para testar e simular a largura de banda e simular tráfego na rede.

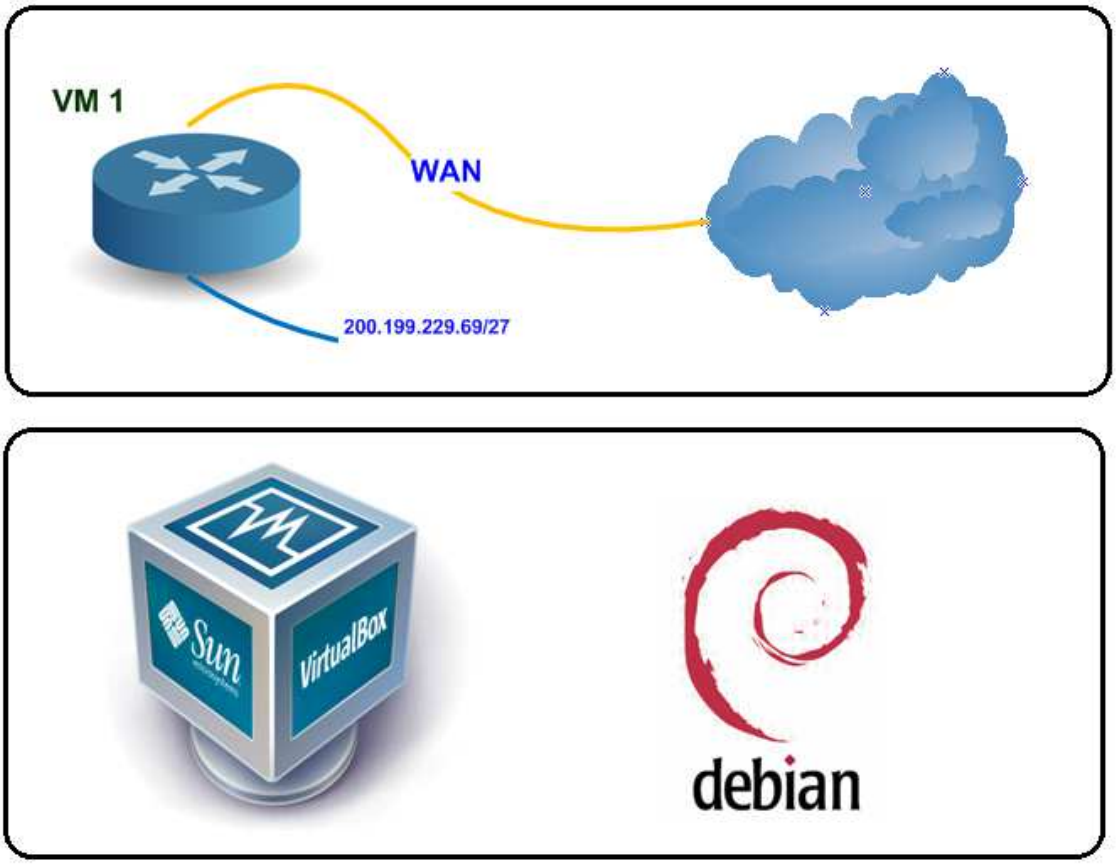

Figura 16: Simulação do roteador da operadora

Após a finalização da etapa de criação e configuração do Cenário 1, foram inicializados os testes, descritos nas subseções seguintes.

4.1.1. Testes sobre o Cenário 1

Após a finalização da etapa de criação do Cenário 1, foram realizados os seguintes testes:

- Teste 1: ICMP, utilizando para obter os resultados de latência, jitter e perda de pacotes;

- Teste 2: largura de banda, utilizado para realizar a aferir a vazão de dados em um canal de comunicação.

O resultado dos testes de ICMP apresentou a latência, o jitter e a perda de pacotes no canal de comunicação. Para a realização desse teste as 7 máquinas virtuais que compõem o Cenário 1 estavam ligadas. O teste consistiu em disparar *ping* das VMs 5, 6 e 7 com destino á VM 1, com duração de 1 hora (3600 segundos).

Para realizar o teste nas máquinas 5 e 6 que utilizam o sistema operacional *Windows*, foi necessário abrir o terminal e digitar o comando “ping 200.199.229.95 –n 3600”. Na máquina virtual 7 que utiliza o sistema operacional Linux a sintaxe do comando é: “ping 200.199.229.95 –w 3600”. A execução desse comando realiza o teste de ping durante o período de 1 hora. O resultado do teste é apresentado na Figura 17.

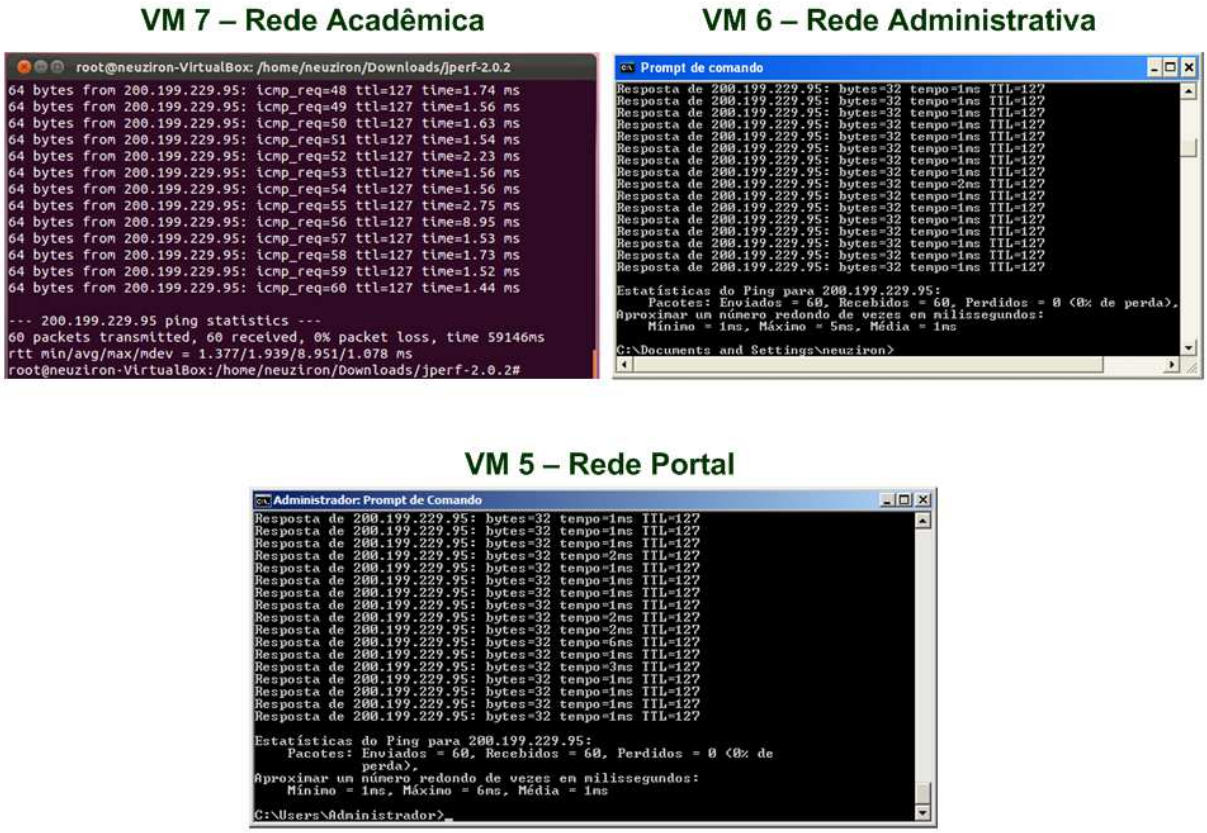

Figura 17: Resultados dos testes de ICMP no Cenário 1

Conforme pode ser observado na Figura 17, os resultados da latência e da perda de pacotes são apresentados nas telas dos terminais. O Jitter é calculado a

partir da soma das diferenças entre os pacotes, onde o resultado é dividido pela quantidade de pacotes recebidos. Os resultados do teste de ICMP são apresentados na **Tabela 5**.

Após a execução do teste de ICMP foi realizado o teste de largura de banda. Esse teste consistiu em realizar download de maneira simultânea das VMs 5, 6 e 7 por um período de 1 hora. A Figura 18 apresenta os resultados na interface gráfica do *software* Iperf, utilizado para realizar a simulação do tráfego. Os resultados dos testes são apresentados na **Tabela 5**.

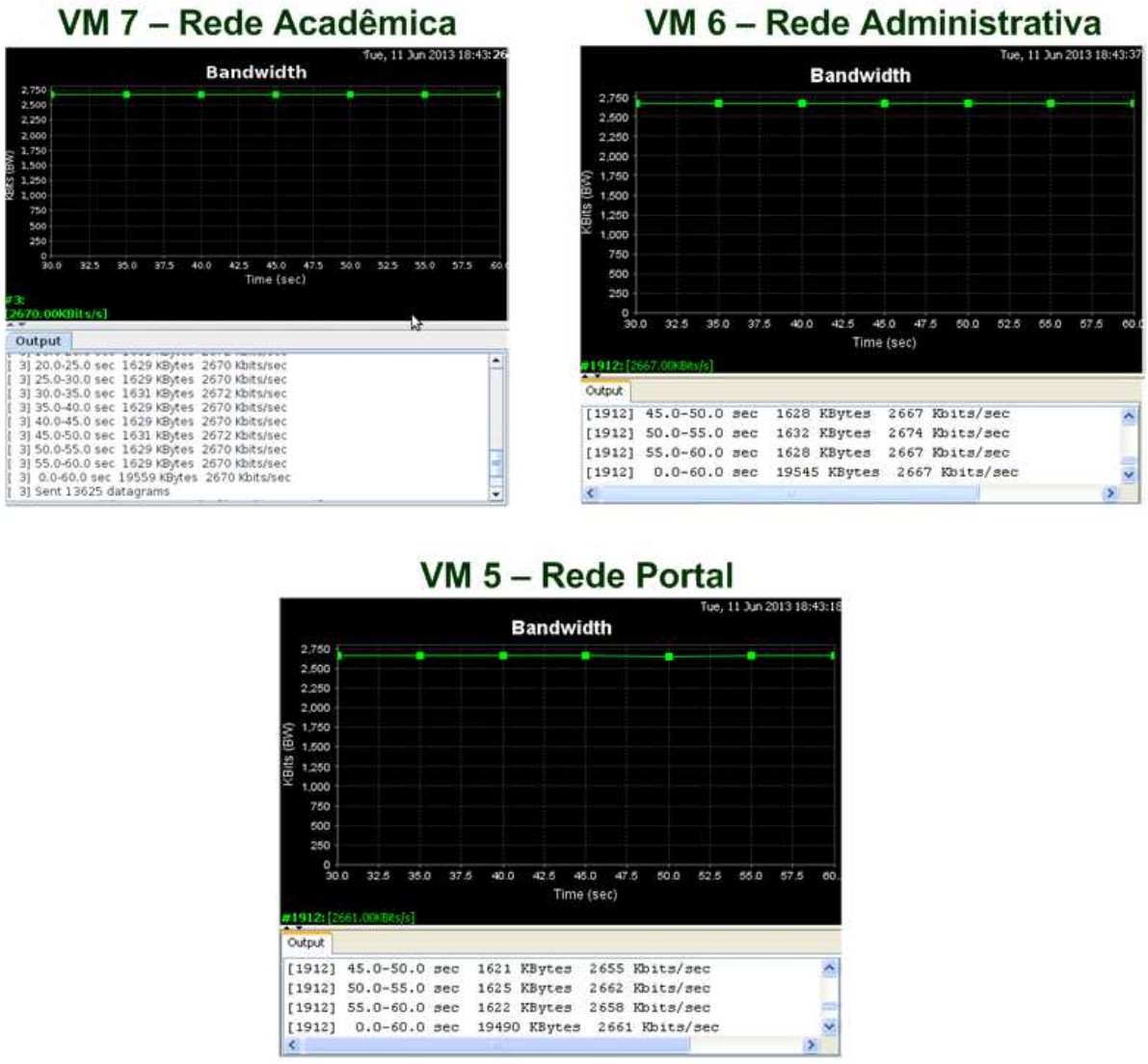

Figura 18: Resultados dos testes de largura de banda no Cenário 1

O teste de largura de banda sobre o Cenário 1 foi aplicado de maneira simultânea nas redes administrativa, acadêmica e portal, simulando a concorrência

pelos insumos de acesso a internet. Os downloads tiveram como destino a VM 1, que foi configurada para ser o servidor de *download*. Para operar como servidor, o Iperf foi inicializado na VM 1 com o parâmetro “Iperf -s”. Dessa forma, a aplicação está configurada para receber as conexões.

Nas VM 5, 6 e 7 a aplicação foi inicializada em modo cliente. Para inicializar a aplicação em modo cliente a sintaxe utilizada foi “iperf -c 200.199.229.95 –t 3600”, o parâmetro -t configura o Iperf para executar o teste por um período de 1 hora (3600 segundos).

Os testes citados foram realizados diversas vezes e não houve alterações significantes nos resultados. Os valores obtidos nos testes de ICMP e largura de banda são apresentados na **Tabela 5**.

Tabela 5: Resultados dos testes realizados no Cenário 1

CENÁRIO 1		
Máquina Virtual	**Parâmetros**	**Resultados**
VM 1 Roteador	Largura de Banda	8 Mbps
VM 5 Rede Portal	Largura de Banda	≅ 2,67 Mbps
	Latência	≅ 1ms
	Jitter	≅ 0ms
	Perda de Pacotes	0
VM 6 Rede Administrativa	Largura de Banda	≅ 2,67 Mbps
	Latência	≅ 1ms
	Jitter	≅ 0ms
	Perda de Pacotes	0
VM 7 Rede Acadêmica	Largura de Banda	≅ 2,67 Mbps
	Latência	1.939ms
	Jitter	≅ 0ms
	Perda de Pacotes	0

Como pode-se observar na **Tabela 5**, a VM 1 possui uma largura de banda de 8Mbps, que é igualmente distribuído entre as VMs 5, 6 e 7 quando os *downloads* são realizados simultaneamente. Dessa maneira, não existe uma largura de banda garantida para determinadas redes e serviços da instituição. A latência das Vms 5 e 6 tiveram valores aproximados de 1ms(milissegundos), esse valor foi de 1.939ms na VM 7.

Como se trata de um ambiente virtual, no qual as conexões de rede também são virtuais, a entrega dos pacotes é feita de maneira rápida, como pode ser visto no tempo da latência. Devido essa fácil e próxima entrega dos pacotes, a perda desses é 0 nas 3 máquinas virtuais. O mesmo ocorre com o jitter que é a variação da latência, em que o valor é bem próximo a 0 nas VMs 5, 6 e 7.

Após a finalização da etapa de testes sobre o Cenário 1, foi inicializada a construção e configuração do Cenário 2. A criação e configuração do Cenário 2, é apresentada na próxima seção.

4.2. Cenário 2

O Cenário 2 foi construído para representar a rede LAN proposta para o CEULP/ULBRA. As máquinas virtuais do Cenário 2 foram clonadas do Cenário 1 e, após a clonagem, foram acrescentadas a ferramenta de gerência de redes e as regras de QoS, como mostra a Figura 19.

Depois de construído o ambiente foi testado e alterado diversas vezes até chegar ao ambiente apresentado. O ambiente apresentado no Cenário 2 é a proposta a ser implantada no CEULP/ULBRA.

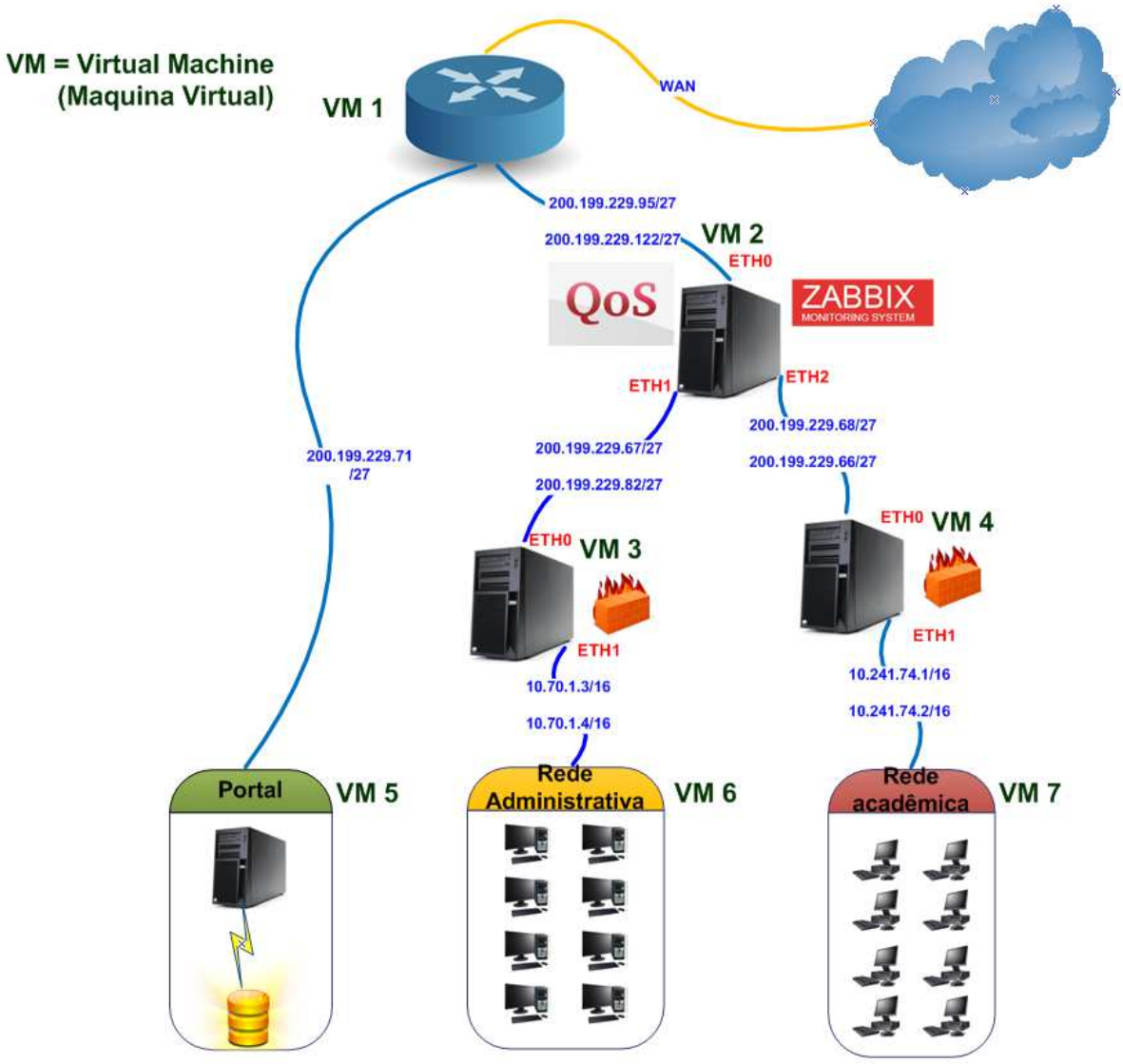

Figura 19: Cenário 2

O Cenário 2, ilustrado na Figura 19, mostra que a ferramenta de gerência de redes, Zabbix, foi instalada na VM 2 e que nessa mesma máquina virtual foram configuradas as regras de QoS.

Como é mostrado da Figura 20 a VM 2 possui o IP 200.199.229.122 configurado na interface ETH0. O acesso à gerência WEB do Zabbix é realizada por meio da URL: http://200.199.229.122/zabbix.

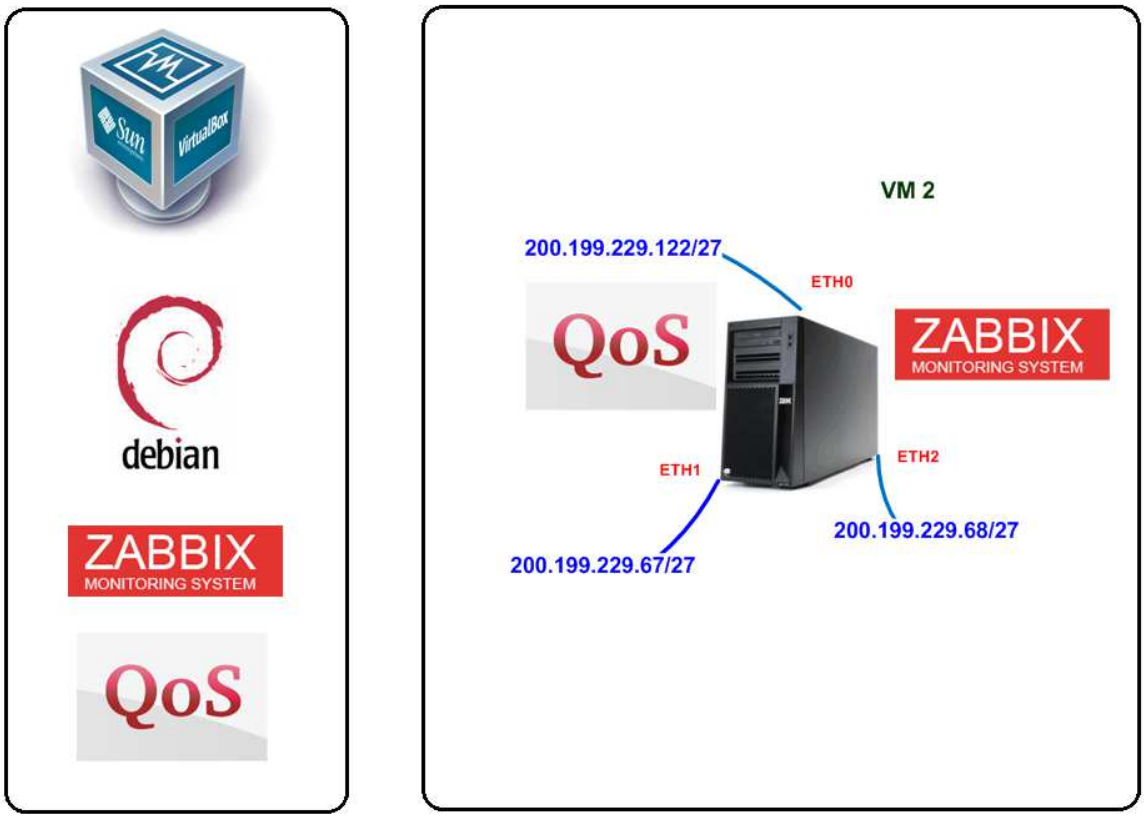

Figura 20: Simulação do gateway das redes acadêmica e administrativa no Cenário 2

Após a instalação e configuração do Zabbix para coletar informações de MIB das VMs, foi criada uma tela para exibição do tráfego de rede das VMs, chamada de “Trafego TCC Todos os Hosts”. Essa tela possibilita a visualização do consumo de tráfego WAN de todos os dispositivos cadastrados, e é apresentada na Figura 21.

Figura 21: Coleta do Tráfego WAN de todas as VMS

A tela apresentada na Figura 20 possibilita a visualização do consumo de tráfego WAN de todos os dispositivos cadastrados. A imagem mostra que no momento da captura os insumos de internet não estavam sendo utilizados.

Além da tela que permite visualizar todas as VMs, foi criada uma segunda tela que mostra o tráfego apenas das VMs 1, 5, 6 e 7 que simulam, respectivamente, o roteador da operadora, rede do portal, rede administrativa e rede acadêmica. Após a instalação e configuração do Zabbix e configuração da coleta de informações via SNMP das VMs, foi inicializada a configuração das regras de QoS.

A partir da coleta de informações do relatório mensal do SARG no ambiente real do CEULP/ULBRA e entrevistas realizadas, foi calculado que no mês maio a rede acadêmica consumiu aproximadamente 62,5% do valor global, a rede administrativa consumiu aproximadamente 25% e o portal 12,5%. Através desse levantamento, foi definido que nesse projeto seria criado apenas regras para controle e priorização do tráfego de download.

No ambiente real o link de dados do CEULP/ULBRA possui 8 Mbps (megabits). No QoS as regras são configuradas utilizando a unidade de medida Kilobits (Kbps). Para realizar a conversão de Mbps para Kbps é necessário multiplicar a quantidade de Mbps por 1024, onde o resultado mostra que a largura de total da banda do CEULP/ULBRA é de 8192 Kbps.

Como apresenta o *script* de configuração da Figura 22, as regras de QoS foram aplicadas para na interface ETH0 da VM 2, que é a interface utilizada como *default gateway* da máquina virtual. No *script* é definido a criação das classes, a largura de banda para cada subclasse e as filas de prioridade.

```
1  # POLITICA DE DOWNLOAD (eth0)
2
3  tc qdisc del dev eth0 root
4
5  tc qdisc add dev eth0 handle 1:0 root htb
6
7  tc class add dev eth0 parent 1:0 classid 1:1 htb rate 7168kbps
8
9  tc class add dev eth0 parent 1:1 classid 1:2 htb rate 5120kbps ceil 7168kbps
10 tc class add dev eth0 parent 1:1 classid 1:3 htb rate 2048kbps ceil 7168kbps
11
12 tc qdisc add dev eth0 parent 1:2 handle 30:0 pfifo limit 10
13 tc qdisc add dev eth0 parent 1:3 handle 40:0 pfifo limit 10
14
15 tc filter add dev eth0 parent 1:0 protocol ip u32 match ip dst 200.199.229.66/32 flowid 1:2
16 tc filter add dev eth0 parent 1:0 protocol ip u32 match ip dst 200.199.229.82/32 flowid 1:3
17
18
```

Figura 22: Arquivo de configuração das regras de QoS

Como é apresentado, na linha 3 da Figura 22, é realizado a exclusão das regras existentes para a interface ETH0. Na linha 5 é adicionado a regra 1:0 para a interface ETH0 utilizando o HTB como algoritmo de ordenação e priorização de filas para garantir a qualidade nos serviços que serão definidos como prioritários. Na linha 7 é adicionado a “classeid” 1:1 que herda da regra 1:0. Nessa classe é definida a banda destinada para as redes administrativa e acadêmica em 7168Kbps.

Na linha 9 é adicionado a “classeid” 1:2 que herda da classe 1:1. Nessa regra é definida a banda destinada para a acadêmica em 5120Kbps. Na linha seguinte é adicionado a “classeid” 1:3 que também herda da classe 1:1. Nessa regra é definida a banda destinada para a administrativa em 2048Kbps. Nas classes 1:2 e 1:3 as taxas de transmissão podem alcançar taxa máxima de download de 7168Kb

A rede do portal representada pela VM 5 no Cenário 2 não utiliza o servidor de GW das redes administrativa e acadêmica. Por isso a reserva de banda de 1024Kbps é realizada de maneira automática ao limitar o tráfego máximo das redes administrativa e acadêmica em 7168Kbps, totalizando os 8192Kbps de largura de banda do roteador, simulado na VM 1.

Após a finalização da etapa de criação e configuração do Cenário 2, foram inicializados os testes. Os testes realizados no Cenário 2 e os resultados obtidos serão apresentados na seção abaixo.

4.2.1. Testes sobre o Cenário 2

Após a finalização da etapa de criação e configuração do Cenário 2, foram realizados os testes aplicados anteriormente no Cenário 1. Conforme pode ser observado na Figura 23, os resultados da latência e da perda de pacotes são apresentados nas telas dos terminais.

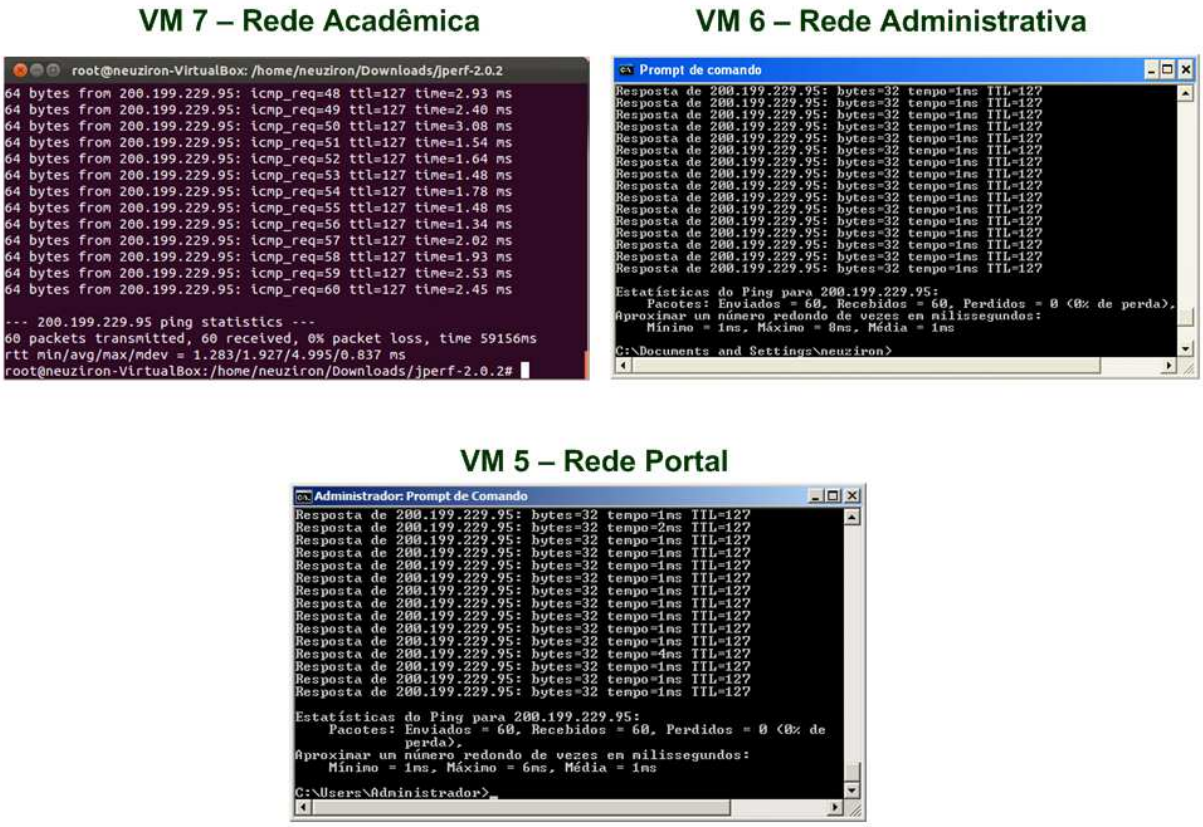

Figura 23: Resultados dos testes de ICMP no Cenário 2

O Jitter é calculado a partir da soma das diferenças entre os pacotes, onde o resultado é dividido pela quantidade de pacotes recebidos. Os resultados do teste de ICMP no Cenário 2 é apresentado na **Tabela 5**.

Após a execução do teste de ICMP foi realizado o teste de largura de banda. Esse teste consiste em realizar download de maneira simultânea das VMs 5, 6 e 7 por um período de 1 hora, como é apresentado na Figura 24.

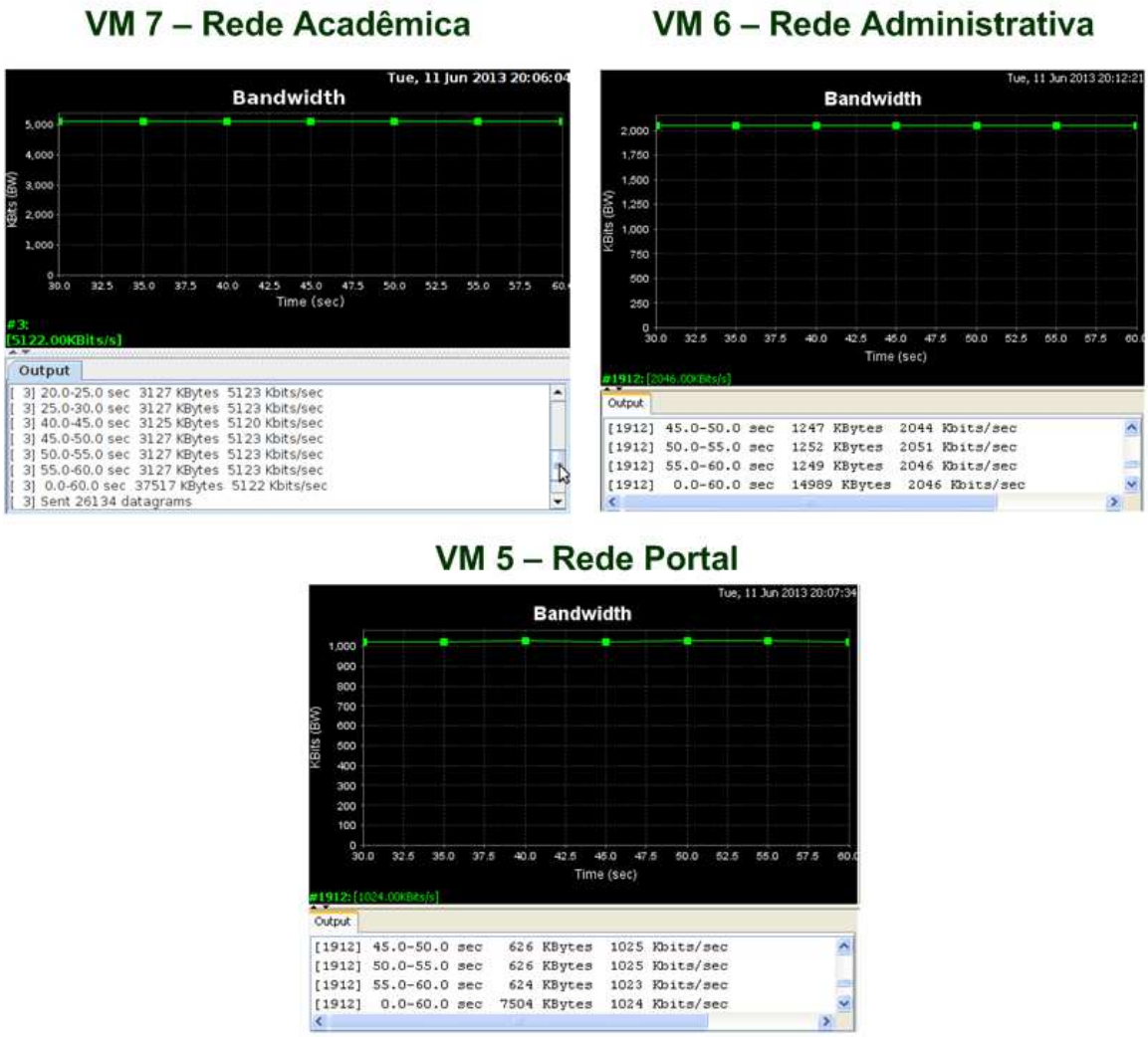

Figura 24: Resultados dos testes de largura de banda no Cenário 2

Assim como no Cenário 1, os downloads realizados simultaneamente pelas VMs 5, 6 e 7 tem como destino a VM 1 que foi configurada para ser o servidor de *download*. Os testes foram realizados diversas vezes e não houve alterações significantes nos resultados.

Os testes de *download* tiveram duração de 1 hora, onde o Zabbix realizou a captura do tráfego WAN das VMs 1, 5, 6 e 7. O gráfico gerado no Zabbix é apresentado na Figura 25.

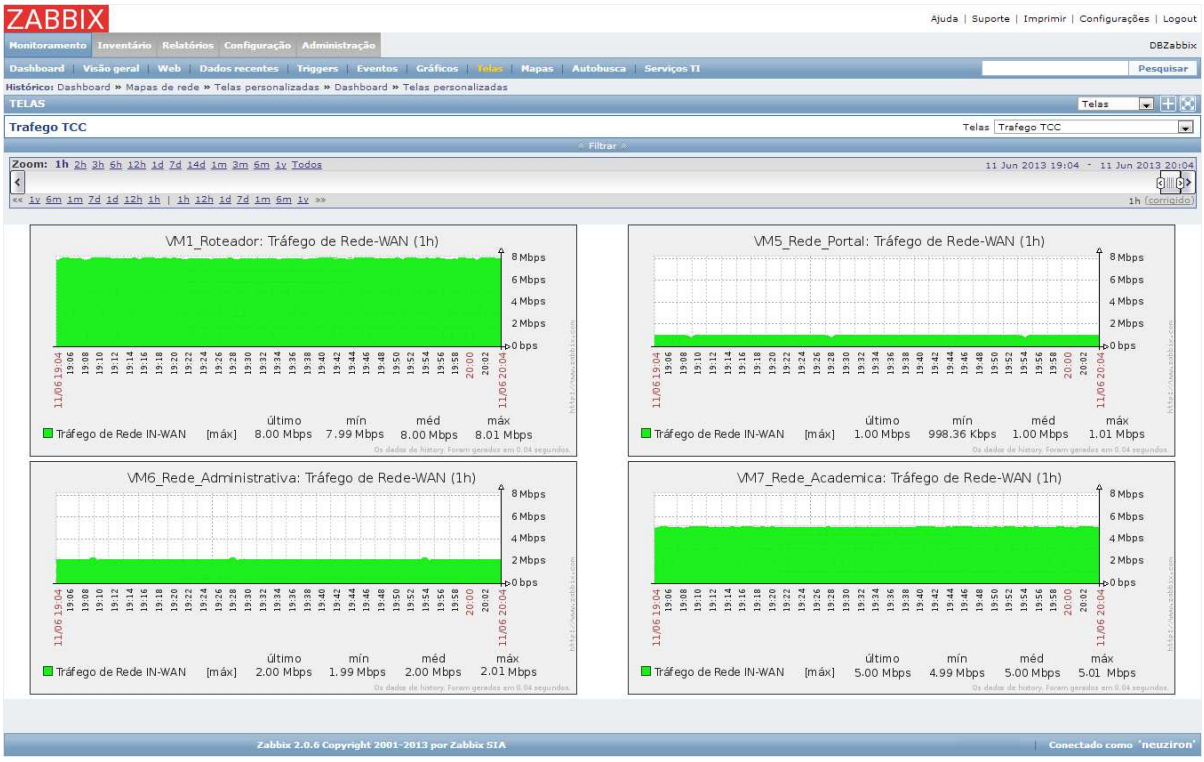

Figura 25: Tela de coleta de tráfego WAN no Zabbix

Como é apresentado na figura 25, as regras de QoS foram aplicadas e o tráfego das interfaces de rede foram monitoradas pelo Zabbix. Os valores obtidos nos testes de ICMP e largura de banda são apresentados na **Tabela 5**

Tabela 6: Resultados dos testes realizados no Cenário 2

CENÁRIO 2		
Máquina Virtual	**Parâmetros**	**Resultados**
VM 1 Roteador	Largura de Banda	8 Mbps
VM 5 Rede Portal	Largura de Banda	≅ 1 Mbps
	Latência	≅ 1ms
	Jitter	≅ 0ms
	Perda de Pacotes	0
VM 6 Rede Administrativa	Largura de Banda	≅ 2 Mbps
	Latência	≅ 1ms
	Jitter	≅ 0ms
	Perda de Pacotes	0
VM 7 Rede Acadêmica	Largura de Banda	≅ 5 Mbps
	Latência	1.927ms
	Jitter	≅ 0ms
	Perda de Pacotes	0

Como pode ser observado na **Erro! Fonte de referência não encontrada.**, a VM 1 possui uma largura de banda de 8Mbps, que é utilizado entre as VMs 5, 6 e 7. Diferente do Cenário 1, as taxas de transferências respeitam as regras de priorização de tráfego quando os downloads são realizados simultaneamente. Dessa maneira as redes simuladas das máquinas possuem uma largura de banda garantida para acesso à internet. No Cenário 2, a latência das Vms 5 e 6 tiveram valores aproximados de 1ms(milissegundos), e a VM 7 apresentou 1.939ms de latência. A **Erro! Fonte de referência não encontrada.** mostra que a perda de pacotes é 0 nas 3 Vms e o *jitter* que é a variação da latência, fica próximo a 0 nas VMs 5, 6 e 7.

A comparação e o comportamento da rede com e sem o uso de gerência de redes e QoS são apresentados na seção seguinte.

4.3. Comparativo entre os resultados dos cenários 1 e 2

Essa seção tem por objetivo apresentar uma analise comparativa entre os resultados obtidos nos testes realizados nos cenários. A Tabela 7 foi construída com os dados dos testes realizados nos Cenários 1 e 2.

Tabela 7: Tabela comparativa entre os cenários

COMPARATIVO			
Máquina Virtual	**Parâmetros**	**Resultados**	
		Cenário 1	**Cenário 2**
VM 1 Roteador	Largura de Banda	8 Mbps	8 Mbps
VM 5 Rede Portal	Largura de Banda	≅ 2,67 Mbps	≅ 1 Mbps
	Latência	≅ 1ms	≅ 1ms
	Jitter	≅ 0ms	≅ 0ms
	Perda de Pacotes	0	0
VM 6 Rede Administrativa	Largura de Banda	≅ 2,67 Mbps	≅ 2 Mbps
	Latência	≅ 1ms	≅ 1ms
	Jitter	≅ 0ms	≅ 0ms
	Perda de Pacotes	0	0
VM 7 Rede Acadêmica	Largura de Banda	≅ 2,67 Mbps	≅ 5 Mbps
	Latência	1.939ms	1.927ms
	Jitter	≅ 0ms	≅ 0ms
	Perda de Pacotes	0	0

A Tabela 7 mostra que a largura de banda do roteador da operadora simulado na VM 1 se manteve nos dois cenários. No Cenário 2, a VM5 que simula a rede do portal teve redução aproximada de 62,55% na largura de banda em comparação com o Cenário 1. Essa redução ocorre vista a priorização do tráfego de download para as redes conforme as regras previamente configuradas. Os demais parâmetros analisados na VM 5 mantiveram os mesmos valores nos dois cenários.

A VM6 que simula a rede administrativa teve redução de aproximadamente 25,09% na largura de banda. Essa redução ocorre vista a priorização do tráfego conforme a definição da largura máxima de banda em 2Mbps. Os demais parâmetros analisados na VM 6 mantiveram os mesmos valores nos dois cenários.

A VM7 que simula a rede acadêmica teve um aumento de aproximadamente 87,26% na disponibilidade de largura de banda. Esse aumento ocorre vista a priorização do tráfego conforme a definição da largura máxima de banda em 5Mbps. Em comparação com o Cenário 1, a latência obteve uma redução de 0.012ms no Cenário 2. A perda de pacotes e o jitter mantiveram os mesmos resultados nos 2 cenários.

Comparando os resultados alcançados com o uso da ferramenta de gerência e QoS, pode-se notar o êxito na priorização do tráfego das redes do CEULP/ULBRA, e a coleta de informações, comprovando melhorias na rede LAN do CEULP/ULBRA.

Na próxima seção serão apresentadas as considerações finais sobre o desenvolvimento deste trabalho.

5 CONSIDERAÇÕES FINAIS

Nesse trabalho foram abordados os conceitos sobre gerência de redes, ferramentas de gerência de redes, coleta de informações em dispositivos gerenciáveis e priorização de tráfego de rede. As compreensões destes conceitos foram de grande importância para que fosse possível a definição e a configuração das ferramentas e aplicação dessas nos cenários virtuais criados.

O uso de ferramentas que auxiliam o administrador no gerenciamento dos ativos de rede facilita e otimiza um trabalho que é oneroso devido às mudanças constantes nas configurações dos computadores. A eficiência do Zabbix como ferramenta de gerência foi confirmada nos testes realizados no Cenário 2, onde a ferramenta, além de realizar os monitoramentos básicos de tráfego, disponibiliza a configuração de outras funcionalidades não apresentas nesse trabalho por não ser o foco principal.

A priorização de tráfego por largura de banda e tipo de tráfego utilizando QoS é uma necessidade de instituições que não possuem um link capaz de atender todas as demandas geradas pelos usuários. Nesse sentido o uso do QoS é proposto para disponibilizar insumos de rede aos serviços essenciais, priorizando e melhorando a velocidade de acesso à redes, ás páginas e serviços mapeados como precípuos.

Como o trabalho teve por objetivo apresentar uma proposta de melhoria de LAN do CEULP/ULBRA utilizando ferramentas de gerência de redes e QoS, o ambiente proposto no Cenário 2 foi apresentado ao administrador de rede do CEULP/ULBRA, que iniciou a implantação das técnicas e ferramentas apresentadas nesse trabalho para mitigar o problema de gargalo no acesso à internet que a instituição enfrenta.

No cenário real da instituição, o ZABBIX foi implantado e está sendo utilizado no monitoramento dos servidores de GW, roteadores e servidor do portal. Além do ZABBIX, foi instalado a ferramenta SqStat que interpreta os logs do Squid e o IfTop que realiza o monitoramento das conexões existentes com a internet. As ferramentas citadas auxiliam o administrador gerir e monitorar o uso dos insumos de internet e da rede da instituição.

5.1. Trabalhos futuros

Com relação aos trabalhos futuros, propõe-se realizar a segmentação por categoria das páginas mais acessadas e que consomem mais recursos de banda de internet. Essa categorização poderá ser dividida em “Redes Sociais”, “*Streaming*”, “Acesso produtivo”, e outras categorias. Na categoria de “Redes Sociais” devem ser inseridos os domínios de redes sociais como Facebook, MySpace, Twitter, Linkedin, etc. Na categoria de “*Streaming*” devem ser inseridos domínios de *Streaming* como Youtube, Vimeo, Rdio, Grooveshark, etc. E na categoria de “Acesso produtivo” deverão ser inseridos os domínios da instituição, motores de busca como Google, Yahoo, Cadê, etc. Após a categorização das páginas, deverá ser configurado as subclasses do QoS que utilizarão o IPTABLES para priorização do tráfego conforme a prioridade dos serviços classificados.

Por fim, outra proposta seria implantar no ambiente real todas as técnicas apresentas e realizar o cadastramento de todos os dispositivos da rede. Os dispositivos poderão ser cadastrados e monitorados por grupos, bloco, setores, redes, etc. Com esse monitoramento é possível realizar a verificação do uso dos insumos de rede por dispositivo e gerar relatórios abrangentes.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Fabiano R.; PIRES, Herbert Domingues. **Gerencia de redes**. Disponível online: http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf. Ultimo acesso em: 24/10/2012.

BLUMENTHAL, U.; WIJNEN, B. **User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**. 1999. Disponível em http://www.ietf.org/rfc/rfc2574.txt. Acesso em: 06/11/2012.

CACIC. Portal Do Software Público Brasileiro. **CACIC: Configurador Automático e Coletor de Informações Computacionais**. Disponível em: http://www.softwarepublico.gov.br/ver-comunidade?community_id=3585. Acesso em 21/11/2012.

COUTO, André Valente. **Uma Abordagem De Gerenciamento De Redes Baseado No Monitoramento De Fluxos De Tráfego Netflow Com O Suporte De Técnicas De Business Intelligence**. 2012. 116 f. Dissertação (Mestrado em Engenharia Elétrica)–Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2012.

DAVIDSON, Jonathan; PETERS, James; BATHIA, Manoj; KALIDINDI, Satish; MUKHERJEE, Sudipto. **Fundamentos de Voip: Uma Abordagem Sistêmica Para a Compreensão dos Fundamentos de Voz Sobre IP.** 2ª Edição. Porto Alegre: Bookman. 2008, 389 p.

DENNING, Peter J. **The ARPANET after Twenty Years.** 1989. Disponível em: http://denninginstitute.com/pjd/PUBS/AmSci-1989-6-arpanet.pdf. Acesso em: 26/10/2012.

FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. **A Simple Network Management Protocol (SNMP)**. 1990. Disponível em http://www.ietf.org/rfc/rfc1157.txt. Acesso em: 06/11/2012.

FRYE, R.; LEVI, D.; Routhier, S.; Wijnen B. **Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework**. 2003. Disponível em http://bgp.potaroo.net/ietf/rfc/PDF/rfc3584.pdf. Acesso em: 02/11/2012.

HARRINGTON, D.; PRESUHN, R.; WIJNEN, B. **An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks**. 2002. Disponível em http://bgp.potaroo.net/ietf/rfc/PDF/rfc3411.pdf. Acesso em: 06/11/2012.

KUROSE, James F.; ROSS Keith. **Redes de computadores: Uma abordagem top-down**. 3ª Edição. São Paulo: Pearson addison Wesley. 2007, 634 p.

LARSEN, A. **Guaranteed Service: Monitoring Tolls**. Data Communications, jun. 1997, p.85-94.

MCCLOGHRIE, K.; CASE, J.; ROSE, M.; WALDBUSSER, S. **Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)**.1996. Disponível em http://www.ietf.org/rfc/rfc1907.txt. Acesso em: 06/11/2012.

MENEZES, Elionildo S.; SILVA, Pedro Luciano L. **Gerenciamento de Redes: Estudos de Protocolos.** 1998. Disponível em: http://www.cin.ufpe.br/~flash/ais98/gerrede/gerrede.html. Acesso em: 01/11/2012.

MUNDY, R.; CASE, J.; PARTAIN, D.; STEWART B. **Introduction to Version 3 of the Internet-standard Network Management Framework**. 1999. Disponível em: http://www.ietf.org/rfc/rfc2570.txt. Acesso em: 06/11/2012.

OLIVEIRA, Décio Tostes. **Gerência de Redes de Computadores: Uma Abordagem com o uso do SMNP.** 2002. Disponível em: http://lrodrigo.lncc.br/images/1/1f/GerRedesUmaAbordagemComUsoDoSMNP.pdf. Acesso em: 07/11/2012.

PERKINS, D.; MCCLOGHRIE, K.; SCHOENWAELDER, J. **Structure of Management Information Version 2 (SMIv2)**. 1999. Disponível em: http://www.ietf.org/rfc/rfc2578.txt.pdf. Acesso em: 06/11/2012.

PINHEIRO, José Mauricio Santos. **Gerenciamento de Redes de Computadores: Uma Breve Introdução.** 2006. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php. Acesso em: 01/11/2012.

ROSE, M.; MCCLOGHRIE, K. **Structure and Identification of Management Information for TCP/IP-based Internets**. 1990. Disponível em: http://www.ietf.org/rfc/rfc1155.txt.pdf. Acesso em: 10/11/2012.

SAMORUKOV, Alex. **About SqStat.** 2006. Disponível em: http://samm.kiev.ua/sqstat/. Acesso em: 12/06/2013.

SPECIALSKI, Elizabeth Sueli. **Gerência de Redes de Computadores e de Telecomunicações**. 2002. Disponível em: http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf. Acesso em: 07/11/2012.

SOURCEFORGE.NET. **Iperf**. 2008, Disponível em: http://iperf.sourceforge.net. Acesso em 21/05/2013.

SOURCEFORGE.NET. **Iperf**. 2013, Disponível em: http://sourceforge.net/projects/iperf. Acesso em 21/05/2013.

STALO Filho, André. **Linux: controle de redes.** 1ª Edição. Florianópolis: Visual Books. 2009, 352 p.

SZTAJNBERG, Alexandre. **Conceitos Básicos sobre os Protocolos SNMP e CMIP**. 1996. Disponível em: http://professor.ucg.br/siteDocente/admin/arquivosUpload/5029/material/GerenciameGer%20de%20Redes(1).htm. Acesso em: 08/11/2012.

TANENBAUM, A. S. **Redes de Computadores**. 5ª Edição. São Paulo: Pearson Education, 2011, 582 p.

WARREM, Paul; LIGHTFOOT, Chris. **Iftop: display bandwidth usage on an interface.** 2009. Disponível em: http://www.ex-parrot.com/pdw/iftop/. Acesso em: 12/06/2013

ZABBIX SIA. **About Zabbix**. 2013, Disponivel: http://zabbixbrasil.org/?page_id=59. Acesso em: 21/05/2013.

APÊNDICE A – Entrevista com o administrador de redes do CEULP/ULBRA

As perguntas abaixo foram respondidas para as redes administrativa e acadêmica.

- Qual o volume do tráfego de download e upload na ultima semana?
- Qual o volume do tráfego de download e upload no ultimo mês?
- Quantos servidores existem na rede e qual sua funcionalidade e serviços que que disponibiliza?
- Quais os horários de maior consumo de banda?
- Quais horários com maior número de acessos?
- Quais as páginas mais acessadas?
- Quais páginas consomem maiores fatias da banda?
- Quais os tipos de tráfegos?
- Qual a quantidade de host na rede?
- Quais ferramentas de monitoramento e acompanhamento são utilizadas para gerenciar a rede?
- Existe alguma ferramenta de gerência de rede implantada para o monitoramento do parque computacional da instituição? Em caso afirmativo, quantos dispositivos são monitorados?
- Quais os principais problemas detectados na rede?

APÊNDICE B – Entrevista com o administrador de redes do portal do CEULP/ULBRA

- Qual o volume do tráfego de download e upload no ultimo mês?
- Quais os horários de maior consumo de banda?
- Quais horários com maior número de acessos?
- Quais as páginas mais acessadas?
- Quais páginas consomem maiores fatias da banda?
- Quais os tipos de tráfegos?
- Qual a quantidade de servidores?
- Quais ferramentas de monitoramento e acompanhamento são utilizadas para gerenciar os servidores?
- Quais os principais problemas detectados na rede do portal?