ANA ELISA LEITÃO ALONSO FERREIRA

ENGENHARIA DE TRÁFEGO EM REDES IP: ESTUDO E APLICAÇÃO DE FERRAMENTAS DE MEDIÇÃO

Dissertação apresentada ao curso de Pós-Graduação em Computação da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de mestre. Área de Concentração: Processamento Paralelo e Distribuído.

Orientadora: Pofa. Dra. Maria Luiza D'Almeida Sanchez
Co-orientador: Prof. Dr. Carlos Alberto Malcher Bastos

Niterói
2005

F 383 Ferreira, Ana Elisa Leitão Alonso.
Engenharia de Tráfego em redes IP: estudo e aplicação de ferramentas de medição / Ana Elisa Leitão Alonso Ferreira – Niterói: [s.n.], 2004.

197 f.:il, 30 cm.

Dissertação (Mestrado em Computação – Processamento Distribuído e Paralelo) – Universidade Federal Fluminense, 2005.

1. Ferramentas de medição e geração de tráfego. 2. Engenharia de tráfego. 3. Qualidade de serviço em redes IP. 4. Redes IP de computação. 5. Computação – Teses. I. Título

CDD 004.67

Dedicatória

Dedico este trabalho à minha família, em especial meu marido Wagner e meus filhos, Caio e Tiago, por todo o apoio, toda a ajuda que recebi. Por compreender todas as minhas muitas ausências, minha falta de disponibilidade para as coisas mais simples, o cansaço das noites em claro e todo o esforço empreendido para que finalmente esta etapa se completasse.

Agradecimentos

Gostaria de agradecer a todos aqueles que direta ou indiretamente contribuíram para este trabalho. Certamente não vou me lembrar de todos, porém gostaria de agradecer em especial:

À minha família, incluindo meu marido, Wagner, meus pais, Cecília e Fernando, minha sogra, Luiza, minhas irmãs, Ana Cristina e Ana Paula, e meus cunhados, Andréa e Robson, por tantas vezes cuidarem dos meus filhos para que eu pudesse trabalhar.

À equipe do NTI, da UFF, Augusto, Léo, Felipe e Marcelo, que esteve junto comigo em alguns dos momentos cruciais deste trabalho, que foram a realização dos testes de homologação dos equipamentos.

Aos profissionais das empresas visitadas, quase todos grandes amigos, pela atenção e por prestar todas as informações solicitadas sem qualquer dificuldade, em especial Zezão, Caputo e Márcia.

Aos colegas Deolinda, Viterbo e Helder e a profa. Maria Luiza pelo apoio, pelo companheirismo e pelo auxílio em situações difíceis.

Aos demais professores e funcionários deste curso que todos à sua maneira me preparam e me auxiliaram a alcançar este desfecho. Obrigada Ângela por todas as vezes que me avisou dos prazos, exigências e restrições.

E ao meu co-orientador que me deu a oportunidade de empreender esta trajetória e me acompanhou em todos os instantes, me levando por vezes do desespero à realização.

Resumo

A qualidade de serviço é uma necessidade cada vez mais presente tanto para usuários como para provedores de serviço, em especial serviço de acesso à Internet. Os usuários finais desejam aumentar o seu grau de satisfação com os serviços e demandam garantias para trafegar aplicações de tempo real e de missão crítica, por outro lado os operadores desejam aumentar seus lucros oferecendo serviços de valor agregado. A implementação de mecanismos de QoS permite o tratamento diferenciado dos vários perfis de tráfego, entretanto o atendimento aos parâmetros de QoS acordados com os clientes via SLAs – *Service Level Agreements* só é possível com a otimização da utilização dos recursos e a constante monitoração da rede.

Este trabalho apresenta um levantamento dos principais tópicos relacionados à qualidade de serviço em *backbones* IP, dando ênfase à engenharia tráfego e à medição como elementos fundamentais para que seja possível atender aos requisitos dos clientes e até mesmo planejar metas de qualidade a serem atingidas. Apesar destes não serem conceitos novos são extremamente importantes e encontram muitas dificuldades para sua utilização prática.

Complementando este levantamento foram analisadas diversas ferramentas desenvolvidas pela comunidade internacional de pesquisa. Dentre estas ferramentas duas foram selecionadas para testes realizados para a homologação de equipamentos para o *backbone* da UFF. Foi feito ainda um estudo em três empresas operadoras de telecomunicações para verificar a utilização da engenharia de tráfego e de ferramentas de medição na gerência de suas redes.

Abstract

Quality of service is a necessity even more present in such a way for users as for service suppliers, in special for service of Internet access. The end users desire to increase its degree of satisfaction with the services and demand guarantees to pass through real time and critical mission applications, on the other hand the operators desire to increase its profits offering aggregate value services. The implementation of QoS mechanisms allows the differentiated treatment of the some profiles of traffic, however the achievement of the QoS parameters commited with the customers via SLAs - Service Level Agreements is possible only with the otimization of the network resources and its constant measurement.

This work presents a survey of the main topics related to the quality of service in IP backbones, giving emphasis to traffic engineering and the measurement as basic elements so that it is possible to achieve the customers requirements and even though to plan quality goals to be reached. Despite these not being new concepts they are extremely important and find many difficulties for its practical use.

Complementing this survey, diverse tools developed for the international community of research had been analyzed. Amongst these tools, two had been selected for tests carried through the equipment homologation for UFF backbone. It was made still a study in three brazilian carries to verify the use of the traffic engineering and measurement tools in the management of its networks.

Índice

Capítulo 1
Introdução

1.1. Qualidade de serviço, engenharia de tráfego e medição

O termo qualidade de serviço é usado extensivamente hoje em dia, não apenas na área de telecomunicações, aonde tem suas raízes, mas também em relação a serviços de banda larga, *wirelles*, multimídia e outros serviços baseados em IP. Redes e sistemas estão gradualmente sendo desenhados considerando requisitos de desempenho fim a fim. Entretanto o termo QoS é usualmente mal-definido (ITUT, 2001). A recomendação E.800 do ITU-T (ITUT, 1994) provê uma definição de QoS muito utilizada em padrões, relatórios e especificações: *"o efeito coletivo do desempenho do serviço que determina o grau de satisfação do usuário"*.

O tratamento diferenciado de fluxos de tráfego é uma necessidade cada vez mais presente tanto para usuários como para provedores de serviço, em especial serviço de acesso à Internet, que cada vez mais vem sendo utilizada para trafegar dados com requisitos de qualidade para os quais o IP não possui suporte nativo. Os usuários finais desejam aumentar o seu grau de satisfação com os serviços e demandam garantias para trafegar aplicações de tempo real e de missão crítica. Por outro lado os operadores desejam aumentar seus lucros oferecendo serviços de valor agregado. A implementação de mecanismos de QoS permite o tratamento diferenciado dos vários perfis de tráfego, entretanto o atendimento aos parâmetros de QoS acordados com os clientes via SLAs – *Service Level Agreements* só é possível com a otimização da utilização dos recursos e a constante monitoração da rede.

A engenharia de tráfego é um conjunto de técnicas voltadas para a otimização do desempenho da rede, cuja utilização facilita o atendimento a padrões de qualidade e a implementação de mecanismos de QoS, permitindo aos provedores de serviços otimizar a utilização e o desempenho de suas redes, de forma a obter um melhor retorno financeiro sem que seja necessário realizar grandes investimentos na infra-estrutura da rede. Apesar de ser extremamente útil, a engenharia de tráfego não é fácil de ser implementada em grandes redes IP, visto que muitas informações não são obtidas automaticamente de forma consistente, bem como parte da configuração ainda é praticamente manual.

A Internet é um caso especial de redes IP em que os pontos fracos e fortes do protocolo se encontram potencializados. Seu sucesso se deve em parte ao paradigma de encaminhamento de pacotes do IP, que torna a implementação de redes mais fácil e barata em comparação com outros protocolos, e à ausência de um organismo central regulador, o que evita problemas de escala pois diferentes partes da rede podem crescer separadamente. Entretanto esta ausência também impede que sejam estabelecidos padrões mínimos de qualidade para desempenho e recuperação da rede. Os pacotes usualmente atravessam muitas fronteiras administrativas no seu caminho entre origem e destino, e freqüentemente o único ponto de acordo entre estas administrações separadas é que todos os problemas são responsabilidade de outra pessoa (JACOBSON, 1997). Isto se torna crítico para serviços que necessitam de garantias de desempenho. Usualmente a medição fim a fim dos parâmetros de qualidade é a única forma possível de aferir as características da rota utilizada por um fluxo de tráfego.

Apesar disto, historicamente, a medição de parâmetros de qualidade e de desempenho tem sido feita inadequadamente na Internet (PAXSON, 1998). Hoje em dia a situação é ainda pior. O gigantesco aumento no número de máquinas, redes, tipos de redes e pontos de interconexão resultam numa ausência generalizada de entendimento do desempenho da rede. A medição consistente de métricas bem definidas é portanto essencial para permitir uma melhor engenharia da rede (KALIDIN, 1999).

Este trabalho apresenta um breve levantamento dos principais tópicos relacionados à qualidade de serviço em redes IP, dando ênfase à engenharia tráfego e à medição como elementos fundamentais para que seja possível atender aos requisitos dos clientes e até mesmo planejar metas de qualidade a serem atingidas. Apesar destes não serem conceitos novos, são extremamente importantes e encontram muitas dificuldades para sua utilização prática. Em seguida são feitos a apresentação e avaliação de ferramentas de geração e medição de tráfego e dois estudos de caso de sua utilização prática.

A coleta e a análise das estatísticas básicas do tráfego, em adição às estatísticas de utilização dos enlaces, são fundamentais para que os provedores tenham a habilidade de desenhar e operar suas redes. As estatísticas em longo prazo, como por exemplo de agregados de dados, em conjunto com estatísticas em curto prazo, por fluxo de dados, provêem informações relativas a:

- Provisionamento de rede
- Acordos de interconexão
- Verificação de SLA (*Per-customer accounting*)
- Balanceamento de tráfego nos pontos de interconexão (*Per-peer accounting*)

- Gerenciamento do desempenho
- Acompanhamento de mudanças de topologia e de roteamento
- Vulnerabilidade e complexidade da conectividade
- Verificação e resolução de problemas
- Dinâmica de fluxo TCP
- Eficiência da tabela de roteamento/espaço de endereçamento (FLOYD, 2002)

Entretanto o grande volume de tráfego e a alta capacidade dos enlaces atualmente utilizados tornam a monitoração e a medição do tráfego para estas e outras utilizações um esforço cada vez maior e mais dinâmico.

O planejamento e a engenharia de redes aplicada aos *backbones* são as atividades que mais necessitam de formas confiáveis e consistentes de coleta e análise de dados, uma vez que é cada vez mais importante conhecer as suas características de desempenho e qualidade. Para alcançar estes objetivos e atender às expectativas dos usuários é preciso medir o desempenho não apenas dos equipamentos de comunicação, mas também a infra-estrutura física, a utilização de recursos das máquinas e os softwares envolvidos desde sistemas operacionais até aplicações em equipamentos e servidores.

1.2. A visão dos organismos de padronização

Organismos de padronização são organizações nacionais ou internacionais que são reconhecidas como autorizadas a escrever padrões. Em alguns casos, como por exemplo o ANSI – *American National Standart Institute*, nos Estados Unidos, existe um processo oficial para credenciar organizações. Em outros casos as organizações são aceitas como organismos de padronização devido ao seu histórico de excelência por muitos anos na área. Os principais organismos de padronizção na área de telecomunicações e comunicação de dados são:

- *Internet Engineering Task Force* (IETF)
- *International Telecommunications Union* (ITU-T)
- *Institute for Electrical and Electronics Engineers* (IEEE)

Outros importantes organismos de padronização estão listados a seguir:

- *International Organization for Standardization* (ISO)
- *Telecommunications Industry Association* (TIA)
- *Committee T1 Telecommunications* (T1)
- *European Association for Standardizing Information and Communication Systems* (ECMA)
- *European Telecommunications Standards Institute* (ETSI)

- *International Committee for Information Technology Standards* (INCITS) (anteriormente X3)

Cada um destes organismos tem diferentes propostas para:

- Definições de qualidade e classes de serviços
- Meios técnicos de implementar e melhorar a qualidade de serviço
- Métodos de medição para qualidade de serviço

1.2.1. IETF

O IETF, *Internet Engineering Task Force*, tem sido por muitos anos o principal responsável pela preparação de padrões para a Internet, isto inclui o IP e muitos dos serviços suportados.

Segundo o IETF, QoS se refere à habilidade de assegurar a qualidade experimentada pelo usuário humano final dos serviços providos pela rede. Isto envolve uma grande faixa de aspectos técnicos e não-técnicos, por exemplo:

- Verificação de desempenho e definição de SLAs (*Service Level Agreements*)
- Comportamento das aplicações para obtenção da qualidade desejada para cada serviço
- Camadas física e de rede de alto desempenho
- Encaminhamento de pacotes – foco principal do IETF

O trabalho do IETF está voltado para a pilha entre o meio físico e a aplicação, tendo desenvolvido protocolos fim a fim para transporte em tempo real, controle e sinalização de redes e aplicações, medição e monitoração de desempenho além de atividades específicas em voz sobre IP (HANCOCK, 2003).

1.2.2. ITU

O ITU-T, ITU *Telecommunications Standardization Sector*, é um orgão permanente do ITU, *International Telecommunications Union*, responsável por estudar questões técnicas e operacionais e elaborar recomendações.

O ITU-T reconhece quatro diferentes perspectivas para QoS:

- Requisitos de QoS dos clientes: determina o nível de qualidade requerida para um serviço em particular, que pode ser expresso em linguagem não-técnica. Possui seu foco em efeitos percebidos pelos usuários fim a fim e é independente da rede.

- QoS oferecida (ou planejada) pelo provedor de serviços: é a definição do nível de qualidade que o provedor de serviço espera oferecer ao cliente. O principal uso desta forma de QoS é o planejamento da rede e de sistemas de medição e a redação de SLAs.
- QoS fornecida pelo provedor de serviço: é uma constatação do nível de qualidade realmente fornecida pelo provedor. É expressa por valores associados a parâmetros, que devem ser os mesmos especificados na QoS oferecida.
- QoS percebida pelo cliente: Geralmente expressa em níveis de satisfação, reporta o nível de qualidade que o cliente acredita ter experimentado.

O ITU-T elaborou recomendações, como por exemplo I.350 (ITUT, 1993a) e Y.1540 (ITUT, 2002a), que tratam de todos os aspectos da QoS: defnição, implantação e medição.

1.2.3. IEEE

O IEEE – *The Institute of Electrical and Electronics Engineers*, (IEEE, 2003) define QoS como a habilidade de um elemento de rede, por exemplo um roteador, um *host* ou uma aplicação, para oferecer algum nível de garantia de que os requisitos de tráfego e de serviço podem ser satisfeitos. O IEEE identifica três níveis de QoS:

- QoS de aplicação: lida com o controle de banda e o policiamento para tráfegos individuais acessando servidores.
- QoS de rede de acesso: controle de banda e policiamento para tráfegos individuais que entram na rede.
- QoS de núcleo de rede (*backbone*): trata da alocação de recursos de rede e controle do tráfego agregado.

Os principais requisitos de QoS identificados pelo IEEE são classificação, condicionamento, priorização, medição, provisionamento e gerenciamento/monitoração de nível de serviço.

1.3. Estrutura deste trabalho

Neste trabalho foi feito o estudo dos principais tópicos relacionados à qualidade de serviço em *backbones* IP, com ênfase na geração e medição de tráfego como base para a implantação e a operação de uma rede com garantias de qualidade de serviço. Foi feito também um levantamento de ferramentas de geração e medição de tráfego desenvolvidas pela comunidade acadêmica e das ferramentas utilizadas comercialmente por três das principais empresas provedoras de serviços de telecomunicações e Internet do mercado brasileiro.

Complementando este levantamento foram selecionadas duas ferramentas para testes reais de equipamentos durante a homologação de *switches* para a atualização do *backbone* da UFF.

No capítulo dois é feita uma breve introdução às principais tecnologias de redes de alta velocidade, em especial redes IP e ATM. Em seguida são apresentados os seus modelos operacionais (OAM), enfocando os tópicos relativos à qualidade de serviço e à medição e geração de tráfego. Este trabalho prioriza as redes IP, devido ao seu óbvio predomínio sobre as demais tecnologias, apesar da permanência do ATM no núcleo da rede de diversos provedores. Neste capítulo ainda são descritos os principais modelos de gerenciamento de redes especificados pela IETF – SNMP (CASE, 1990) e RMON (WALDBUSSER, 1995). São identificadas as interligações e as diferenças entre o gerenciamento, a monitoração e a medição de redes.

No capítulo três são apresentadas as principais metodologias e métricas para medição de desempenho de redes, bem como um resumo da sua utilização. Este é um tópico controverso pois existem diversos organismos de padronização que divulgam documentos semelhantes porém com diferentes enfoques tanto sobre medições como sobre qualidade de serviço. Por este motivo são apresentadas inicialmente métricas “tradicionais”, derivadas das métricas utilizadas em redes de telecomunicações, e em seguida métricas desenvolvidas especificamente para redes IP pela IETF.

O capítulo quatro aborda a necessidade de implementar QoS em redes IP e os modelos e mecanismos desenvolvidos para tal. Este capítulo faz inicialmente uma rápida revisão dos conceitos fundamentais e dos modelos desenvolvidos para assegurar qualidade em redes IP, incluindo uma nova filosofia de serviços *“non-elevated”*. Em seguida é tratada a questão da medição em redes que implementam QoS, tanto como forma de assegurar o bom funcionamento da rede e a sustentabilidade dos serviços através do controle de admissão, como também para a monitoração e verificação da qualidade realmente provida.

O capítulo cinco trata da engenharia de tráfego, fundamental para o atendimento aos parâmetros de qualidade em redes de grande abrangência e alta velocidade. É dada uma visão geral do que é a engenharia de tráfego, seu modelo de funcionamento e subsistemas componentes. Em seguida são tratadas questões de medição específicas, como a escala de tempo, as bases de medição e entidades de medição utilizadas na engenharia de tráfego. Também é apresentada a necessidade de obtenção da matriz de tráfego da rede e a monitoração do seu desempenho, bem como as dificuldades encontradas na prática atual.

No capítulo seis são estudadas as ferramentas utilizadas para monitoração, medição e geração de tráfego. São apresentados os tipos de ferramentas usadas na operação de redes e são listados exemplos de ferramentas de geração e medição de tráfego que permitem

uma enorme flexibilidade para a realização de medições de desempenho. Também estão relacionados os principais projetos de medição ativa, passiva e de infra-estrutura de medição sendo desenvolvidos internacionalmente para redes de grande alcance, mais especificamente para a Internet. Adicionalmente foram feitas visitas a três importantes empresas prestadoras de serviços de telecomunicações e de Internet para levantar o panorama atual das ferramentas de monitoração e medição utilizadas comercialmente.

No capítulo sete são apresentados dois estudos de caso da utilização das ferramentas de geração e medição de tráfego durante testes de homologação de equipamentos. Estes testes são parte do processo de substituição dos equipamentos do núcleo da rede de comunicação de dados da UFF, e visam ratificar as informações prestadas pelo fabricante a respeito das características e funcionalidades dos *switches*, e verificar o seu desempenho em situações que simulam o ambiente de produção.

Por fim o capítulo oito apresenta as conclusões e propostas de novos trabalhos, ampliando e dando continuidade ao já realizado.

Capítulo 2

Redes, OAM e Gerenciamento

2.1. Introdução

Este capítulo aborda as tecnologias de rede IP e ATM , revendo brevemente suas principais características, funções de OAM – Operação, Administração e Manutenção, e modelos de gerenciamento e monitoração. Embora sejam tecnologias que atuam em diferentes camadas a comparação se impõe devido à competição estabelecida na prática no universo das redes de alta velocidade: ATM x IP sobre gigabit Ethernet ou mesmo diretamente sobre redes óticas.

As tecnologias de redes de alta velocidade estão cada vez mais permitindo a convergência das redes de telecomunicações e de comunicação de dados, transportando um volume e uma variedade de tráfego cada vez maior. Estas redes vão continuar a se expandir em termos de extenção geográfica e organizacional, velocidade e complexidade. Para assegurar a estabilidade e a confiabilidade da rede, e o atendimento aos requisitos de qualidade dos diferentes tipos de tráfego é necessário realizar a medição das características do tráfego e a monitoração do desempenho da rede através de métricas bem definidas. Estas medições fornecem dados para que os provedores possam gerenciar suas redes eficientemente. Para atingir este objetivo são utilizados os mecanismos de OAM próprios de cada tecnologia, bem como aplicações de gerenciamento e técnicas de engenharia de tráfego. OAM compreende um conjunto de ações realizadas visando obter a máxima produtividade da rede e dos recursos utilizados, integrando as funções de operação, administração e manutenção. Provê indicações de falhas, informações de desempenho e diagnósticos da rede.

As redes IP não possuem recursos nativos de OAM, utilizando para isto uma grande variedade de ferramentas desenvolvidas, em geral, para atender a uma necessidade específica. Esta situação é totalmente diversa para o ATM, pois o desenvolvimento da tecnologia ATM contemplou também o desenvolvimento de mecanismos de OAM que são parte integrante da rede. Assim é possível utilizar estas informações como subsídio para a gerência da rede.

A gerência de redes compreende diversos aspectos, entre eles a monitoração e a medição dos padrões de qualidade da rede. A monitoração da rede e de seus elementos permite a utilização de técnicas de otimização da distribuição do tráfego (engenharia de tráfego), obtendo assim a melhoria da qualidade de serviço. A monitoração da rede possibilita as seguintes ações:

- Otimização do desempenho, através do balanceamento da carga e da identificação pró-ativa de gargalos e de recursos subutilizados,
- Diagnóstico e a solução de falhas antes de sua percepção pelo usuário, aumentando a disponibilidade e a confiabilidade da rede,
- Planejamento da rede.

Para alcançar estes objetivos e atender às expectativas dos usuários é preciso medir não apenas o desempenho dos equipamentos de comunicação, mas também a utilização da infra-estrutura física, dos recursos das máquinas e os *softwares* envolvidos desde sistemas operacionais até aplicações em equipamentos e servidores.

A monitoração da rede é feita na fase de instalação e aceitação, e, principalmente, durante a sua operação. Na fase de instalação são realizados complexos testes envolvendo a geração e medição de tráfego. A escolha do teste e a avalição dos resultados obtidos são determinados pela especificação da rede. A informação é usada para justificar a afirmação de que a rede está funcionando adequadamente.

A medição em uma rede operacional é muito diferente da realizada na fase de implantação em termos do objeto da medição e da utilização da informação obtida. A monitoração e a medição de redes operacionais possui características muito particulares, uma vez que envolve o fornecimento de dados para definições estratégicas e lida com o tráfego do cliente, que não deve perceber qualquer impacto das atividades desenvolvidas para o gerenciamento da rede.

Em uma rede operacional a informação coletada é utilizada para suportar o negócio de serviços de rede. Este é o requisito principal para um sistema de monitoração para redes em produção. As informações de medição suportam os processos de negócio da empresa. Outra diferença importante na fase operacional é o foco da medição. Não é a rede e sim o tráfego do usuário que deve ser medido. Obviamente algumas partes da rede, incluindo equipamentos e infra-estrutura, são monitoradas e o desempenho de alguns elementos pode ser medido ou deduzido a partir da medição do tráfego do usuário. Entretanto é sobre a qualidade do serviço que o usuário experimenta que tanto o operador como o cliente desejam obter informações. Apenas o operador está interessado no desempenho da rede e esta

informação não é fornecida ao cliente, embora importante para otimização de processos internos, como provisionamento e recuperação.

Um sistema de gerenciamento para uma rede operacional deve suportar pontos de medição (*probes*) geograficamente distribuídos em toda a rede. Também é necessário disponibilizar informações importantes para os processos de negócio da empresa sempre que for requerido. Assim, é importante que este sistema seja distribuído e flexível. Devido ao grande número de equipamentos e a variedade de fabricantes, os sistemas de gerência, monitoração e medição devem ser escaláveis e capazes de lidar com diversos protocolos e aplicações de gerenciamento. Os organismos de padronização desenvolveram modelos de gerenciamento para atender a estas necessidades sob diferentes enfoques. Neste capítulo também serão apresentados os principais modelos atualmente em uso.

2.2. ATM

O ATM (ATM, 2004) foi concebido para ser uma tecnologia multisserviço, apropriada para uma faixa de aplicações virtualmente ilimitada. Uma rede ATM pode prover conexões com diferentes níveis de serviço.

O conceito de negociar, para cada conexão, o comportamento esperado em termos de tráfego e desempenho permite aos usuários uma melhor correlação entre os requisitos da aplicação e a capacidade da rede. Dada a presença de uma mistura heterogênea de tráfego e a necessidade de controlar adequadamente a alocação de recursos da rede para cada componente do tráfego, um alto grau de flexibilidade e utilização da rede pode ser obtido provendo um conjunto de parâmetros a serem selecionados dentro da camada ATM. As categorias de serviço ATM foram definidas para atender a esta necessidade.

As categorias de serviço oferecidas pelo ATM foram padronizadas por dois organismos. Apesar das diferentes nomenclaturas, a definição e a utilização de cada categoria são muito semelhantes, como pode ser visto na tabela 2.1 abaixo (ATM, 1996).

ATM FORUM TM4.0 "ATM SERVICE CATEGORY"	ITU-T I.371 "ATM TRANSFER CAPABILITY"	TYPICAL USE
Constant Bit Rate (CBR)	Deterministic Bit Rate (DBR)	Real-time, QoS guarantees
Real-Time Variable Bit Rate (rt-VBR)	(for further study)	Statistical mux, real-time
Non-Real-Time Variable Bit Rate (nrt-VBR)	Statistical Bit Rate (SBR)	Statistical mux
Available Bit Rate (ABR)	Available Bit Rate (ABR)	Resource exploitation, feedback control
Unspecified Bit Rate (UBR)	(no equivalent)	Best effort, no guarantees
(no equivalent)	ATM Block Transfer (ABT)	Burst level feedback control

Tabela 2.1 – Categorias de serviço ATM (ATM, 1996)

Estas categorias de serviço relacionam requisitos de qualidade de serviço e características de tráfego com o comportamento da rede (procedimentos e parâmetros). A intenção é especificar uma combinação de qualidade de serviço e parâmetros de tráfego que seja apropriada para um dado conjunto de aplicações, segundo a interpretação do usuário, e que permita esquemas de multiplexação específicos, na visão da rede.

Parâmetros de Tráfego

Os parâmetros de tráfego de uma fonte descrevem suas características inerentes. Um conjunto destes parâmetros constitui um descritor da fonte de tráfego que, em conjunto com os parâmetros Cell Delay Variation Tolerance (CDVT) e Conformance Definition, caracterizam uma conexão ATM. Os seguintes parâmetros são considerados na definição de categorias de serviço:

- PCR (Peak Cell Rate) – Taxa de pico.
- SCR (Sustainable Cell Rate) – Taxa média.
- MBS (Maximum Burst Size) – Tamanho máximo de rajada.
- MCR (Minimum Cell Rate) – Taxa mínima

Os parâmetros de QoS selecionados para corresponder aos objetivos de desempenho da rede podem ser negociados, por exemplo via procedimentos de sinalização, ou podem ser adotados valores padrão. Um ou mais valores dos parâmetros de QoS podem ser oferecidos por conexão.

- CDV (Cell Delay Variation) – Variação do retardo.
- MaxCTD (Maximum Cell Transfer Delay) – Retardo máximo.
- CLR (Cell Loss Ratio) – Taxa de perda de células.

Existem diversos outros parâmetros de QoS, porém a sua negociação ainda não está prevista, como por exemplo Cell Error Ratio (CER), Severely Errored Cell Block Ratio (SECBR) e Cell Misinsertion Rate (CMR).

A tabela 2.2 abaixo relaciona as categorias de serviços aos seus descritores de tráfego e às garantias oferecidas.

SERVICE CATEGORY	TRAFFIC DESCRIPTION	GUARANTEES			USE OF FEEDBACK CONTROL
		Min Loss (CLR)	Delay/Variance	Bandwidth	
CBR	PCR	X	X	X	NO
rt-VBR	PCR, SCR, MBS	X	X	X	NO
nrt-VBR	PRC, SCR, MBS	X	NO	X	NO
ABR	PCR, MCR+ behavior parameters	X	NO	X	X
UBR	(PCR)	NO	NO	NO	

Tabela 2.2 Categorias de serviços x Descritores de tráfego x Garantias (ATM, 1996)

A tabela 2.3 exemplifica as áreas de aplicação para as categorias de serviço ATM.

APPLICATION AREA	BR	T-VBR	RT-VBR	BR	BR
Critical Data	**	*	***	*	n/s
LAN Interconnect LAN Emulation	*	*	**	***	**
Data transport/ Interworking (IP-FR-SMDS)	*	*	**	***	**
Circuit emulation -PABX	***	**	n/s	n/s	n/s
POTS/ISDN - Video Conference	***			n/s	n/s
Compressed Audio	*	***	**	**	*
Video Distribution	***	**	*	n/s	n/s
Interactive Multimedia	***	***	**	**	*

Optimum: ***, good: **, fair:*, not quoted are felt presently not applicable with advantage (might be in the future); n/s = not suitable.

Tabela 2.3 – Áreas de aplicação para as categorias de serviço ATM (ATM, 1996)

2.2.1. OAM em redes ATM

Os procedimentos necessários para operação, administração e manutenção (OAM) de redes ATM requerem que os vários nós da rede compartilhem informações. Também as entidades de gerência da camada ATM, em cada nó, precisam trocar informações para fornecer gerenciamento de VPCs/VCCs (FARKOUH, 1993; ANDERSON, 1996; GILLESPIE, 1997). Informações como notificações de falha, solicitações de testes, dados de monitoração e de desempenho precisam ser distribuídos entre os vários nós que suportam cada VPC ou VCC.

Célula OAM

O mecanismo básico utilizado para as funções de gerenciamento nas redes ATM é a célula OAM. As informações operacionais são trocadas através de células OAM que podem ser inseridas em diferentes pontos de uma conexão (VPC ou VCC).

A figura 2.1 (TEKELEC, 1997) ilustra os dois formatos possíveis da célula OAM, um para medições em VPCs e outro para medições em VCCs.

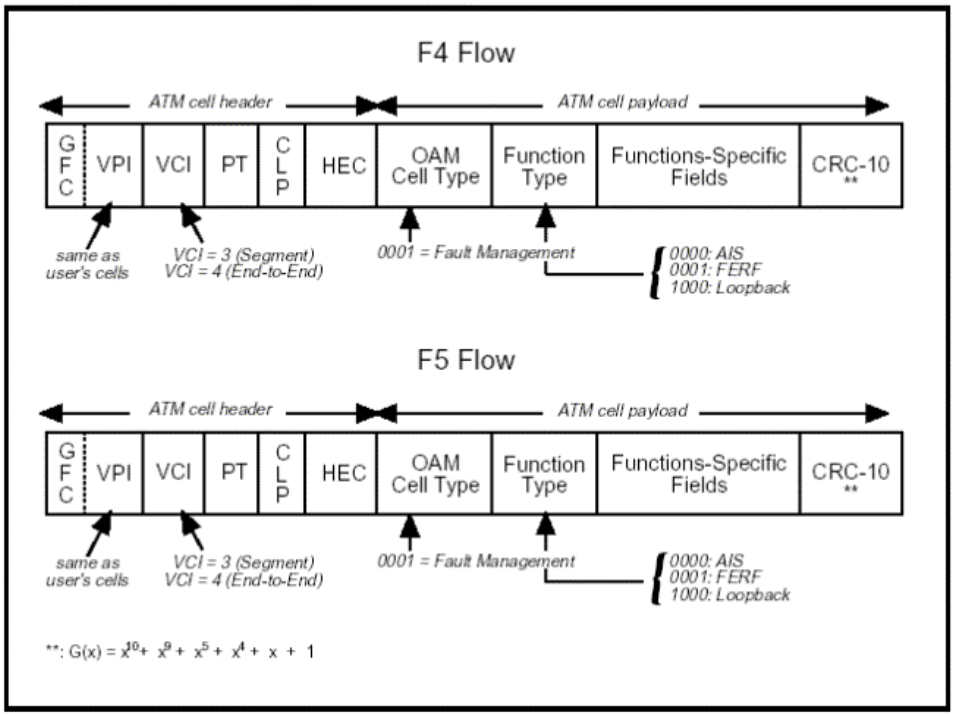


Figura 2.1 Formato da célula OAM ATM

Existem dois tipos de indicação de falha enviados através de células OAM: AIS – *Alarm Indication Signal* e FERF – *Far End Receive Failure*. Nas duas formas de indicação são providas informações sobre o tipo e a localização da falha.

Também é possível a verificação de conectividade através do envio de células OAM, uma vez que seu *payload* contém os seguintes campos: *loopback indication*, *correlation identifier*, *loopback location identifier*, e *source identifier*. Estes campos permitem o estabelecimento de *loopbacks* usados para assegurar a continuidade da conexão lógica.

Parâmetros de desempenho ATM

Os parâmetros de desempenho ATM são em sua maioria definidos pela recomendação I.356 (ITUT, 1996a) do ITU-T. Os parâmetros mais usados são (NGUYEN, 2000):

- Erros
- CER – *Cell Error Ratio*: Número de células erradas entre dois pontos de medição. Uma célula errada é definida como uma célula que contém um erro no HEC (*Header Error Check*) ou no *payload*.
- CLR – *Cell Loss Ratio*: Número de células perdidas entre dois pontos de medição.
- *Cell Missequence Ratio*: Número de células fora de seqüência entre dois pontos de medição.
- *Cell Misinsertion Rate*: Número total de células inseridas erroneamente observadas durante um intervalo de medição especificado, dividido pela duração do intervalo. Uma célula inserida erroneamente é uma célula que aparece em um canal incorretamente, devido a erros do equipamento de rede.
- SES – *Severely Errored Seconds*: Segundos durante os quais a soma de erros, células fora de seqüência e perdidas excede um limiar pré-definido.
- Retardo
- CTD – *Cell Transfer Delay*: Tempo necessário para uma célula ir de um ponto a outro na rede.
- 1pt CTDV – *Cell Transfer Delay Variation*: Mede passivamente em um único ponto da rede a variação do tempo de chegada de cada célula em relação a um tempo esperado de chegada. Este parâmetro é definido apenas para tráfego CBR.
- 2pt CTDV – *Cell Transfer Delay Variation*: Mede ativamente a variação do retardo entre dois pontos da rede comparando o retardo da célula com um valor esperado. Este valor é determinado no início do teste pelo envio e monitoração de células de teste.

Entretanto os mecanismos OAM nem sempre são usados devido à relação custo-benefício. A inserção de células OAM quando a rede já está congestionada certamente agrava o problema. (TEIXEIRA, 1999).

2.3. IP

O requisito básico da utilização original do protocolo IP é a sobrevivência a falhas. Para atender a esta necessidade foi desenvolvido o paradigma de encaminhamento de dados utilizado até hoje, que consiste na fragmentação dos dados em pacotes encaminhados separadamente por qualquer rota disponível, escolhida com base apenas nas informações locais de cada roteador. Estas características nativas do IP dificultam o provimento de serviços com qualidade garantida, uma vez que não se conhece *a priori* por qual rota os pacotes serão encaminhados.

O IP não especifica qual a tecnologia de rede a ser utilizada, de forma que é suportado por particamente qualquer tipo de rede. Com o crescimento da Internet em capacidade e topologia, o protocolo IP vem se tornando cada vez mais um padrão de fato, inclusive nos *backbones* de alta velocidade. O protocolo IP pode ser utilizado em redes de diversas tecnologias de alta velocidade, em especial as redes Fast/Gigabit Ethernet. Também está sendo estudada e padronizada a utlização do IP diretamente sobre redes óticas, reduzindo o *overhead* das camadas intermediárias.

2.3.1. OAM em redes IP

O IP, conforme definido na RFC 791 (DARPA, 1981), não implementa nenhum mecanismo de OAM, deixando estas funções para as redes que o suportam. Entretanto foram desenvolvidas diversas soluções para atender às diferentes necessidades surgidas nas situações práticas, por exemplo as aplicações Ping (POSTEL, 1981a) e Traceroute (JACOBSON, 1989) e a medição de dados de desempenho por fluxos utilizando a arquitetura RTFM (BROWNLEE, 1999). Estas aplicações estão descritas no capítulo sete que trata das ferramentas utilizadas para monitoração da rede, medição e geração de tráfego.

Assim as funções de OAM das redes IP estão dispersas em várias entidades desenvolvidas por grupos de trabalhos separados, ou são simplesmente inexistentes. Atualmente a área de OAM do IETF (OPS, 2004) possui os seguintes grupos de trabalho: *Authentication, Authorization and Accounting, Control And Provisioning of Wireless Access Points, Distributed Management, Domain Name System Operations, Global Routing Operations, Network Configuration, Resource Allocation Protocol, Configuration Management with SNMP* e *IPv6 Operations* entre outros.

2.4. Modelos de gerenciamento IP

Estão descritos a seguir dois importantes modelos de gerenciamento, que como tal, além da monitoração e medição da rede, também fazem a detecção e o diagnóstico de falhas, o armazenamento de dados históricos, a geração de relatórios ou a disponibilização de dados para tal e possibilitam a implementação de políticas de QoS e segurança de rede.

2.4.1. SNMP

O SNMP – *Simple Network Management Protocol* (CASE, 1990) é um protocolo de gerenciamento utilizado em redes IP como parte de um *framework* de gerência (CASE, 1993) que também especifica uma estrutura (SMI) e uma base de dados (MIB) para a informação de gerenciamento.

2.4.1.1. Elementos da arquitetura

SMI - Structure of Management Information

A informação de gerenciamento é vista como um conjunto de objetos gerenciáveis armazenados virtualmente na MIB – *Management Information Base*. Conjuntos de objetos relacionados são definidos em módulos da MIB. Estes módulos são escritos utilizando um subconjunto da ASN.1 – *Abstract Syntax Notation One* (ISO, 1987) da OSI, chamado SMI – *Structure of Management Information* (MCCLOGHRIE, 1990), definindo assim uma estrutura de dados para a informação de gerenciamento.

MIB - Management Information Base

A MIB – *Management Information Base* (MCCLOGHRIE, 1998) define uma relação de objetos gerenciáveis considerados essenciais para a gerência de uma rede TCP/IP. Uma vez que estes elementos são essenciais, não é permitida a implementação parcial da MIB. Assim qualquer implementação conterá todos os objetos definidos na MIB. Entretanto podem ser acrescentados novos objetos à MIB, através da adição de módulos específicos de fabricantes e de objetos largamente utilizados, mesmo que não sejam padronizados, e de novas versões da MIB.

Os objetos da MIB estão organizados nos seguintes grupos:

- **Grupo System:** Contém informações como o nome do sistema e da pessoa de contato, descrição do sistema entre outras.

- **Grupo Interfaces:** Neste grupo está descrita uma tabela que possui uma entrada para cada interface do sistema com informações que são comuns a qualquer tecnologia, como o estado operacional da interface, estimativa da banda utilizada, contadores de erros e estatísticas do tráfego recebido e enviado.
- **Grupo Address Translation:** O grupo *address translation* consiste de uma única tabela que faz o mapeamento entre endereços de rede e endereços físicos.
- **Grupo IP:** Este grupo é composto de parte da configuração individual, variáveis estatísticas e tabelas. Estas informações são úteis para roteadores e outros equipamentos que implementam o protocolo IP.
- **Grupo ICMP:** O grupo ICMP – *Internet Control Message Protocol* é feito de uma lista de contadores do tráfego estatístico e outra de parâmetros de configuração.
- **Grupo TCP:** Compõem este grupo informações individuais, variáveis estatísticas e uma tabela que armazena a atividade das conexões TCP – *Transport Control Protocol*.
- **Grupo UDP:** O grupo UDP – *User Datagram Protocol*, de forma semelhante aos demais grupos de protocolo também possui informações de configuração individual, estatísticas e tabelas de informações detalhadas.
- **Grupo EGP: O** grupo EGP – *Exterior Gateway Protocol* é composto de variáveis que armazenam o tráfego EGP, dados sobre a vizinhança EGP e sobre o AS – *Autonomous System*.

Protocolo de gerenciamento

O SNMP modela todas as funções dos agentes de gerenciamento como alterações ou inspeções de variáveis da MIB. Ou seja, uma entidade em um equipamento remoto, assim como a entidade central de gerência, o NMS – *Network Management System*, interage com o agente residente no elemento de rede para obter ou alterar valores de variáveis.

A estratégia implícita no SNMP é a de que a monitoração do estado da rede em qualquer nível de detalhamento é realizada primariamente através da consulta (*polling*) da informação apropriada. Um número limitado de mensagens não solicitadas (*traps*) guia a temporização e o foco do *polling*. A comunicação da informação de gerência entre as entidades de gerenciamento é realizada pelo SNMP através da troca de mensagens do protocolo. Esta troca requer apenas um serviço de datagramas não confiável e cada mensagem é representada inteira e independentemente por um único datagrama de transporte. Uma mensagem consiste de um identificador de versão, um nome de community e uma PDU – P*rotocol Data Unit*, que indica o tipo de operação: solicitação ou alteração do valor de uma

ou mais variáveis; envio à estação de gerência de uma informação solicitada ou de uma notificação não solicitada.

SNMPv2

A versão 2 do SNMP foi desenvolvida principalmente para solucionar questões relativas à segurança das operações do protocolo de gerenciamento. A interação entre as duas versões é possível através da utilização de um *proxy agent behavior* ou de uma estação de gerência bilíngüe (CASE, 1996e). No modo *proxy* a conversão entre as versões é feita por um agente de *proxy*, de forma transparente tanto para a estação de gerência como para os agentes de gerência dos elementos.

No modo bilíngüe a estação de gerência pode suportar ambas as versões. Quando é necessário o contato com um agente, o NMS consulta uma base de dados local para selecionar o protocolo correto a ser utilizado. Para prover transparência para as aplicações de gerenciamento e para os usuários, o NMS deve mapear as operações simulando a ação de um *proxy*.

2.4.2. RMON

O RMON – *Remote MONitoring* (WALDBUSSER, 1995) é uma arquitetura para o gerenciamento pró-ativo de redes, integrada ao SNMP. A arquitetura RMON significou uma evolução no gerenciamento de redes. As arquiteturas existentes atuavam de forma reativa na solução de problemas, o RMON define um modelo pró-ativo de atuação, utilizando a definição de limites de tolerância para os parâmetros da rede. (LESSA, 1999).

Em sua definição RMON utiliza equipamentos de monitoração remota, chamados monitores ou *probes*, como instrumentos para o gerenciamento da rede, dedicados à implementação do módulo RMON MIB. Entretanto foram desenvolvidas outras abordagens, implementando as funções RMON em *swithes*, roteadores e outros equipamentos de rede através da inclusão de placas específicas ao equipamento ou através de aplicações de monitoração adicionadas aos *softwares* de equipamentos e servidores e de clientes de gerência. Apesar das diferentes abordagens de implementação, as funções RMON atuam como um recurso dedicado à gerência da rede, disponível para atividades de coleta de dados.

Para ser considerado "baseado em RMON", um produto deve implementar uma versão completa de ao menos um dos grupos definidos nas MIBs Token Ring e Ethernet. São encorajadas implementações proprietárias adicionais como forma de melhoria e atualização do padrão.

O principal objetivo do RMON é permitir o gerenciamento pró-ativo. As *probes* monitoram a rede continuamente, executando diagnosticos e armazenando informações de desempenho. Quando são detectadas situações pré-estabelecidas, como por exemplo condições de falhas, de erros ou condições em que os parâmetros da rede ultrapassam o limite de tolerância, os eventos podem ser armazenados e a estação de gerência notificada. No caso de falhas, a informação coletada pode ser utilizada para diagnosticar a causa do problema, uma vez que o monitor pode armazenar dados no momento da falha.

Complementando este objetivo principal, existem outros que visam melhorar a utilização dos recursos da rede e da gerência, Estes objetivos são a adição de mais informações aos dados coletados, agregando valor à gerência e também à rede; a operação dos monitores independentemente da gerência (*offline*); e a possibilidade de múltiplos gerentes.

Os maiores benefícios proporcionados pelo padrão RMON são:

- Análise e monitoração poderosas que coletam informações como estatísticas de segmento e tendências, análise do padrão de tráfego em cada nó, largura de banda usada e alarmes. Os dados providos por agentes RMON permitem que fabricantes criem aplicações de gerência que reduzam o trabalho da administração da rede e os custo com a solução de problemas.
- Identificação de tendências em segmentos locais utilizando dados estatísticos e históricos.
- Decodificação das sete camadas de protocolos do modelo OSI permitindo uma análise detalhada sem o custo de um analisador de protocolo dedicado. A maioria dos problemas das aplicações cliente/servidor pode ser diagnosticada usando o filtro de captura de pacotes do RMON e dados do vários grupos.
- Monitoramento de *sites* remotos a partir de um ponto central.
- Interoperabilidade de fornecedores: Com RMON, uma variedade de diferentes estações de gerência e agentes, fornecidos por diversos vendedores, pode se comunicar entre eles através da mesma rede.
- Criação de eventos quando limiares predefinidos são atingidos: RMON tem limiares predefinidos que podem remotamente monitorar dispositivos de rede e enviar exceções quando estes dispositivos não estão mais em um limite de operação aceitável.

2.4.2.1. Estrutura da MIB

RMON v.1

O padrão RMON está definido em um módulo da MIB específico, subdividido em grupos. Estes grupos são unidades básicas para a implementação da arquitetura RMON, ou seja, se um equipamento de monitoração remota implementa um grupo, então deve implementar todos os objetos deste grupo. Entretanto todos os grupos desta MIB são opcionais. Os grupos a seguir descritos foram numerados de 01 até 10 e usados pela RMON-MIB versão 1 e pela RMON Token Ring.

- **Grupo Ethernet Statistics:** este grupo contém estatísticas medidas por pontos de prova para cada interface ethernet monitorada em um equipamento, ou seja, utilização (nível 2: camada MAC) e erros para cada subrede monitorada.
- **Grupo History Control:** controla a periodicidade da amostragem estatística dos dados em vários tipos de rede.
- **Grupo Ethernet History:** armazena amostras estatísticas coletadas pelo grupo *ethernet statistics* em redes ethernets.
- **Grupo Alarm:** periodicamente este grupo coleta amostras estatísticas das variáveis e compara com limites de tolerância configurados previamente. Se uma variável monitorada ulttrapassa este limite, então é gerado um evento. Permite ao operador definir um intervalo de amostragem e um alarme para qualquer contador registrado pelo agente. Este grupo requer a implementação do grupo de eventos.
- **Grupo Host:** o grupo *host* contém estatísticas associadas com cada máquina descoberta na rede monitorada. Contém contadores de vários tipos de tráfego para e de servidores conectados a subrede.
- **Grupo Host TopN:** este grupo contém estatísticas que descrevem quais são as máquinas que encabeçam a listagem baseada em algum(ns) parâmetro(s) de cada estatística do grupo Host.
- **Grupo Matrix:** armazena estatístcas sobre “conversas” entre conjuntos de dois endereços, ou seja, informações sobre a matriz de tráfego da rede. Mostra erros e informações de utilização no formato matriz, para qualquer par de endereços de rede.
- **Grupo Filter**: este grupo permite que pacotes sejam verificados por uma equação de filtro. Os pacotes selecionados formam um fluxo que pode ser capturado ou gerar eventos e gravar estatísticas baseadas nos pacotes.

- **Grupo Packet Capture:** o grupo *packet capure* permite que os pacotes selecionados sejam capturados antes de serem injetados na rede. Este grupo requer a implementação do grupo de filtro e decide como os dados são enviados ao console gerente.
- **Grupo Event:** este grupo controla a geração e a notificação de eventos a partir do equipamento no qual está implementado e contém uma tabela de eventos gerada pelo agente RMON.

RMON v.2

A segunda versão do RMON, o RMON v.2 (WALDBUSSER, 1997), realiza um mapeamento de todos os grupos RMON em diversos protocolos de rede como IP, IPX, DECnet, AppleTalk e protocolos OSI em geral. O RMONv.2 torna-se essencial para o gerenciamento pró-ativo das redes atuais, pois permite um monitoramento até o nível de aplicação, possibilitando coletar informações como a banda usada por uma determinada aplicação, entre muitas outras vantagens (GIORGI, 1996).

- **Grupo Protocol Directory:** o grupo *protocol directory* armazena e manipula uma lista dos protocolos que podem ser monitorados pela *probe*, permitindo a adição, remoção e configuração das entradas nesta lista.
- **Grupo Protocol Distribution:** este grupo coleta as quantidades relativas de octetos e pacotes para os diferentes protocolos detectados no segmento da rede.
- **Grupo Address Map**: o grupo *address map* faz um mapeamento de endereços MAC para endereços de rede descobertos pelo monitor, e verifica em qual interface eles estavam na última utilização.
- **Grupo Network Layer Matrix:** através do cálculo da quantidade de tráfego enviado entre cada par de endereço de rede descoberto pela *probe*, este grupo permite que seja estimada a matriz de tráfego da camada de rede.
- **Grupo Application Layer Host:** este grupo calcula a quantidade de tráfego, por protocolo, enviado e recebido para cada máquina (servidor) cujo endereço de rede foi descoberto pela *probe*.
- **Grupo Application Layer Matrix:** de forma semelhante ao grupo *network layer matrix*, este grupo permite que seja estimada a matriz de tráfego da camada de aplicação, calculando a quantidade de tráfego, por protocolo, enviada entre cada par de endereço de rede descoberto pela *probe*. Implementações desse grupo requerem que o grupo Network Layer Matrix também seja implementado.

- **Grupo User History Collection:** este grupo combina mecanismos usados nos grupos *alarm* e *history* para prover um mecanismo de história especificado pelo usuário. Esta função tem sido feita tradicionalmente por aplicações NMS, via *polling* periódico. O grupo *user history collection* permite que essa tarefa seja descarregada em uma *probe* RMON.
- **Grupo Probe Configuration:** este grupo permite controlar a configuração de vários parâmetros operacionais da *probe*.

O RMON especifica os dados a serem coletados de segmentos remotos, possibilitando uma visão agregada da rede, já o RMON2 permite um monitoramento de tráfego ampliado: com RMON2 é possível monitorar o tráfego desde a camada 2 até a 7 do modelo OSI (*Open Systems Interconnect*). Isto significa que é possível ver como flui o tráfego de rede em cada um dos 7 níveis do modelo OSI - uma capacidade que tem um impacto significativo no controle e resolução de erros em ambiente cliente/servidor.

Extensões do padrão RMON

Outras RFCs estendem as funções RMON definindo padrões de gerenciamento para elementos não cobertos pela RFC 1757. Na sua maioria, e assim como o próprio padrão RMON, definem extensões de MIB para realizar tarefas específicas. Estão listadas a seguir algumas destas extensões:

- RMON MIB *Extensions for Switched Networks* (SMON MIB) (WATERMAN, 1999)
- RMON MIB *Extensions for Interface Parameters Monitoring* (IFTOPN) (ROMASCANU, 2001)
- RMON *Extensions for Differentiated Services* (DSMON MIB) (BIERMAN, 2002a)
- RMON *Protocol Identifiers for IPv6 and Multi Protocol Label Switching* (MPLS) (STEPHAN, 2004)
- RMON *for High Capacity Networks* (HCRMON MIB) (WALDBUSSER, 2002)
- *Application Performance Measurement* MIB (APM MIB) (WALDBUSSER, 2004)
- RMON MIB *Extensions for High Capacity Alarms* (BIERMAN, 2002b)
- *Real-Time Application Quality of Service Monitoring* (RAQMON) MIB (SIDDIQUI, 2005)
- *"Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)"* (STEPHAN, 2004)

2.5. Conclusão

Neste capítulo foram abordados dois itens muito importantes – OAM e gerenciamento de redes, que se interligam em busca de um mesmo objetivo: obter o melhor rendimento possível através da operação otimizada da rede e da utilização máxima dos recursos disponíveis. Foi possível observar a diferença na filosofia adotada durante o desenvolvimento das tecnologias ATM e IP, explicitada nos mecanismos de OAM e de gerência disponibilizados. Esta mesma diferença também aparece na garantia de qualidade assegurada aos serviços de rede através de mecanismos de QoS, como será visto no capítulo 4. Na tecnologia ATM estes recursos são nativos e realmente permitem uma melhor utilização da rede. Já na tecnologia IP, as funções de OAM e QoS estão dispersas em várias entidades desenvolvidas por grupos de trabalhos separados, ou são simplesmente inexistentes. Estas comparações permitem observar que o ATM é uma tecnologia notadamente superior, entretanto é também muito complexa e, portanto, os equipamentos e a mão de obra são mais caros, muitas vezes inviabilizando a sua implantação. Juntando este problema ao fenômeno da utilização comercial da Internet, o IP se tornou um padrão de fato também em *backbones* e redes de alta velocidade.

Em conjunto com os mecanismos e funções de OAM, também são utilizados sistemas de gerência. Um sistema de gerência de redes deve ser escalável e flexível, permitindo a sua distribuição física e lógica de forma a cobrir toda a rede da empresa, seu crescimento, acompanhando a implantação de novos equipamentos de diferentes fabricantes, protocolos e aplicações. Um bom sistema de gerência deve ser capaz de realizar a monitoração e a medição da utilização e da qualidade da rede e dos serviços providos, detecção e diagnóstico de falhas, controle da topologia e da configuração da rede e dos elementos entre outras funções.

Capítulo 3
Medição e Geração de Tráfego

3.1. Introdução

Conhecer as características de desempenho e qualidade de uma rede é possível através da coleta de dados sobre o seu comportamento em diferentes cirunstâncias. Os dados são armazenados, correlacionados e analisados para determinar o desempenho da rede e a qualidade dos serviços providos, identificando por exemplo situações anormais, como congestionamento, falhas e etc.

A coleta de dados deve abranger uma ampla variedade de grandezas e de funções cobrindo desde serviços básicos de comutação de pacotes aos requisitos de desempenho da rede para aplicações específicas. Estes dados são indispensáveis para as atividades de pesquisa e planejamento, assim como para subsidiar o desenvolvimento, administração e manutenção da infra-estrutura operacional. Além disso é importante que as atividades de coleta de dados não interfiram com a estabilidade da rede e com a sua viabilidade operacional, ou seja, a capacidade de prestar serviços dentro dos níveis mínimos de operação definidos pela gerência da rede. Também é necessário assegurar que a coleta de dados não viole considerações a respeito de privacidade, segurança e políticas de uso aceitável da rede.

Em geral, qualquer atividade de coleta de dados deve ser feita considerando-se o seu impacto nos serviços e usuários da rede. Estas atividades devem ser planejadas para atingir as metas operacionais ou de pesquisa com o menor impacto possível. Ou seja as grandezas a serem avaliadas e as metodologias utilizadas devem ser escolhidas cuidadosamente, evitando sempre que possível a utilização de recursos que sabidamente interfiram no desempenho ou na qualidade da rede. Em alguns casos, os dados podem ser coletados continuamente, por exemplo para medir a quantidade de pacotes ou a distribuição da utilização de uma aplicação específica. Em outros casos isto se torna impossível devido à utilização intensiva de recursos que as investigações planejadas irão demandar, como por exemplo alta carga de tráfego na rede ou dedicação exclusiva do pessoal técnico envolvido. Nestes casos são utilizadas janelas de manutenção, intervalos específicos para a realização de atividades que podem degradar severamente o desempenho da rede, alocados em horários de baixa utilização por parte dos usuários e muitas vezes previamente agendados.

Um aspecto relevante para a avaliação da rede é o local ou locais aonde as medições são feitas. Algumas medições tomam como base observações feitas em mais de um ponto da rede. Por exemplo para obter a medida de tempo que um pacote leva para ir de uma máquina origem para uma máquina destino é necessário armazenar os horários em que o pacote sai da origem e chega ao destino usando relógios precisos e sincronizados. A realização de medições fim a fim também é útil para a obtenção de medidas na Internet, onde é muito comum que um caminho atravesse a rede de mais de um provedor de serviços. Uma vez que é irreal a cooperação entre os diferentes provedores para medir cada rede individualmente, são feitas medições fim a fim que fornecem informações úteis retratando a rede segundo a percepção do usuário.

Outro ponto importante a considerar é a escala de tempo para obtenção e disponibilização dos dados. As informações coletadas pela medição do tráfego podem ser disponibilizadas para o usuário final ou outra aplicação em tempo real ou não, dependendo das atividades que serão desenvolvidas e das ações que serão tomadas na rede. Controle de tráfego geralmente requer informação em tempo real. Para planejamento da rede e gerência de capacidade a informação pode ser provida após o processamento dos dados, sem a necessidade de ser em tempo real.

O grupo de trabalho IP *Performance Metrics* (IPPM, 2004) do IETF (IETF, 2004) desenvolveu o "*Framework for IP Performance Metrics*" (MAHDAVI, 1998), um conjunto de definições, métricas e recomendações para medição de desempenho de redes IP. O *Framework* apresenta termos para descrever a rede, explica a necessidade de métricas úteis, concretas e bem definidas, capazes de serem medidas repetidamente e de forma confiável. Sem o uso de métricas padronizadas e metodologias bem entendidas por todos, pode ser muito difícil de compreender ou mesmo impossível de comparar diferentes implementações.

3.2. Utilização da Medição e Geração de tráfego

Medições de tráfego em redes são fundamentais nas atividades de gerência, diagnóstico de problemas de desempenho, implantação e verificação de contratos de qualidade de serviço, planejamento de capacidade, bilhetagem, dentre outras. As atividades realizadas na operação de redes podem ser agrupadas em três grandes funções: caracterização do tráfego, monitoração da rede e controle do tráfego.

- Caracterização do tráfego: A caracterização do tráfego é feita através da identificação de padrões de tráfego, particularmente padrões de pico e suas variações estatísticas, incluindo o desenvolvimento de perfis de tráfego para capturar variações diárias, semanais ou sazonais. Também é feita a determinação da distribuição do

tráfego na rede, com base em fluxos, interfaces, enlaces, nós, pares de nós, caminhos e destinos. Estes dados auxiliam ainda no planejamento da capacidade, juntamente com a estimativa da carga de tráfego de acordo com as classes de serviço nos diferentes roteadores e na rede. Adicionalmente é possível observar as tendências de crescimento do tráfego de forma a prever a demanda futura.

- Monitoração da rede: A determinação do estado operacional da rede, incluindo detecção de falhas é uma necessidade básica para qualquer rede. Para redes que oferecem garantias de qualidade de serviço é necessário ainda a monitoração da continuidade e da qualidade dos serviços, assegurando assim que os objetivos de QoS estão sendo atingidos pelas diversas classes de tráfego e verificando o desempenho dos serviços prestados. A monitoração também serve como um meio de seccionalizar questões de desempenho apresentadas pelos clientes e avaliar a efetividade das políticas de engenharia de tráfego. Estas ações podem ser baseadas no uso dos dados históricos de desempenho.
- Através da monitoração da rede é possível ainda verificar o cumprimento de acordos de interconexão entre provedores de serviço, medindo e monitorando o fluxo de tráfego que atravessa os enlaces de interconexão e os roteadores de borda. Isto inclui a estimativa do tráfego inter e intradomínio, assim como o tráfego originado, terminado ou em trânsito entre os pares. Observe que os provedores geralmente não divulgam detalhes do tráfego interno ao seu sistema autônomo.
- Controle do tráfego: A otimização adaptativa do desempenho da rede em resposta a eventos, como por exemplo o rerroteamento para contornar congestionamentos ou falhas, é a principal utilização do controle do tráfego. Para redes com QoS o controle do tráfego dá suporte ao controle de admissão baseado em medições, ou seja, pela predição da demanda futura do agregado dos fluxos existentes é tomada a decisão de admissão de novos fluxos.
- Um exemplo da utilização de medições em mecanismos de controle de tráfego é a configuração de mecanismos de policiamento em resposta às medidas de carga de tráfego e de desempenho. O operador da rede pode descartar seletivamente fluxos de baixa prioridade para melhorar o desempenho dos fluxos de alta prioridade e manter condições de QoS mais restritas. Outro caso pode ser o uso de resultados de medições para realimentar decisões de roteamento tomadas pelos protocolos IGP, por exemplo para reajustar os pesos dos enlaces (LAI, 2003a).

3.3. Medição Ativa x Medição Passiva

Existem várias abordagens para medição das características das redes. As duas abordagens mais comuns são medição passiva e medição ativa. Na medição ativa é injetado tráfego sintético na rede entre os pontos de medição. A avaliação deste tráfego e a medição de suas características permite a obtenção de informações sobre a rede, tais como retardo unidirecional e latência. Já para a obtenção passiva de medidas é observado o tráfego da rede, sem interferências. Ambas possuem vantagens e dada a complementaridade dos dois mecanismos é muito útil explorar meios de obter a melhor combinação. Uma possibilidade é utilizar os pacotes de teste da medição ativa para agendar a realização de medições passivas para obtenção das medidas apropriadas nos pontos apropriados ao longo do caminho durante a execução da medição ativa. Quando esta se completa então as medições passivas podem ser interrompidas, reduzindo então a coleta de dados desnecessários. Através da comparação e do contraste entre as medições ativa e passiva é possível a co-validação das diferentes medidas obtendo assim informações muito mais detalhadas sobre o experimento.

Uma vez que uma máquina realizando medições ativas geralmente está dedicada à atividade de geração/recepção do tráfego de teste, em muitas situações pode ser utilizado um *hardware* modesto, por exemplo um PC executando um sistema Unix. Uma exceção é a geração a altas taxas (gigabps e acima), quando mesmo para a obtenção de medidas simples devem ser utilizados instrumentos de maior poder computacional. Uma máquina realizando medições passivas por outro lado normalmente possui outras funções e deve lidar com todo o tráfego que passa pelo ponto de medição. Esta tarefa, que pode ser agravada pelo tipo de medição realizada (p.ex. coleta de informações de todos os fluxos que atravessam uma interface), torna-se cada vez mais difícil com o aumento da taxa de transmissão.

3.3.1. Medição Passiva

Medições passivas são obtidas observando o tráfego normal da rede, ou seja não perturbam a rede. Isto pode ser feito utilizando equipamentos especialmente desenvolvidos para este propósito, como um *sniffer*, ou funções embutidas em equipamentos como roteadores, *switches* ou mesmos equipamentos de acesso a rede e interface com o usuário. Exemplos destas funções embutidas incluem RMON – *Remote Monitoring* (WALDBUSSER, 1995) e SNMP – *Simple Network Management Protocol* (CASE, 1990). Os equipamentos são periodicamente acessados através de um *polling* realizado pela estação de gerenciamento e os dados coletados são transferidos para uma base de dados centralizada. Estas informações permitem então inferir o desempenho e o estado da rede. Os padrões RMON e SNMP

armazenam os dados dos equipamentos na MIB – *Management Information Base* (MCCLOGHRIE, 1991), uma base de dados local padronizada que provê informações de gerenciamento, tornando possível a utilização de um único sistema de gerência para equipamentos de diferentes fabricantes e diferentes tecnologias.

A abordagem passiva não injeta tráfego na rede para obtenção das medidas, ou seja, é medido o tráfego real. Entretanto, o mecanismo de consulta necessário para coleta dos dados e os alarmes e avisos enviados pelos equipamentos geram tráfego na rede, que pode ser considerável. Além disto a quantidade de dados obtidos pode ser substancial, especialmente quando é feita análise de fluxos e captura de informação de todos os pacotes, como é o caso da sua aplicação mais comum: medir fluxos de tráfego, ou seja, contar o número de pacotes e bytes que atravessam roteadores e enlaces entre fontes e destinos especificados.

Uma vez que, com esta abordagem, é possível a visualização de todos os pacotes na rede, podem surgir questões sobre a privacidade ou a segurança da forma como é feito o acesso e a proteção aos dados obtidos.

Outro problema potencial da abordagem passiva é o fato de que as medidas se baseiam no tráfego que flui através do enlace que está sendo medido. Caso este tráfego não possua o volume e/ou outras características necessárias para a medição passiva, existe a possibilidade de que as medidas obtidas não sejam confiáveis.

3.3.2. Medição Ativa

A abordagem ativa de medição se baseia na capacidade de injetar pacotes de teste na rede ou enviar pacotes para servidores e aplicações, observando seu progresso na rede e medindo o serviço obtido. Uma vez que é criado tráfego extra, este tráfego e seus parâmetros são artificiais. O volume e outros parâmetros do tráfego introduzido devem ser totalmente ajustáveis de forma que pequenos volumes de tráfego sejam suficientes para obter medidas significativas.

Por outro lado a medição ativa permite o controle explícito da geração de pacotes para criar os cenários de medição. Isso inclui o controle da natureza do tráfego gerado, as técnicas de amostragem, a temporização, freqüência, escalonamento, tipo e tamanho dos pacotes de forma a emular várias aplicações. Também pode-se controlar estatísticas de qualidade, o caminho e a função escolhida para serem monitorados.

A medição ativa facilita a emulação de cenários e simplifica a verificação do atendimento aos requisitos de qualidade de cada serviço, providos através de mecanismos de QoS, ou dos acordos de nível de serviço (SLAs). Obviamente as medições ativas podem

distorcer o comportamento da rede, afetando assim os resultados das medições (COTTRELL, 2001).

3.4. Medição de Ida e Volta x Medição Unidirecional

Muitos caminhos na Internet são assimétricos, ou seja, a seqüência de roteadores atravessados por um pacote transmitido de uma origem para um destino é diferente da seqüência atravessada no retorno deste mesmo destino para esta mesma fonte (PAXSON, 1996; PAXSON, 1997). Na presença de caminhos assimétricos medições tradicionais de ida e volta por exemplo, *round trip time meters* (rttm) como *ping* e *traceroute*, medem o desempenho de dois caminhos diferentes em conjunto. É possível que estes caminhos diferentes atravessem diferentes provedores de serviço e até mesmo tipos de redes diferentes. Mesmo no caso em que o caminho é simétrico, a carga, e portanto o desempenho, pode ser extremamente diferente nas duas direções.

Em redes que oferecem serviços com qualidade assegurada, o provisionamento em uma direção pode ser diferente do provisionamento na direção reversa, diferindo portanto as garantias de cada caminho. Medições unidirecionais permitem mensurar estas diferentes entidades separadamente e verificar as garantias de ambas. O principal exemplo é a medição do retardo unidirecional – *one way delay meter* (owdm).

Entretanto para a realização de medições unidirecionais é necessário a utilização de um relógio externo para a sincronização das máquinas. A precisão desta referência externa varia conforme a natureza da rede que está sendo avaliada. Tipicamente para redes locais ou para redes de alta capacidade deve ser da ordem de microssegundos, uma vez que valores típicos de *round trip time* para estas redes variam de centenas de microssegundos (3 ms LAN 100 Mbps Ethernet (NETPREDICT, 2004)) a dezenas de milissegundos (28 ms *Backbone* Internet Embratel (EMBRATEL, 2004), 90 ms Enlace MCI Transatlântico entre Londres e Nova York (MCI, 2004)). Esta exigência se torna cada vez mais importante com o aumento da capacidade da rede que está sendo medida e com a sensibilidade das novas aplicações, em especial as aplicações multimídia de tempo real. Uma forma de prover uma referência de sincronismo confiável é a utilização de um GPS, entretanto esta adição introduz uma série de custos extras. Além do preço do equipamento em si, em torno de centenas de dólares, existe o custo associado à necessidade de instalar uma antena em um local aonde haja visada para os satélites e um cabo até o monitor. Isto não só torna mais cara e complexa a instalação como introduz um caminho de cobre entre o telhado e a máquina aumentando a necessidade de proteção contra sobrecargas elétricas.

Percebe-se assim uma das vantagens da utilização de medidas de ida e volta, a facilidade para sua obtenção. Diferentemente das medidas unidirecionais, é possível com freqüência realizar algum tipo de medida do retardo de ida e volta sem a necessidade de instalar qualquer hardware ou software específico para medição no destino. São bem conhecidas várias abordagens, incluindo o uso do ICMP (POSTEL, 1981a) ou do TCP (POSTEL, 1981b), como por exemplo *ping* e *traceroute*. Entretanto algumas abordagens podem introduzir uma incerteza maior no tempo de resposta do destino.

A outra vantagem é a facilidade de interpretação dos resultados. Em algumas circunstâncias o tempo de ida e volta é de fato a grandeza de interesse. A sua dedução a partir do retardo unidirecional e de estimativas do tempo de processamento é um método menos direto e potencialmente menos preciso.

Portanto, é interessante considerar o que pode estar sendo perdido quando não são feitas medidas unidirecionais. A maioria dos caminhos na Internet são assimétricos entretanto para a maior parte das aplicações, especialmente aquelas que utilizam o TCP como protocolo de transporte, não faz diferença se o retardo é simétrico ou assimétrico, ou seja, é o tempo total de ida e volta que influenciará no desempenho da aplicação. Entre estas aplicações estão incluídas web, FTP e telnet. Uma exceção importante é voz sobre IP. Enlaces que possuem retardo altamente assimétrico podem tornar possível o tráfego de voz em uma direção e impossível na outra. Presumivelmente outras aplicações multimídia de tempo real que não possuem uma "realimentação", como vídeo, também são afetadas pelo retardo assimétrico.

Em resumo, medidas de ida e volta (RTT) são mais fáceis de serem obtidas e não necessitam de nenhum equipamento externo para sincronização dos monitores, porém perdem-se informações sobre a rede e seu desempenho. Apesar disto estas medidas podem ser aceitáveis caso a investigação se limite às aplicações similares às atualmente em uso e não haja prospecção de novas aplicações mais exigentes e/ou novas tecnologias de rede de maior capacidade.

3.5. Métricas e medidas

De acordo com o tipo e a utilização das grandezas, podem ser definidos dois tipos de medições: medições relativas à utilização de recursos de rede e medições de tráfego relativas ao desempenho. Para cada tipo deve ser especificado um conjunto de pontos de medição de forma a criar segmentos de rede específicos para os propósitos de medição. Um ponto de medição pode ser uma fronteira física entre o nó e o enlace adjacente, ou uma interface lógica entre duas camadas de protocolos em uma pilha de protocolos.

Medições relativas à utilização de recursos

Este tipo de medição utiliza um conjunto de métricas compreendendo as diferentes utilizações para cada recurso da rede, como por exemplo capacidade de processamento e memória dos roteadores, enlace e buffers, pelos diferentes tipos de tráfego: tráfego de controle (por exemplo controle de roteamento), tráfego de sinalização e tráfego de usuário das diferentes classes de serviços.

A quantidade de tráfego de controle e sinalização que trafega na rede é função de vários fatores, entre eles o tamanho e a topologia da rede, os protocolos de controle e sinalização utilizados, a quantidade de tráfego de usuário transportado, a quantidade de eventos de falha e etc..

Estas métricas de utilização de tráfego de controle e sinalização auxiliam o dimensionamento e o compartilhamento apropriado dos recursos da rede de forma que o tráfego de usuário seja adequadamente suportado.

Medições de tráfego relativas ao desempenho

Este tipo de medição é o foco deste trabalho. O principal componente da gerência do desempenho é a monitoração contínua e em tempo real da qualidade e da condição da rede e de seus vários elementos para assegurar que seja sustentado um serviço de qualidade ininterrupto. Isto requer o uso de medições ativas e passivas para coletar informações sobre o estado operacional da rede e seu desempenho. Dentre as métricas mais comuns estão latência, *jitter*, perda de pacotes e vazão. Existem vários esforços dos organismos de padronização no sentido de estabelecer um conjunto de métricas úteis e claras, de fácil entendimento e utilização por parte de usuários e operadores. Os trabalhos mais significativos são os desenvolvidos pelo ITU-T (ITUT, 2004a), recomendações das séries E (400 a 899), I (220 a 250), G (1000) e outras, e pelo IETF, RFCs e drafts do grupo de trabalho IPPM – *IP Performace Metrics* (IPPM, 2004). Existem ainda trabalhos mais antigos desenvolvidos pelo IEEE (IEEE, 2003) para as primeiras redes de dados, redes telefônicas ou mesmo para sistemas elétricos que nortearam por bastante tempo as medições em redes de telecomunicações.

3.5.1. Métricas mais comuns

Esta seção descreve as métricas mais comumente usadas para descrever o desempenho de rede. Estas métricas são em geral derivadas de definições do IEEE (IEEE, 2003) e do ITU-T (ITUT, 2004a) para redes telefônicas e para redes de dados como X.25

(ITUT, 1976), PDH (ITUT, 1988), SDH (ITUT, 1991) e ISDN (ITUT, 1993b). Devido à sua larga utilização ao longo do tempo e às adaptações feitas para atender aos novos cenários, algumas métricas não seguem mais fielmente a sua definição formal original. Embora não exista muito acordo sobre como exatamente elas são definidas é apresentada a seguir uma visão prática.

Latência

Latência, para redes de computadores é uma expressão de quanto tempo um pacote leva para ir de um ponto para outro. Porém grande parte dos provedores, por exemplo Telefónica (TELEFÓNICA, 2004) e Embratel (EMBRATEL, 2003), realiza a medição da latência enviando um pacote para um servidor remoto que é retornado para a origem. Este é o método empregado na prática pelos provedores para determinar o retardo de backbone para o cumprimento dos SLAs. Neste caso o *round-trip-time* é considerado a latência da rede, e possui os seguintes componentes:

- Tempo de transporte: O tempo que o pacote leva para ser transmitido através dos enlaces físicos que compõem o caminho através da rede,
- Tempo de enfileiramento (*queuing*): O tempo de espera nas filas internas dos roteadores, que varia de acordo com o algoritmo de escalonamento utilizado e com as políticas de QoS e policiamento adotadas,
- Tempo de retransmissão: O tempo necessário para o roteador receber o pacote na sua interface de entrada, processá-lo, ou seja, verificar se pertence a algum fluxo, agregado ou LSP, determinar a sua rota e, caso seja necessário, fazer o policiamento e condicionamento do tráfego, e encaminhar para a interface de saída. Este componente em conjunto com o tempo de enfileiramento descreve o tempo que o pacote leva para atravessar os roteadores entre os enlaces da rede,
- Tempo de resposta do servidor: O tempo requerido pelo servidor para processar um pacote entrante e gerar um pacote de resposta.

Valores típicos de latência variam de centenas de microssegundos, em uma rede local, a centenas de milissegundos, como é o caso de enlaces via satélite. A aplicação comumente usada para medir a latência pelos provedores é o ping, embora a sua validade seja questionável uma vez que os roteadores encaminham os demais pacotes prioritariamente em relação à resposta aos pacotes *echo* ICMP. Assim o valor de latência obtido pelo ping pode não retratar o que será experimentado por outras aplicações, principalmente quando a rede estiver muito carregada. A medida de latência resultante é uma aproximação do desempenho

da rede e não uma medida verdadeira do retardo da rede. Apesar disso esta é uma métrica de desempenho largamente utilizada.

A latência da rede não é uma medida fixa e varia de acordo com as condições da rede. A carga do servidor, o congestionamento da rede e mudanças de roteamento influenciam o valor da latência. Para detectar variações na latência é comum produzir gráficos diários mostrando a latência média para pequenos intervalos, por exemplo de um a cinco minutos. Estes gráficos freqüentemente mostram variações diurnas, com a latência aumentando durante os períodos de maior utilização do dia. Aumentos ou reduções repentinas, causadas por mudanças de rotas, ataques à segurança da rede ou simplesmente rajadas de tráfego, também podem ser mostradas.

Perda de Pacotes

A perda de pacotes na rede é a fração dos pacotes perdidos no trânsito entre origem e destino durante um intervalo de tempo especificado, expressa como uma porcentagem dos pacotes enviados para o destino durante este intervalo. A perda de pacotes pode variar conforme o congestionamento do caminho até o valor máximo definido para o serviço ou, caso não haja nenhuma definição, até que seja impossível recuperar a informação enviada. Altas taxas de perda podem tornar a rede inviável. Porém uma perda moderada de pacotes não é por si mesma uma indicação de falha de rede, uma vez que alguns serviços podem tolerar a perda de alguns pacotes e estes na maioria das vezes são reenviados pelo TCP que usa a perda de pacote como um sinal indicando a necessidade de enviar os dados a uma taxa mais baixa. Assim, muitos serviços irão continuar a operar efetivamente mesmo em face de alguma perda de pacotes.

Um segundo ponto particularmente importante é o fato de que o TCP utiliza a detecção de pacotes perdidos como um meio de perceber o congestionamento da rede. Assim é esperado uma perda ocasional de pacotes em fluxos TCP.

Vazão

Vazão é a taxa a que os dados são enviados através da rede, normalmente expressa em bits por segundo (bps), bytes por segundo (Bps) ou pacotes por segundo (pps). Na maioria das vezes esta métrica se refere à taxa total de transferência de dados para todo o tráfego sendo transportado, porém também pode ser útil medir a vazão a uma granularidade mais fina, por exemplo para transações web, para voz sobre IP, para destinos específicos e etc..

A vazão é medida continuamente pela contagem de bytes transportados durante um intervalo de tempo especificado. A escolha deste intervalo deve ser feita cuidadosamente

pois intervalos longos irão incorporar as rajadas, possíveis apenas por breves períodos, ao valor medido. Por outro lado intervalos pequenos implicam numa taxa de coleta de dados maior e podem medir as rajadas de forma exagerada. Da mesma forma que para a latência são produzidos gráficos diários mostrando a vazão média para pequenos intervalos para detectar suas variações. Entre as causas das variações apresentadas pela vazão se encontram os períodos de maior utilização do dia, mudanças de rotas, ataques à segurança da rede ou rajadas de tráfego.

Capacidade

A capacidade do enlace é a vazão máxima que um caminho pode prover para uma aplicação quando não há outro tráfego competindo pelos recursos (*cross traffic*). A medição da capacidade é crucial para detecção de problemas, calibração e gerenciamento de caminhos.

A capacidade de um caminho é determinada pelo enlace de menor capacidade (*narrow link*). A capacidade de um enlace é determinada pelo seu meio físico e pela tecnologia de transmissão utilizada. Por exemplo a capacidade teórica de enlaces utilizando fibras óticas é da ordem de Terabits por segundo, entretanto as tecnologias de transmissão ótica atualmente em uso (WDM (ITUT, 1998a), CWDM (ITUT, 2002c), DWDM (ITUT, 2002d)) limitam a vazão máxima a Gigabits por segundo.

Utilização do Enlace

Os enlaces possuem uma taxa máxima de transmissão de dados, conhecida como taxa de acesso, taxa nominal que é a capacidade do enlace. A utilização do enlace durante um intervalo de tempo específico, é simplesmente a vazão deste enlace durante o intervalo determinado, expressa como uma porcentagem da sua taxa de acesso.

Algumas tecnologias possuem velocidades máximas bem definidas em seus enlaces, como por exemplo enlaces PDH E1/E3 (2/34Mbps) (ITUT, 1988). Outros tipos de enlaces, como por exemplo PVCs Frame Relay, possuem além da taxa de acesso uma segunda taxa, a CIR (*Committed Information Rate*), que é a taxa de transmissão de dados que está sendo paga pelo cliente. Porém é permitido que o tráfego ultrapasse a CIR por curtos períodos, ou seja, o enlace irá transportar pequenas rajadas sem perdas. A utilização destes enlaces deve ser calculada como uma fração da CIR e não da taxa de acesso.

Banda disponível

A banda disponível é a vazão máxima que um caminho pode prover para uma aplicação, dada a atual carga de tráfego do caminho, ou seja, a banda disponível sob uma

determinada utilização do enlace ou do caminho. Medir a banda disponível é de grande importância para a predição do desempenho fim a fim de aplicações, para a seleção dinâmica de caminhos, para engenharia de tráfego e para a seleção da classe de serviço. A banda disponível de um caminho é determinada pelo enlace com a menor banda sem utilização(*tight link*).

Disponibilidade

Apesar de muitas descrições de serviços não proverem uma definição explícita de disponibilidade, a sua utilização implícita é similar ao que o ITU-T (ITUT, 2004) usa na sua recomendação E.800 (ITUT, 1994) como definição de disponibilidade, ou seja, "a habilidade de um item de estar em um estado capaz de realizar a função requerida em um dado instante de tempo, ou em qualquer instante dentro de um dado intervalo, assumindo que os recursos externos, se necessários, estão sendo providos".

Do ponto de vista do usuário, disponibilidade em um intervalo de tempo especificado é a porcentagem do intervalo durante a qual o sistema esteve disponível para uso normal. Porém é preciso definir o que é "estar disponível", por exemplo considere:

- Disponibilidade de serviço: como sendo capaz de enviar pacotes de um serviço especificado para uma máquina em particular e receber pacotes de resposta.
- Disponibilidade de máquina: como sendo capaz de enviar pacotes, por exemplo ping, para uma máquina em particular e receber pacotes de resposta.
- Disponibilidade de rede: como sendo capaz de enviar pacotes através de uma rede e receber pacotes de resposta.

Em cada um destes casos é possível testar a disponibilidade enviando pacotes apropriados e observando os pacotes de resposta ou a sua falta. Por exemplo para testar a disponibilidade de um serviço web basta fazer o download de páginas especificadas do servidor alvo da monitoração usando um web browser. Desta forma pode-se medir também latência, perda de pacotes e vazão. Já para testar a disponibilidade de máquina basta enviar pacotes de ping para a máquina alvo. É necessário que a máquina seja capaz de responder a pacotes ICMP. O teste de disponibilidade de rede também é feito utilizando um utilitário muito comum. Executa-se traceroute (JACOBSON, 1989) para a máquina alvo de forma a determinar a conectividade da rede alvo. Desta forma determina-se se há algum caminho na rede para alcançar a máquina alvo, porém não será necessariamente o melhor caminho em caso de falha de enlaces.

Medições como estas irão produzir também estimativas dos valores de latência e perda de pacotes para cada caso. Para cada caso é necessário decidir quais valores para

máximo de latência e de perda de pacotes são requeridos para um serviço efetivo. Caso os valores medidos estejam fora destes limites o serviço será considerado indisponível.

Esta abordagem para a definição de disponibilidade é modelada nas técnicas para medição de conectividade discutidas pelo IPPM-IETF (IPPM, 2004). Para os três casos apresentados conectividade significa a habilidade de enviar um tipo de pacote escolhido pelo usuário de uma máquina origem até o destino e receber um pacote de resposta gerado pelo destino.

Disponibilidades são usualmente relatadas como uma figura única mensal, informando a porcentagem de tempo que a rede ou o serviço esteve disponível. A causa mais comum para a perda de disponibilidade de rede são falhas de rede, por exemplo, pode haver um corte na fibra ou algum dos equipamentos de rede pode falhar. O tempo de indisponibilidade deve iniciar no momento em que a indisponibilidade da rede é detectada. Outra causa de indisponibilidade são os desligamentos programados, ou seja uma janela especificada para manutenção ou upgrades. Outras importantes grandezas relacionadas com a disponibilidade incluem:

- MTTR – Mean Time to Repair: O tempo médio, em minutos ou horas, gasto para restaurar o serviço normal após uma falha.
- MTBF – Mean Time Between Failures: o tempo médio, em horas ou dias, entre o início do serviço normal e a próxima falha.

MTTR e MTBF são métricas importantes que deveriam ser parte de qualquer fórmula de disponibilidade.

Confiabilidade

Medidas tradicionais de qualidade também medem a confiabilidade da rede, que é a probabilidade do sistema executar com sucesso as suas funções durante um período de tempo determinado, considerando que os recursos do ambiente externos, se necessários, estão sendo providos (RELIABILITY, 2003). Isto inclui a habilidade de manter, testar e suportar o sistema durante o seu ciclo de vida (IERS, 2004). Para redes de comunicação de dados a confiabilidade pode ser medida pela freqüência com que é recebido um pacote de resposta errado. Uma resposta errada em uma rede é um pacote corrompido, que não é o mesmo de não receber resposta – o que indicaria perda de disponibilidade.

Protocolos de transporte de rede provêm verificação da correção dos dados transferidos. Caso o software da camada de transporte detecte alguma corrupção, os pacotes afetados são retransmitidos de forma que o usuário percebe apenas uma baixa taxa de

transmissão. Esta taxa reduzida afeta a qualidade do serviço, possivelmente até o ponto em que o serviço deve ser considerado como indisponível.

3.5.2. Métricas IPPM – IETF

O IETF, através do grupo de trabalho IPPM – IP *Performance Metrics* (IPPM, 2004) definiu e recomenda um conjunto de métricas para avaliação do desempenho da rede. Estas métricas se destinam a definir de forma clara e sem ambigüidades as principais características que influenciam o desempenho da rede e das aplicações suportadas. Algumas aplicações são sensíveis a uma ou mais grandezas, tendo o seu desempenho degradado ou mesmo não executando se os parâmetros da rede entre as máquinas estiverem acima de valores limites. O valor preciso do limite para ser considerado excesso depende da aplicação. Quanto pior estejam as características da rede, torna- se mais difícil para os protocolos de camada de transporte sustentar altas taxas. Assim é de extrema importância definir e mensurar estas características.

Todas as métricas propostas pelo IPPM têm seu foco na rede e foram desenvolvidas considerando um pacote genérico (tipo P) usado para obtenção das medidas. Considerando que uma propriedade fundamental de muitas métricas IP é o fato de que seu valor depende do tipo de pacote usado para fazer a medição foi introduzida a noção de um tipo de pacote genérico utilizado na definição das métricas. O valor da métrica pode depender das propriedades do pacote realmente utilizado, como protocolo, número de porta (TCP ou UDP), tamanho e arranjos para tratamento especial, como empregado pelos modelos de QoS, IntServ e DiffServ, que serão tratados no capítulo 4. Portanto o pacote utilizado deve ser informado juntamente com o valor medido como parte do contexto em que a medição foi realizada.Também devem ser consideradas como parte deste contexto o caminho atravessado pelos pacotes de teste, a calibração dos erros e o limite definido para o retardo. Estão descritas a seguir as principais métricas desenvolvidas.

Conectividade

Conectividade é a base sobre a qual a Internet está construída, ou seja, é a conectividade entre as diversas máquinas e as diversas redes que permite a troca de dados na Internet. O protocolo IP é robusto em relação à manutenção da conectividade, mesmo em caso de falha de enlaces, quando ocorre o rerroteamento do tráfego através um novo caminho. Esta é uma importante característica nativa do IP, utilizada desde os primórdios da Internet. Assim, as métricas que determinam se um par de máquinas podem se encontrar uma à outra, devem formar a base do conjunto de medidas que descrevem o desempenho de uma rede IP. O IPPM

(IPPM, 2004) definiu várias métricas para conectividade, algumas das quais servem principalmente como parte integrante de outras métricas. Estão relacionadas abaixo as principais métricas para medir conectividade:

- Conectividade instantânea unidirecional: Duas máquinas origem e destino têm conectividade instantânea unidirecional em um tempo T, se um pacote transmitido pela origem no tempo T chegar ao destino. Para a maioria das aplicações, por exemplo qualquer conexão TCP, a conectividade bidirecional é mais pertinente , apesar disto a conectividade unidirecional pode ser interessante para aplicações de segurança, como para testar um *firewall*. Esta métrica entretanto serve como um bloco para construção de outras métricas.
- Conectividade instantânea bidirecional: Duas máquinas origem e destino têm conectividade instantânea bidirecional se a origem tem conectividade instantânea unidirecional para o destino e o destino tem conectividade instantânea unidirecional para a origem, ou seja origem e destino estão totalmente conectadas no tempo T.
- Conectividade unidirecional: A origem tem conectividade unidirecional para o destino durante o intervalo [T, T+dt] se para qualquer T pertencente a [T, T+dt] a origem tem conectividade instantânea unidirecional para o destino.
- Conectividade bidirecional: Origem e destino têm conectividade bidirecional entre si durante um intervalo [T, T+dT] se a origem tem conectividade unidirecional para o destino durante o intervalo e se o destino tem conectividade unidirecional para a origem durante o intervalo. Esta métrica ainda não é a necessária para definição da noção de conectividade geralmente utilizada, que requer a noção de que um pacote enviado da origem para o destino pode gerar uma resposta do destino para origem que irá alcançar a origem, uma vez que a duração do intervalo pode não ser suficiente para origem e destino responderem aos pacotes enviados pela outra máquina. Esta deficiência motivou a próxima métrica.
- Conectividade bidirecional temporal: Esta métrica define a noção de conectividade geralmente utilizada, ou seja, a origem pode enviar um pacote para o destino que encaminha uma resposta. Uma vez que muitas aplicações utilizam diferentes tipos de pacotes em cada uma das direções da conexão esta métrica pode ser utilizada nestas condições. (MAHDAVI, 1999).

Retardo Unidirecional e Perda Unidirecional de Pacotes

A obtenção de medidas unidirecionais entre origem e destino é útil por diversas razões, conforme discutido na seção 3.3. A determinação do retardo e da perda de pacotes unidirecionais são úteis em especial pelas indicações que provêem sobre a rede:

O valor mínimo do retardo unidirecional provê uma indicação do retardo devido apenas ao tempo de propagação e transmissão e do retardo que será experimentado quando o caminho estiver com baixa utilização. Já valores acima do mínimo provêm uma indicação do nível de utilização do caminho.

A sensibilidade de aplicações de tempo real e de protocolos de camada de transporte à perda de pacotes se torna especialmente importante quando produtos que consomem muita banda e possuem alto retardo devem ser suportados.

Além da assimetria dos caminhos em redes IP, a utilização de métricas unidirecionais em vez de métricas de ida e volta é motivada também pelo fato de que o desempenho de algumas aplicações pode depender em grande parte do desempenho em uma direção. Por exemplo a transferência de arquivos usando FTP pode depender mais do desempenho na direção em que os dados fluem do que na direção na qual são enviados as confirmações. Já para redes que implementam qualidade de serviço a assimetria se reflete principalmente no provisionamento de caminhos que assegurem garantias de QoS em ambas as direções, seja para implantação de um nova rota ou para o contorno de pontos em condição crítica como falhas e congestionamentos.

O retardo unidirecional é definido como o intervalo de tempo dT entre o envio do primeiro bit de um pacote pela fonte (T) e o recebimento do último bit do pacote pelo destino (T+dT). Quando o destino não recebe o pacote, o retardo é indefinido, informalmente é considerado infinito (ALMES, 1999a).

A perda de pacotes unidirecional entre uma fonte e um destino a um tempo T é 0, caso o pacote cujo primeiro bit foi enviado no tempo T seja recebido no destino. Caso o pacote não seja recebido o valor da métrica é 1. Ou seja, a perda de pacotes unidirecional é 0 exatamente quando o retardo unidirecional é um valor finito, e 1 quando o retardo é indefinido. (ALMES, 1999b)

Se o pacote chega corrompido é contado como perdido, uma vez que pode não ser viável identificar o pacote, caso a corrupção esteja no cabeçalho IP, ou caso a corrupção esteja no payload, o pacote pode não possuir todas as informações necessárias à metodologia de medição. Mesmo pacotes corrompidos em outras partes são considerados perdidos para evitar

inconsistências. Se o pacote chega duplicado é contado como recebido. Se o pacote é fragmentado e por qualquer razão não for remontado é considerado perdido.

Erros e incertezas nos métodos de medição unidirecionais são fortemente influenciados pelas incertezas dos relógios de origem e destino. Os relógios devem estar sincronizados e qualquer erro de sincronização irá contribuir no erro da medida do retardo e conseqüentemente também da perda. A resolução de ambos os relógios também contribui para o erro, pois seu valor será adicionado às medidas obtidas. Outras fontes de erros e incertezas para perda são o limite de perda de pacotes, que está relacionado à sincronização, e a limitação de recursos da interface de rede ou do software do instrumento de recepção, que podem causar o descarte de pacotes fazendo com que o pacote de teste seja considerado como perdido mesmo tendo alcançado seu destino.

Retardo de Ida e Volta (*Round Trip Time*)

Assim como as medidas unidirecionais, a medição do retardo de ida e volta pode trazer importantes indicações sobre o desempenho da rede, indicando o nível de utilização ou o retardo intrínseco da rede, conforme seu valor seja mínimo ou não. A medição do retardo de ida e volta apesar de várias fraquezas já mencionadas é de mais fácil implementação e utilização. Na maioria das vezes não é preciso nenhuma instalação ou configuração especial no destino. Mesmo as ferramentas utilizadas pela origem são bem conhecidas e documentadas, de larga utilização há muitos anos, o que facilita muito a realização das medições e a interpretação dos seus resultados.

O retardo de ida e volta é o intervalo de tempo dT entre: o envio pela origem do primeiro bit de um pacote em um tempo T, o recebimento e o retorno imediato do pacote pelo destino, e o recebimento pela origem do último bit do pacote em um tempo T+dT. O retardo é indefinido, informalmente considerado infinito, caso o pacote não seja recebido pelo destino ou o pacote de resposta não seja recebido pela origem.

A medição do retardo pode ser iniciada tanto pela origem como pelo destino, mantendo-se a mesma métrica. Esta ambigüidade é intencional e é o preço a ser pago para evitar a definição de duas métricas semelhantes. Para a realização da medição a origem deve possuir um conhecimento preciso do “time-of-day” de forma a poder tirar conclusões úteis a respeito do estado da rede em um tempo T.

Da mesma forma que para o retardo unidirecional, pacotes corrompidos ou que não podem ser remontados são considerados como não recebidos. Pacotes duplicados são considerados recebidos e o primeiro a chegar à origem é utilizado para determinar o retardo. (ALMES, 1999c).

Variação do Retardo (Jitter)

Esta métrica é baseada na diferença do retardo unidirecional de pacotes selecionados. A diferença dos retardos é chamada Variação do Retardo de Pacotes IP (IPDV – IP Packet Delay Variation). Esta métrica é valida para medidas entre duas máquinas cujos relógios estejam sincronizados ou não.

Um importante uso da variação do retardo é o dimensionamento de buffers para reprodução de aplicações que requerem uma entrega regular de pacotes, como por exemplo reprodução de voz e vídeo. Outro uso para esta métrica é a determinação da dinâmica de filas em uma rede ou um roteador, uma vez que mudanças na variação do retardo podem estar relacionadas a mudanças no tamanho das filas em um dado enlace ou combinação de enlaces.

Este tipo de métrica é especialmente robusta com respeito a diferenças e variações nos relógios das duas máquinas. Isto permite o seu uso mesmo se as duas máquinas que suportam as medições não estiverem sincronizadas. Se como uma primeira aproximação o erro que afeta a primeira medida do retardo unidirecional for o mesmo que afeta a segunda medida, eles serão cancelados durante o cálculo do IPDV. O erro residual relacionado aos relógios é a diferença dos erros, supondo que haja mudanças entre o momento em que foi feita a primeira medição e o momento em que foi feita a segunda. Assim, a precisão relatada é freqüentemente comparável à que pode ser encontrada com relógios sincronizados, sendo da mesma ordem de magnitude dos erros de sincronização.

Precisão e resolução entretanto são questões importantes. As recomendações feitas para a medição do retardo unidirecional também se aplicam neste caso, com uma consideração adicional sobre resolução, uma vez que neste caso a incerteza introduzida é o dobro da incerteza na medição do retardo. Erros introduzidos por estes efeitos são freqüentemente maiores do que os introduzidos pelos relógios (skew e drift) (DEMICHELIS, 2002).

3.6. Conclusão

As métricas tradicionalmente utilizadas, baseadas em padrões do IEEE (IEEE, 2003) e do ITU-T (ITUT, 2004), e as métricas desenvolvidas pelo IETF (IETF, 2004) para redes IP, muitas vezes lidam com a mesma grandeza ainda que com enfoques diferentes. Isto faz com que freqüentemente haja uma falta de entendimento sobre o que está sendo medido e o significado dos resultados das medições. Assim é difícil assegurar que clientes e empresas fornecedoras de serviços de telecomunicações e Internet possuam a mesma percepção sobre o

que é garantido e o que é fornecido em termos de qualidade de serviço, bem como o estabelecimento e o cumprimento de SLAs – *Service Level Agreement*.

As métricas e metodologias de medição descritas neste capítulo demonstram a importância da existência de métricas bem definidas, identificando inequivocamente os parâmetros de qualidade e desempenho de redes, bem como o esforço feito pelos organismos de padronização e pela comunidade internacional de pesquisa para o seu desenvolvimento. Entretanto também fica clara a defasagem entre o desenvolvimento das tecnologias de encaminhamento de dados, seja de comutação, roteamento ou tunelamento, e das tecnologias de medição para redes IP.

Capítulo 4
Qualidade de Serviço - QoS

4.1. Introdução

Neste capítulo serão abordados os principais mecanismos utilizados para assegurar a qualidade dos serviços oferecidos por redes IP, ou seja, o tratamento diferenciado de parte dos pacotes. A garantia de qualidade de serviço não é uma característica do IP, tendo sido desenvolvida apenas *a posteriori*, visando permitir a utilização da Internet para tráfego com requisitos específicos, como voz e vídeo. Os usuários buscam assegurar que o seu tráfego crítico ou multimídia não será descartado, retardado ou degradado por causa de congestionamentos ou outros problemas na rede.

Projetos de novas redes de alta capacidade com qualidade de serviço, como o programa de QoS da Internet2 (INTERNET2, 2004) e do GÉANT (LIAKOPOULOS, 2003), realizaram um considerável esforço e investimento no *design*, teste e promoção de serviços de emulação de circuitos em redes IP, ou seja, serviços *premium* com garantias de qualidade estritas. Porém o desenvolvimento e a implantação destes serviços em redes públicas tem sido frustrados não apenas devido à pouca demanda, mas também por falta de suporte por parte dos fabricantes de equipamentos e outras barreiras logísticas, financeiras e organizacionais. Aqui estão alguns dos problemas desencorajadores, sumarizados de um artigo (TEITELBAUM, 2001b) escrito por Teitelbaum e Stanislav Shalunov, pesquisadores da Internet2.

- A garantia de serviço pressupõe que todos os roteadores ao longo da rota suportem protocolos de QoS. Garantias reais demandariam quantidades enormes de provedores de serviço internet (ISPs) concordando em colocar e espalhar por suas redes os protocolos para assegurar a QoS, simultânea e coordenadamente. A Internet não funciona assim.
- ISPs precisariam cooperar de jeito a ajudar seus competidores mais do que a eles mesmos. Em outras palavras, um ISP que estivesse prometendo serviços *premium* como forma de ganhar clientes, teria que pedir então a ISPs competidores que o ajudassem a cumprir suas promessas.
- Novos e complexos mecanismos de pagamento teriam que ser postos em prática.

- Sistemas complexos de monitoramento teriam que ser dispostos ao longo das rotas de forma a obter informações para assegurar aos clientes que estão obtendo aquilo pelo que estão pagando.
- Uma vez que ISPs comecem a oferecer serviços com garantia de qualidade, ficam estimulados a degradar o serviço normal como maneira de levar os clientes a pagar mais pelo serviço *premium.* Por outro lado usuários maliciosos ficam estimulados a modificar o tráfego oferecido à rede de forma a obter mais ou melhores serviços pelo mesmo preço, reforçando assim a necessidade de policiamento, autenticação e condicionamento do tráfego.

Esta situação levou o grupo de QoS da Internet2 a uma mudança drástica na forma de lidar com a priorização de pacotes e conseqüentemente a implementação de QoS. Ao invés de levar os usuários a competir por tratamento preferencial, sugeriram que eles voluntariamente aceitassem um *status* mais baixo, um tratamento degradado. Foram adotados dois serviços dentro desta linha de atuação: o serviço *scavenger*, ou cata-lixo, e o serviço "melhor esforço alternativo".

O serviço cata-lixo utiliza a banda residual, que "sobra" na rede após atendimento ao melhor esforço, para encaminhar o tráfego a baixíssima prioridade. É ideal para aplicações que não são sensíveis ao retardo.

O serviço melhor esforço alternativo (ABE – *Alternative Best Effort)* (ABE, 2004) foi pensado tendo em vista aplicações interativas, que requerem baixos retardos mas podem tolerar perdas. No ABE, o aplicativo pede que pacotes sejam descartados em caso de congestionamento, ao invés de enfileirados. Dessa forma, ABE ajuda os aplicativos a evitar o *jitter* ao mesmo tempo em que reduz o congestionamento para todo o tráfego. (ORAM, 2002)

4.2. QoS em redes IP

Os mecanismos para oferecer QoS e assegurar o correto tratamento do tráfego não são nativos da tecnologia IP, tendo sido desenvolvidos após a ampla utilização do IP pelo mercado. Esta aliás foi a grande motivação para o desenvolvimento de serviços com qualidade garantida e a grande dificuldade encontrada para a sua implementação em larga escala.

O IETF desenvolveu dois modelos, IntServ e DiffServ, que utilizam os mesmos componentes básicos para oferecer diferentes formas de tratamento da qualidade de serviço.

Componentes do tratamento da qualidade de serviço

Os principais componentes do tratamento da QoS, utilizados em todas as técnicas que serão abordadas, estão divididos entre o plano de dados e o plano de controle. No plano de dados são tratados os pacotes individualmente, sendo uma tendência evitar grandes modificações no protocolo de forma a manter uma compatibilidade mínima com as redes IP já existentes. No plano de controle estão as maiores mudanças, uma vez que a noção de fluxo (*stream*) de dados não é nativa do IP.

- Plano de dados:
  - Escalonar pacotes nas filas de espera (WFQ – *Weighted Fair Queueing*).
  - Tratar congestionamento nas filas de espera (WRED – *Weighted Random Earlier Detection*, tail drop).
  - Condicionamento (classificação, marcação, shaping e policiamento).
  - Mecanismos fim a fim.
- Plano de controle
  - Sinalização (fluxo elementar ou agregado).
  - Controle de admissão para reserva de recursos (fluxo elementar ou agregado).

O tratamento de congestionamento pode ser dividido em preventivo, *shaping/policing* e RED/WRED, e corretivo , por exemplo o controle fim a fim TCP que tenta reduzir o tráfego que entra na rede: *slow start* e *congestion avoidance* (diminuição da janela de transmissão de pacotes em caso de perda).

O oferecimento de um serviço com qualidade garantida gera a necessidade de que este serviço seja mensurável e sustentável. O provisionamento deste serviço vai requerer uma visão coerente da rede e não apenas dos equipamentos, como é correntemente implementado na maioria das redes. De forma similar assegurar a qualidade de serviço no nível de transporte requer uma engenharia de tráfego com uma visão mais completa da rede, incluindo informações dinâmicas sobre congestionamento e conectividade.

4.3. Modelos de qualidade de serviço em redes IP

Os principais modelos que foram desenvolvidos pelo IETF são: serviços integrados (IntServ) e diferenciados (DiffServ). A principal diferença entre os modelos IntServ e DiffServ é o nível de granularidade em que as ações de condicionamento do tráfego são feitas. O IntServ, que possui uma forte influência do ATM e de redes de comutação de circuitos, oferece um nível fino de granularidade – suas ações são baseadas nos fluxos

individuais de dados. Esta fina granularidade torna possível a existência simultânea de conexões de áudio e vídeo de alta qualidade e de transferência de dados a alta velocidade. O IntServ provê meios de oferecer QoS real, fim a fim. Entretanto, existem muitas complicações com esta abordagem fim a fim. As redes devem ser capazes de manter informações sobre as solicitações de recursos de cada fluxo e os usuários devem ser capazes de passar para a rede informações sobre a utilização de recursos. O DiffServ visa resolver este primeiro problema no núcleo das redes através da agregação da informação dos fluxos. O segundo problema pode ser resolvido através da medição do tráfego no controle de admissão.

O DiffServ oferece uma granularidade de diferenciação mais grossa. Os fluxos são agregados para tornar o processamento o mais fácil possível no núcleo da rede, aonde a quantidade de fluxos individuais é enorme. Todo o pré-processamento necessário para a agregação é feito na borda da rede. A qualidade oferecida pelo DiffServ depende do provisionamento da rede e da distribuição do tráfego dentro da rede. Neste processo os pontos de acesso a uma rede DiffServ possuem um papel essencial.

4.3.1. Integrated Services – Visão Geral

Modelo de referência

A primeira premissa deste modelo é que os recursos, por exemplo banda, devem ser explicitamente gerenciados para atender ao requisitos das aplicações. Isto implica que reserva de recursos e controle de admissão são partes essenciais do serviço.

A figura 4.1 ilustra a implementação do modelo de referência para roteadores IntServ.

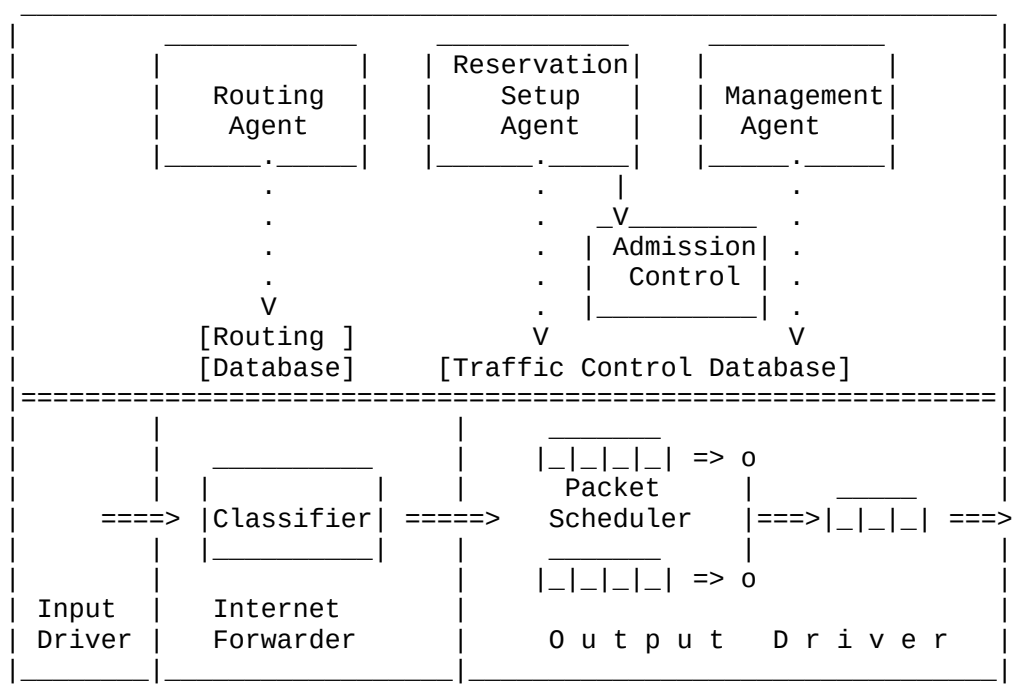


Figura 4.1 Roteador IntServ - modelo de referência (BRADEN, 1994)

Ao assegurar garantias de serviços a fluxos de dados individuais, pretende-se prover o desempenho razoável da aplicação. Estas garantias, que associam qualidade de serviço aos fluxos individuais, são direcionadas por requisitos econômicos ou de compartilhamento de recursos. O IntServ é voltado quase exclusivamente para garantir o tempo de entrega dos pacotes. Ou seja, o retardo por pacote é a métrica central utilizada pela rede para garantir qualidade de serviço. De forma ainda mais restritiva é assumido que apenas os valores máximo e mínimo do retardo são relevantes.

O modelo de reserva descreve como uma aplicação pode reservar recursos e negociar um nível de qualidade de serviço. O modo mais simples é aquele em que a aplicação solicita um nível em particular e a rede atende ou recusa. Freqüentemente esta negociação pode ser mais complexa. Muitas aplicações são capazes de utilizar uma faixa de níveis de QoS.

4.3.2. Differentiated Services – Visão Geral

Modelo de referência

O desenvolvimento do DiffServ considerou o atendimento aos seguintes requisitos:

- Acomodar uma grande variedade de serviços fim a fim ou dentro de uma rede em particular.
- Permitir dissociar o serviço da aplicação específica em uso.
- Trabalhar com as aplicações existentes sem a necessidade de mudanças nas APIs ou modificações nos *softwares*, assumindo o desenvolvimento apropriado dos classificadores, marcadores e outras funções de condicionamento do tráfego.
- Dissociar o condicionamento do tráfego do provisionamento do serviço dos modos de encaminhamento (*forwarding behaviors*) implementados no núcleo da rede.
- Não depender de aplicação de sinalização nó a nó.
- Requerer apenas um pequeno conjunto de modos de encaminhamento, cuja complexidade de implementação não domine o custo dos equipamentos de rede e que não introduza gargalos em implementações futuras de sistemas de alta velocidade.
- Evitar a manutenção de descritores de estado por fluxo ou por cliente nos nós do núcleo da rede.
- Utilizar apenas classificação de agregados no núcleo da rede.

A arquitetura DiffServ é baseada em um modelo simples, no qual o tráfego entrante é classificado e possivelmente condicionado nas bordas da rede e associado a diferentes tipos de agregados (*behavior agregates*). Cada agregado é identificado por um único DSCP – *DiffServ code point*. Dentro do núcleo da rede os pacotes são encaminhados de acordo com o comportamento nó a nó associado com o DSCP, seu modo de encaminhamento (*forwarding behavior*). A classificação feita no núcleo da rede é baseada apenas no DSCP. Nas bordas é feita a classificação MF (*multi-field*), que seleciona os pacotes baseado na combinação de um ou mais campos do cabeçalho, como endereços da origem e do destino, campo DS, identificação do protocolo, número das portas de origem e destino e outras informações como por exemplo a interface de entrada. Todas estas informações devem ser autenticadas.

A figura 4.2 ilustra a implementação do modelo de referência para roteadores DiffServ.

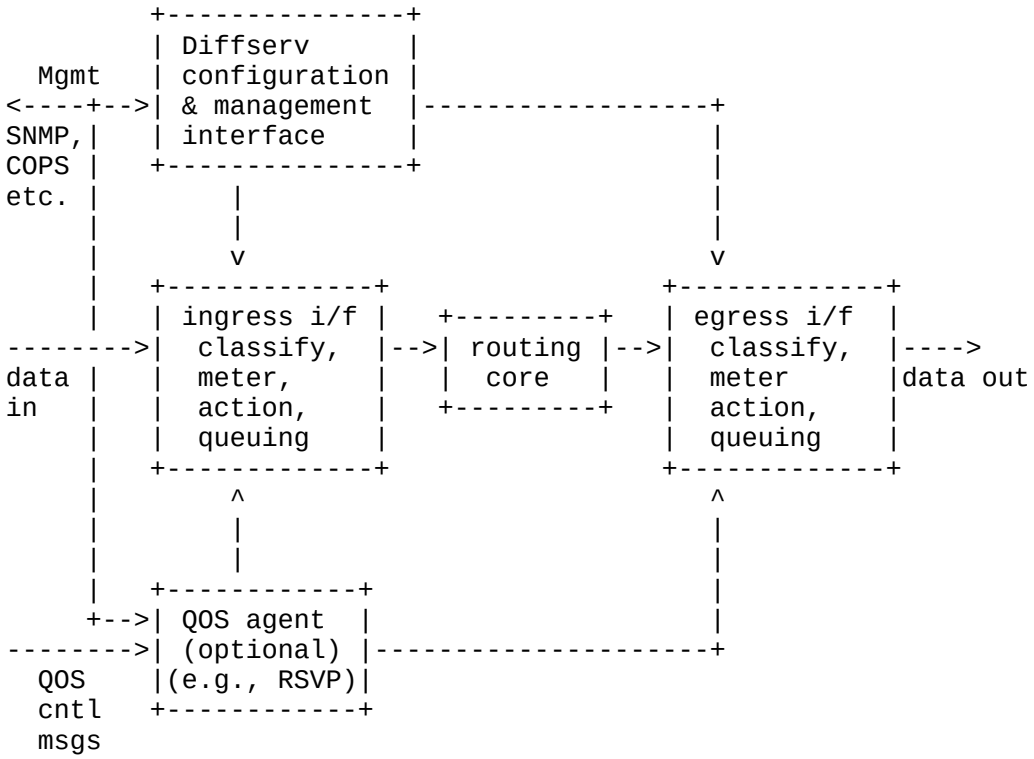


Figura 4.2 Roteador DiffServ - modelo de referência (BERNET, 2002)

Os parâmetros de operação do DiffServ são monitorados e provisionados através da interface de gerenciamento. Os parâmetros monitorados incluem estatísticas relacionadas ao tráfego transportado nos vários níveis de serviço. Estas estatísticas podem ser importantes para questões comerciais e para acompanhar a conformidade do tráfego com as especificações de condicionamento de tráfego (TCSs) negociadas com os clientes.

Os parâmetros provisionados são os parâmetros do TCS para classificadores e medidores e os parâmetros de configuração do PHB para elementos de fila e ações de marcação, descarte e etc.

O administrador da rede interage com a configuração DiffServ e com a interface de gerenciamento através de protocolos de gerenciamento, como SNMP ou COPS, ou através de outras ferramentas de configuração de roteadores, como console via telnet e interface serial.

4.3.3. Serviços “Non-elevated”

O serviço Scavenger

Scavenger (QBSS, 2004) ou “cata-lixo é uma aplicação do *framework DiffServ* para a criação de um serviço que dá tratamento diferenciado, porém degradado em relação ao serviço padrão (melhor esforço), para diferentes pacotes. Esta aplicação do *DiffServ* não suporta a utilização de serviços com qualidade assegurada (AF – *Assured Forwarding* e EF – *Expedited Forwarding*), porém permite que o serviço melhor esforço alcance um desempenho melhor, equivalente ao obtido em uma rede superdimensionada.

A utilização de um serviço degradado como alternativa ao melhor esforço torna desnecessária a utilização de mecanismos de policiamento, condicionamento, marcação, e de controle de admissão do tráfego, simplificando muito a operação da rede.

O serviço cata-lixo é um mecanismo de rede que permite aos usuários e aplicações utilizar a capacidade residual da rede de modo a não afetar de forma significativa o desempenho da classe melhor esforço. O serviço cata-lixo cria uma rede virtual paralela de capacidade muito baixa. Entretanto esta capacidade é elástica e pode se expandir, ocupando a capacidade não utilizada da classe melhor esforço.

Os usuários ou suas aplicações devem marcar voluntariamente o tráfego que será tratado como cata-lixo com o DSCP definido globalmente para o serviço (001000, em binário). A adoção de um DSCP global evita a necessidade da sua remarcação nas bordas da rede, reduzindo assim a complexidade e o custo dos equipamentos. Isto implica também na possibilidade de implantar o serviço cata-lixo gradativamente dentro da rede, configurando apenas os roteadores dos enlaces congestionados. Os demais equipamentos podem simplesmente ignorar esta marcação e tratar o tráfego cata-lixo como melhor esforço.

Atualmente o serviço cata-lixo está sendo utilizado nas redes Abilene (INTERNET2, 2004) e ANS (*Advanced Networks & Services*) (ADVANCED, 2004) e está sendo testado pelas universidades de Stanford (SLAC) (SLAC, 2004) e de Indiana (projeto GRAPE) (GRAPE, 2004) e pelo TF-NGN (CHOWN, 2002), entre outros grupos de pesquisa.

O serviço melhor esforço alternativo

O serviço “melhor esforço alternativo”(ABE – *Alternative Best Effort*) (ABE, 2004) é um serviço novo para redes IP, que provê um menor tempo de enfileiramento (*queueing*) e consequentemente menor retardo. Por ser uma variação do serviço de melhor esforço não são necessárias mudanças no plano de controle, ou seja, não é necessário

implementar qualquer um dos modelos de QoS. Este serviço foi desenvolvido para atender aplicações que possuem restrições rigorosas de tempo real, como por exemplo áudio interativo, sem a utilização de serviços com qualidade garantida (*elevated*).

Para utlizar o serviço ABE a aplicação deve escolher entre receber um menor retardo ou uma maior vazão. Todos os pacotes da classe melhor esforço são marcados como verde ou azul. Os pacotes verdes recebem um retardo menor, limitado a um valor máximo, porém também recebem uma menor vazão para assegurar que os pacotes azuis não sofrerão nenhum impacto. Os pacotes azuis recebem o tratamento normal do serviço menor esforço. A escolha entre uma cor ou outra será feita de acordo com o tipo de tráfego e o estado da rede. É considerado normal que um mesmo fluxo tenha pacotes azuis e verdes.

Os pacotes verdes são encaminhados prioritáriamente, como forma de atender à garantia de baixo retardo, porém são descartados sempre que ameaçam o desempenho dos pacotes azuis. Não há qualquer garantia de vazão ou de perda, seja para pacotes verdes ou azuis, porém o serviço ABE assegura que os pacotes azuis não terão seu desempenho degradado em relação ao desempenho que teriam se a rede apenas oferecesse o serviço de melhor esforço. Assim os pacotes verdes não recebem um tratamento melhor do que os azuis, apenas diferente.

4.4. Medição em redes com QoS

Mesmo com a utilização maciça de enlaces de alta velocidade e de mecanismos de QoS, é possível que as aplicações não estejam sendo atendidas nas suas necessidades específicas.

A verificação de que estão sendo realmente providas as garantias de QoS não é uma tarefa fácil. É especialmente difícil em redes superdimensionadas, nas quais mesmo aplicações da classe de melhor esforço são transmitidas em condições muito boas, com pouca ou nenhuma perda de pacotes, baixo retardo e jitter mínimo. Isto deve-se ao fato de que as garantias de qualidade de serviço não são exatamente sobre o desempenho que é experimentado pela aplicação, mas sobre o desempenho que seria experimentado em caso de congestionamento. Conseqüentemente uma observação de valores ótimos para estas métricas durante longos períodos não confirma que os mecanismos de QoS estão funcionando corretamente.

Entretanto em uma rede carregada é possível fazer uma verificação através da análise de desempenho da rede por classe de serviço, utilizando métricas que caracterizam o comportamento tanto da rede física como também dos protocolos, roteamento, tráfego e serviços existentes. A análise de desempenho de redes envolve a análise de métricas que

caracterizam o comportamento tanto da rede física como também dos protocolos, roteamento, tráfego e serviços existentes. Dentre as principais métricas estão a largura de banda, o retardo, o jitter e a perda de pacotes.

Assim, é necessária a implantação de uma infra-estrutura de medições e análise, para garantir a QoS esperada pelas aplicações, sobretudo aquelas mais críticas. Os dados obtidos através das medições também podem ser utilizados pelo controle de admissão e para a otimização e o planejamento da rede, entre outras funções.

A infra-estrutura de medições consiste num conjunto de equipamentos e ferramentas que visam coletar dados sobre as métricas de interesse. São diversos os tipos de medições que podem ser efetuadas: medições por fluxo de tráfego (RTFM – Real Time Flow Measurement) (FLOYD, 1993; JAMIN, 1996; FEHER, 1999), medições passivas, em que são coletadas informações sobre todos os pacotes que trafegam por um dado enlace, e medições ativas, nas quais são gerados pacotes de teste e monitorado o desempenho para o mesmo através da rede. As medições também podem ser efetuadas para os tráfegos dos agregados da arquitetura DiffServ. Isto envolverá, medições para *Expedited Forwarding* (EF), *Assured Forwarding* (AF) (FLOYD, 1999) e melhor esforço (IQOM, 2004).

4.4.1. Verificação das garantias de QoS

Uma vez que a conexão tenha sido aceita e o serviço esteja sendo provido torna-se necessário verificar as garantias de QoS em diversos momentos. Inicialmente faz-se a monitoração para a verificação do serviço durante a fase de aceitação por parte do cliente, que deseja se certificar de que o serviço contratado está sendo realmente provido. Após a aceitação é feita a monitoração contínua do serviço e do perfil de tráfego do cliente para fins de gerenciamento e bilhetagem. Esta monitoração entretanto não faz a verificação das garantias de QoS, apenas detecta caso haja o seu descumprimento por parte da rede ou caso o cliente altere o seu tráfego e viole o SLA. Verficações adicionais são feitas para a solução de problemas e/ou a pedido do cliente.

Durante a fase de monitoração, o provedor do serviço deve assegurar o desempenho da sua rede e verificar se o desempenho específico do serviço acordado com o cliente está sendo atingido. Esta é uma tarefa complexa e para isto deve ser empregada uma infraestrutura de medição apropriada e diversas medições do desempenho devem ser feitas.

Escopo da monitoração

A exata localização dos nós de monitoração e medição na rede e as medições realizadas entre eles definem o escopo da monitoração. A utilidade das medidas de QoS é afetada pela localização dos nós de monitoração e medição.

Para a avaliação do desempenho fim a fim do serviço os nós de monitoração e medição devem estar localizados o mais perto possível do usuário, no caso em que o provedor do serviço também fornece o CPE, o nó de monitoração pode estar dentro das instalações do cliente. Caso isso não seja possível, o ponto ideal é o roteador de ingresso ou o primeiro estágio de concentração do tráfego. A escolha do roteador de concentração aumenta a escalabilidade da infraestrutura de medição, porém neste caso a distância, em número de *hops*, entre o usuário e o nó de monitoração deve ser considerada como uma fonte de incerteza nas medidas obtidas. Esta incerteza é devida ao trânsito através dos equipamentos intermediários e aos conseqüentes enfileiramentos e fragmentações a que os pacotes ficam sujeitos. Medições inter e intra-domínio devem ser executadas para identificar qual o ponto responsável pela degradação do desempenho, violando o SLA (LIAKOPOULOS, 2003).

Para avaliação do desempenho da rede devem ser monitorados além do ponto de entrada da rede, os pontos intermediários de concentração e os pontos principais de encaminhamento, como por exemplo roteadores do núcleo da rede e pontos de interconexão com outros domínios. Alguns testes devem ser executados para assegurar o funcionamento correto dos mecanismos de QoS, entre eles :

- Precisão dos mecanismos de classificação, medição, condicionamento e escalonamento do tráfego;
- Provisionamento de fluxos ou classes, de forma a verificar a alocação dos recursos de acordo com o requerido pelas aplicações e pela política de utilização da rede;
- Medição das métricas de desempenho em diferentes estados de carga da rede, para verificar se as garantias de qualidade estão sendo realmente providas;

4.5. Conclusão

Este capítulo tratou dos mecanismos clássicos para a implementação de QoS em redes IP: diffserv e intserv, identificando as principais características de cada um, seus pontos fortes e fraquezas. São relatadas ainda as dificuldades de sua implementação em um âmbito maior, compreendendo a sua utilização generalizada na Internet como forma de atender à demanda por serviços com garantias de QoS. Esta demanda é gerada basicamente por clientes

que possuem aplicações críticas e desejam assegurar garantias de desempenho para suas aplicações.

Uma forma de tentar enfrentar estas dificuldades e ainda oferecer serviços com alguma diferenciação no seu tratamento pela rede é a utilização de serviços degradados (“*non elevated*”) conforme sugerido pelo grupo de QoS da Internet 2. Na Internet 2 foram adotados dois serviços dentro desta linha de atuação: o serviço scavenger, ou cata-lixo, e o serviço “melhor esforço alternativo”.

Uma outra abordagem da questão de oferecer garantias de qualidade e priorização a alguns serviços que será vista no capítulo cinco, é a utilização da engenharia de tráfego. Uma boa engenharia da rede faz com que sejam raras as situações em que os fluxos de tráfego com garantias de QoS apresentem ganhos por serem tratados pelos mecanismos dos modelos intserv ou diffserv em relação ao tráfego de melhor esforço. A implementação do MPLS reforça este cenário em que o provimento de qualidade de serviço é feito sem a utilização de modelos ou mecanismos específicos.

Qualquer que seja a escolha acerca da forma de prover QoS, a medição dos parâmetros de qualidade e desempenho da rede permanece sendo um ponto fundamental para assegurar o bom funcionamento da rede e a sustentabilidade dos serviços através do controle de admissão, como também para a monitoração e verificação da qualidade realmente provida.

Capítulo 5
Engenharia de Tráfego

5.1. Introdução

A engenharia de tráfego consiste na medição do tráfego e de parâmetros da rede para sua avaliação e modificação de forma a alcançar metas de otimização do desempenho. Algumas ações de engenharia de tráfego são executadas a longo prazo, como por exemplo planejamento da capacidade da rede e implantação de novas tecnologias e equipamentos. Outras ações são de tempo real, por exemplo policiamento dos fluxos e condicionamento e priorização automatizada do tráfego.

A engenharia de tráfego é baseada em mecanismos de medição e realimentação e na distribuição otimizada do tráfego dentro da rede, utilizando métricas baseadas na estratégia do operador, na demanda de tráfego e nos requisitos do usuário. Envolve também a adaptação do roteamento do tráfego às condições da rede, com o objetivo de alcançar o desempenho contratado pelo usuário e o eficiente uso dos recursos da rede.

A engenharia de tráfego torna-se ainda mais necessária uma vez que a demanda do tráfego ou incidentes na rede não são previsíveis. Eventos extrínsecos, como um *site* que gera um tráfego inesperadamente alto ou ataques à segurança, podem gerar uma grande demanda e conseqüentemente congestionar a rede. Adicionalmente, fatores intrínsecos como falhas de equipamentos e nos meios de transmissão requerem ações de engenharia de tráfego para fazer melhor uso dos recursos de rede existentes de forma a atender a estas flutuações na condição da rede.

Neste capítulo é dada uma visão geral da engenharia de tráfego, seu modelo de funcionamento e subsistemas componentes. Em seguida são tratadas questões de medição específicas, como a escala de tempo, as bases de medição e entidades de medição utilizadas na engenharia de tráfego. Também são apresentadas a necessidade de obtenção da matriz de tráfego da rede e a monitoração do seu desempenho, bem como as dificuldades encontradas na prática atual.

5.2. Visão Geral da Engenharia de Tráfego

Há alguns anos o desempenho da rede como visto pelos usuários é o verdadeiro parâmetro de desempenho a ser considerado pelos provedores de serviço. Isto significa que deve ser tomado um cuidado especial na escolha de quais medidas de desempenho serão otimizadas. A rede deve transmitir os pacotes a partir dos nós de ingresso até os nós de egresso de forma eficiente, rápida e econômica. Além disso, em um ambiente com várias classes de serviço, como por exemplo redes diffserv, os parâmetros de compartilhamento de recursos da rede devem ser apropriadamente determinados e configurados de acordo com as políticas e modelos de serviço prevalecentes, de forma a resolver questões de competição surgidas da interferência mútua entre os pacotes através da rede.

Os objetivos de otimização da engenharia de tráfego devem ser vistos como um processo contínuo e interativo de melhoria do desempenho da rede e não apenas como uma meta momentânea. Estes objetivos têm sido relacionados com o controle da rede, a despeito de metas de otimização específicas de qualquer ambiente em particular.

Os aspectos de controle dentro da engenharia de tráfego podem ser pró-ativos ou reativos. No caso pró-ativo o sistema de controle de engenharia de tráfego toma medidas preventivas para evitar estados desfavoráveis de rede que sejam previsíveis. Também podem ser realizadas ações de aperfeiçoamento para induzir a um estado mais desejável no futuro. No caso reativo o sistema de controle responde corretivamente e talvez adaptativamente a eventos que já ocorreram na rede.

A dimensão de controle da engenharia de tráfego responde a múltiplos níveis temporais de solução de eventos da rede. Certos aspectos do gerenciamento da capacidade, com por exemplo o planejamento da capacidade, respondem a um intervalo de tempo bastante longo, variando de dias a possivelmente anos. A introdução de redes de transporte óticas comutadas automaticamente (possivelmente baseadas em MPLS (ROSEN, 2001)) pode reduzir significativamente o tempo de planejamento da capacidade por provisionar banda ótica muito rapidamente. As funções de controle de roteamento funcionam a um nível de resolução temporal intermediário, variando de milissegundos a dias. Finalmente, as funções de processamento de pacotes, por exemplo gerência de filas e escalonamento, respondem a nível temporal de resolução muito pequeno, variando de picossegundos a milissegundos, uma vez que lidam com estatísticas de tempo real do comportamento do tráfego.

Outro importante objetivo da engenharia de tráfego é facilitar a operação confiável da rede, provendo mecanismos que melhorem a integridade da rede e adotando políticas que enfatizem a capacidade de sobrevivência da rede. Isso resulta na minimização da

vulnerabilidade da rede e da indisponibilidade de serviço devido a erros, faltas e falhas na infra-estrutura.

5.2.1. Engenharia de tráfego e gerência da rede

A engenharia de tráfego é definida como o aspecto da engenharia de rede que lida com as questões de avaliação e otimização de desempenho em redes operacionais. A engenharia de tráfego envolve a aplicação de tecnologia e princípios científicos para medição, caracterização, modelagem e controle do tráfego.

A engenharia de tráfego pode ser compreendida como um grupo de funções que auxliam a gerência e a operação da rede, em conjunto com os mecanismos de OAM. Estas funções são utilizadas principalmente na gerência de desempenho, cuja principal função é assegurar que os objetivos de otimização estão sendo atingidos; na gerência de falhas, que pretende dectar, isolar e solucionar problemas na rede; e na gerência de configuração, que controla a topologia e a configuração dos elementos da rede.

Gerência de Desempenho

A gerência de desempenho envolve a execução de atividades que buscam otimizar o desempenho da rede e a avaliação do desempenho, utilizando largamente as técnicas e funções da engenharia de tráfego.

A otimização do desempenho pode ser alcançado através do gerenciamento da capacidade e do tráfego da rede. O gerenciamento da capacidade inclui o planejamento da capacidade, controle de roteamento e gerência dos recursos da rede. Os recursos de maior interesse incluem largura de banda dos enlaces, espaço dos *buffers* e recursos computacionais. Já o gerenciamento do tráfego inclui funções de controle do tráfego nos nós, como condicionamento do tráfego, gerência de filas e escalonamento, e outras funções que regulam o transporte do tráfego através da rede ou arbitram o acesso aos recursos da rede entre diferentes pacotes ou fluxos de dados.

A avaliação do desempenho da rede é uma atividade crítica dentro da gerência de desempenho e da engenharia de tráfego, muito importante para assegurar a efetividade dos métodos usados e para a monitoração e verificação de conformidade com as metas de desempenho. Os resultados da avaliação podem ser usados para identificar problemas existentes, guiar reotimizações da rede e auxiliar na predição de futuros problemas potenciais.

Assim, um dos componentes principais da gerência de desempenho é a monitoração do desempenho, ou seja, a monitoração contínua em tempo real da qualidade e da saúde da rede e de seus vários elementos. Apenas assim é possível assegurar a sua

confiabilidade e a sua disponibilidade, bem como o fornecimento dos diferentes serviços, mantendo a qualidade de cada classe de serviço (QoS), e o cumprimento dos acordos de interconexão e SLAs – *Service Level Agreements* fechados. Isso requer o uso de medições, tanto passivas como ativas, para coletar informações sobre o estado operacional da rede e acompanhar o seu desempenho. Devem ser gerados alarmes quando algum elemento da rede ultrapassar limites de operação pré-estabelecidos.

A degradação do desempenho pode ocorrer como resultado de instabilidade do roteamento, congestionamento, ou falha de componentes da rede. Períodos de congestionamento podem ser detectados quando a utilização dos recursos de um segmento da rede excede um certo limite, ou quando o tempo para o pacote atravessar um roteador (*cross router delay*) se torna inesperadamente grande. Perda excessiva de pacotes ou queda da vazão podem ser utilizados como formas de detecção de falhas, levando a atividades de proteção e restauração (LAI, 2003a), servindo de subsídio para a gerência de falhas.

Gerência de falhas

A engenharia de tráfego permeia todas as ações da gerência de falhas, estando distribuída entre a monitoração e a otimização da rede. Permite a detecção, reconhecimento, isolamento e correção dos eventos de falhas que indicam operações anormais de equipamentos, redes ou sistemas. A gerência de falhas pode ser dividida nas seguintes tarefas:

- Coleta de dados e detecção de falhas: Esta tarefa se confunde com a monitoração de desempenho da rede, porém seu enfoque é a identificação e, sempre que possível, a antecipação da falha. Para isto é feita a monitoração de taxas de erro, retardos de transmissão entre outras entidades. Devem ser utilizados limiares para a geração de alarmes.
- Diagnóstico de problemas ou Isolamento de falhas: Uso de técnicas, como correlação de eventos e testes de diagnóstico, para determinar a localização e o motivo da falha. Também são usados sistemas especialistas nesta tarefa.
- Resolução de problemas: Esta tarefa se confunde com a otimização da rede a curto e a longo prazo, porém voltada especificamente para ações corretivas. A sua meta é limitar o impacto da falha na rede, de forma que cause o mínimo possível de degradação do seu desempenho, e em seguida reestabelecer os elementos com problemas. Da mesma forma que na tarefa anterior podem ser usados sistemas especialistas que sugerem ações automaticamente.
- Supervisão de Alarmes: Provê a indicação de quais elementos estão em perfeitas condições, quais estão funcionando parcialmente e quais estão fora de operação. Inclui

níveis de severidade e pode indicar possíveis causas e provê registro de ocorrências e emissão de relatórios para análise.

Gerência de configuração

A engenharia de tráfego também se interrelaciona com a gerência de configuração, demandando mudanças de configuração de equipamentos e utilizando as informações da *baseline*, um conjunto de dados de configuração dos elementos da rede, para determinação de rotas ótimas e rotas alternativas. A gerência de configuração realiza as funções de controle, identificação, coleta e alimentação de dados para configuração dos elementos de rede e vice-versa. Pode ser subdividida em gerência de topologia e gerência de dispositivos.

A gerência de topologia fornece diferentes visões da rede: conectividade física (topologia física), conectividade lógica (topologia lógica, geralmente a nível IP), visão administrativa, ou seja, agrupamento dos dispositivos de acordo com regras organizacionais da empresa, e visão de serviços, evidenciando os dispositivos de rede utilizados pelos diferentes serviços. Idealmente estas topologias deveriam ser levantadas de forma automática visto que a quantidade de elementos em uma rede grande torna a impossível realizar esta tarefa manualmente.

A gerência de dispositivos permite a sua configuração remota e o armazenamento destas configurações formando uma *baseline*. Assim é possível configurar um ou mais dispositivos semelhantes usando um arquivo de *baseline* armazenado, verificar se a configuração de todos os elementos da rede está de acordo com a *baseline* e reconfigurar a rede ou parte dela apartir da *baseline* em caso de problemas. A gerência de dispositivos permite ainda realizar atualizações automaticamente, em horários de baixa utilização da rede ou em janelas de manutenção, de vários dispositivos simultâneamente.

5.2.2. Modelo do processo da engenharia de tráfego

O modelo do processo da engenharia de tráfego (AWDUCHE, 2002) é interativo e dividido em quatro fases que se repetem continuamente. A primeira fase é definir as políticas de controle relevantes, que governam a operação da rede. Estas políticas podem depender de diversos fatores, incluindo o modelo de negócio, a estrutura de custo da rede, as restrições operacionais e os critérios de otimização.

A segunda fase do modelo é um mecanismo de feedback, envolvendo a aquisição de dados de medição a partir da rede operacional. Se os dados empíricos não são facilmente disponíveis na rede, então o uso de simulações pode ser feito para refletir o comportamento

prevalecente ou esperado da rede. A carga utilizada na simulação pode ser uma extrapolação dos dados empíricos ou uma estimativa. Também pode ser obtida usando modelos matemáticos de características de tráfego ou outros meios.

A terceira fase é a análise do estado da rede e a caracterização da carga de tráfego.A análise de desempenho pode ser pró-ativa ou reativa. A análise de desempenho pró-ativa identifica problemas potenciais que ainda não existem, mas podem se manifestar no futuro. A análise reativa identifica problemas existentes, diagnostica suas causas e avalia as diversas alternativas para solucionar o problema, se necessário.

A fase de análise pode envolver a investigação da concentração e da distribuição do tráfego através da rede ou subredes relevantes, identificando as características da carga de tráfego, identificando gargalos, potenciais ou existentes, e patologias da rede, como pontos críticos de falha.

A quarta fase do modelo é a otimização da rede. A otimização pode incluir o uso de técnicas apropriadas para controlar o tráfego entrante ou para controlar a distribuição do tráfego através da rede. Ações de otimização também podem envolver a adição de enlaces ou o aumento de sua capacidade, o emprego de hardware adicional, como roteadores ou switches, o ajuste sistemático dos parâmetros associados com o roteamento, como métricas IGP ou atributos BGP, e o ajuste dos parâmetros de gerenciamento de tráfego. A otimização do desempenho da rede pode envolver o início de um processo de planejamento da rede para melhorar a sua arquitetura, topologia, capacidade e tecnologia, bem como a configuração dos elementos da rede para acomodar crescimentos atuais e futuros.

Os componentes principais do modelo do processo da engenharia de tráfego incluem: subsistema de medição, subsistema de modelagem e análise e subsistema de otimização.

Subsistema de Medição

Medição é crucial para as funções de engenharia de tráfego. O estado operacional da rede só pode ser determinado conclusivamente através de medições. A medição também é critica para a otimização, pois provê dados de realimentação que serão usados pelos subsistemas de controle.

A medição também é necessária para determinar a qualidade dos serviços da rede e avaliar a efetividade das políticas de engenharia de tráfego.

A medição, como suporte das funções de engenharia de tráfego, pode ocorrer em diferentes níveis de abstração. Por exemplo, podem ser usadas medições para determinar

características no nível de pacotes, agregados de tráfego, componentes e mesmo da rede inteira.

Subsistema de Modelagem, Análise e Simulação

Modelagem e análise são aspectos importantes da engenharia de tráfego. Modelagem envolve a construção de uma representação física ou abstrata que mostre as informações relevantes acerca do tráfego e da rede.

Um modelo da rede é uma representação abstrata que capture as suas características e atributos principais, como restrições e atributos de nós e enlaces. Um modelo da rede pode facilitar as análises e simulações que podem predizer o desempenho da rede sob várias condições e também guiar os planos de expansão da rede.

Em geral os modelos de engenharia de tráfego podem ser classificados como estruturais ou comportamentais. Modelos estruturais focam na organização da rede e seus componentes. Modelos comportamentais focam na dinâmica da rede e na carga de tráfego.

Ferramentas de simulação de rede são extremamente úteis para engenharia de tráfego. Devido à complexidade das análises quantitativas realistas do comportamento da rede, certos aspectos do estudo de desempenho da rede só podem ser efetivamente conduzidos usando simulações.Um bom simulador também pode ser usado para validar a efetividade de soluções planejadas para problemas da rede.

Subsistema de Otimização

A otimização do desempenho da rede envolve resolver os problemas da rede transformando estas questões em conceitos que permitam identificar e implementar uma solução.

A otimização do desempenho pode ser corretiva ou para aperfeiçoamento da rede. Na otimização corretiva, a meta é remediar um problema que está ocorrendo ou é incipiente. Na otimização para aperfeiçoamento a meta é melhorar o desempenho da rede mesmo quando problemas explícitos não existem nem podem ser antecipados.

As interações para otimização podem consistir de subprocessos de otimização em tempo real e de planejamento e recuperação de rede. A diferença entre otimização em tempo real e planejamento de rede é primariamente em relação à escala de tempo em que operam e a granularidade de suas ações.

A otimização de tempo real é necessária devido a incidentes aleatórios como cortes na fibra ótica ou mudanças na demanda de tráfego que ocorrem independentemente de quão bom seja o *design* da rede. Estes incidentes podem causar a manifestação de

congestionamentos e outros problemas na rede operacional. A otimização de tempo real deve solucionar estes problemas em uma escala de tempo de pequena a média, variando de microssegundo a minutos ou horas. Exemplos de otimização de tempo real incluem gerência de filas, ajuste de métricas IGP/BGP e , no caso da utilização de tecnologias orientadas a conexão, como MPLS e ATM, a mudança explicita de circuito (LSPs, VPCs, VCCs) de forma a mudar o caminho de alguns agregados de tráfego. Em todas estas situações entretanto a estabilidade é uma importante consideração na otimização de tempo real do desempenho da rede.

Uma das funções dos subprocessos de planejamento da rede é iniciar ações para sistematicamente evoluir a arquitetura, a tecnologia, a topologia e a capacidade da rede. Quando existe um problema na rede a otimização de tempo real deve prover uma solução imediata. Devido à necessidade de uma resposta rápida, a solução de tempo real pode não ser a melhor possível. O planejamento da rede pode então ser subseqüentemente necessário para refinar a solução e melhorar a situação. O planejamento da rede também é requerido para expandir a rede de forma a suportar o crescimento do tráfego e mudanças na sua distribuição temporal. Uma mudança na tecnologia, topologia e/ou capacidade da rede pode ser o resultado de um planejamento da rede.

5.3. Medições para Engenharia de Tráfego

O grupo de trabalho de engenharia de tráfego - TEWG (TEWG, 2004) do IETF (IETF, 2004) vem desenvolvendo um *framework* para medições para engenharia de tráfego na Internet (LAI, 2003a). O foco do trabalho do TEWG é intradomínio, ou seja, dentro de um dado *autonomous system* (AS) e por isso também se aplica a redes IP corporativas, e não apenas a provedores de serviço de Internet. Seu objetivo é prover princípios para o desenvolvimento de um conjunto de sistemas de medição para dar suporte à engenharia de tráfego em redes IP, de forma a assegurar a qualidade dos demais aspectos da engenharia de tráfego – planejamento, dimensionamento, controle e monitoração do desempenho.

Medições de tráfego podem ser realizadas tendo como base fluxos, interfaces, enlaces, nós, pares de nós ou caminhos. Estes objetos levam à definição de diferentes entidades de medição, como por exemplo volume de tráfego, tempo médio de duração de um fluxo, banda disponível, vazão, retardo, variação do retardo, perda de pacotes e utilização de recursos. Estas informações do tráfego em conjunto outras informações da rede, como por exemplo topologia da rede, configuração dos roteadores, matriz de tráfego e outras estatísticas são essenciais para a engenharia de tráfego. Medições da carga de tráfego na rede também são importantes, especialmente para a gerência de desempenho.

Os principais componentes da medição voltada para a engenharia de tráfego identificados pelo *framework* (LAI, 2003a) são:

- as escalas de tempo, que determinam qual a granularidade de tempo em que as medições serão realizadas e consequentemente a sua utilização nas diversas ações engenharia de tráfego e da gerência da rede;
- as bases de medição, que permitem identificar em que nível de abstração e de agregação o tráfego será medido;
- as entidades de medição, que relacionam as métricas utilizadas na engenharia de tráfego;
- e a matriz de tráfego da rede, que é o levantamento de como o tráfego se distribui dentro da rede.

5.3.1. Escalas de Tempo

A informação coletada pelas medições de tráfego pode ser fornecida ao usuário final ou a uma aplicação, seja em tempo real ou para armazenamento, de acordo com as atividades a serem realizadas. O controle de tráfego geralmente requer informação em tempo real. Para planejamento da rede e gerenciamento da capacidade a informação pode ser provida após o processamento dos dados. Existem três escalas de tempo que são classificadas segundo a utilização da informação(ASH, 2001; MORTIER, 2002):

- Planejamento de rede: Utiliza informações cuja alteração é da ordem de dias, meses ou anos, para fazer previsões de tráfego que serão base para ampliações de rede e modificações na configuração da rede em longo prazo. Entre estas configurações estão planejamento da topologia da rede, planejamento de rotas alternativas para sobrevivência a falhas ou determinação da necessidade de aumento da capacidade antecipando o crescimento projetado do tráfego. O planejamento em longo prazo inclui a seleção e o projeto para introdução de novas arquiteturas, tecnologias e fabricantes.
- Gerenciamento da capacidade: O planejamento da capacidade, em uma escala de tempo intermediária, lida com a implementação dos planos desenvolvidos pelo planejamento de rede, atividades em curto prazo e eventos extraordinários. Tipicamente é feita uma previsão mensal do tráfego e da demanda. Informações que se alteram num prazo de minutos, horas ou dias são usadas para gerenciar as facilidades empregadas, através da manutenção apropriada ou de ações de engenharia para otimizar a sua utilização. Por exemplo, novos caminhos MPLS (ROSEN, 2001) podem ser estabelecidos ou caminhos existentes podem ser modificados de forma a cumprir os

contratos de SLA. Também pode ser feito balanceamento de carga ou o tráfego pode ser rerroteado para otimizar novamente a rede após uma falha.

- Controle de rede em tempo real: Usa informações que se modificam em milissegundos, ou menos, para fazer adaptações às condições atuais da rede o mais próximo possível ao tempo real. Desta forma para combater congestionamentos localizados, as ações de gerenciamento do tráfego podem realizar rerroteamentos temporários para redistribuir a carga. Quando ocorre a detecção de uma falha, o tráfego pode ser encaminhado para uma rota secundária pré-estabelecida até que rotas mais otimizadas possam ser encontradas.

5.3.2. Bases de Medição

As medições podem ser classificadas de acordo com o local aonde são feitas e o nível de agregação do tráfego medido. Existem várias opções de como realizar medições, uma delas é obter as medidas diretamente dos elementos de rede, por exemplo via SNMP (CASE, 1990). Coletar as medidas em elementos de rede operacionais, como roteadores, pode vir a causar problemas de desempenho. Existe atualmente um grande número de produtos de medição e monitoração disponíveis no mercado. Assim, uma opção é utilizar estes euipamentos, o que pode ter vantagens de desempenho porém introduz um custo adicional.

As seguintes bases de medição são utilizadas na engenharia de tráfego (LAI, 2003a; LAI, 2003b):

- Fluxos: A medição baseada em fluxos é conceitualmente similar à realizada em redes de telefonia e outras redes de comutação de circuitos. Destina-se a coletar informações detalhadas sobre o fluxo, incluindo endereços IP e números de portas de origem e destino, tipo de serviço, início e fim do fluxo e etc. Uma vez que gera uma grande quantidade de dados é normalmente utilizada em estudos especiais e apenas em roteadores selecionados, geralmente em roteadores de acesso, de borda ou de concentração. Não é recomendável seu uso em roteadores de *backbone*, no núcleo da rede ou em estudos de longa duração.
- Interfaces, enlaces e nós: Medições passivas podem ser feitas em cada elemento da rede através de suas interfaces, enlaces e nós, porém estes dados têm a desvantagem de que a identidade de cada fluxo é perdida. Por exemplo, a monitoração passiva via SNMP é usada para coletar dados nas interfaces dos roteadores, seja de borda ou de *backbone*, que são armazenados na MIB (MCCLOGHRIE, 1991). Estes dados incluem contadores de pacotes e octetos enviados e recebidos, pacotes descartados ou errados.

- Pares de nós: O principal tipo de medição baseado em pares de nós é a medição ativa. Medições ativas, como as especificadas pelo IPPM (IPPM, 2004) por exemplo, podem ser conduzidas entre cada par dos roteadores principais para determinar o desempenho do núcleo da rede. Estas medidas complementam as obtidas pelas medições passivas descritas acima.
- Caminhos: A medição baseada em caminhos é utilizada em redes MPLS. De forma semelhante a um fluxo, um caminho é associado a um par de nós, entretanto um caminho não é de granularidade tão fina quanto um fluxo. Caminhos são utilizados normalmente para transportar fluxos agregados. Por causa de suas propriedades, medições baseadas em caminhos são mais escaláveis e podem ser usadas para fornecer, de forma mais simples, uma visão da demanda de tráfego precisa e abrangente. Isto pode impulsionar o desenvolvimento de novas metodologias e técnicas para a medição baseada em caminhos.

5.3.3. Entidades de Medição

As entidades de medição relevantes para a engeharia de tráfego compreendem entidades de medição relacionadas ao tráfego e ao desempenho, ao estabelecimento de uma conexão ou caminho, e à utilização de recursos.

Entre as entidades relacionadas ao estabelecimento de uma conexão ou caminho está, por exemplo, a proporção de conexões recusadas. Esta entidade é util para monitorar o desempenho de redes que utilizam controle de admissão de conexões. Também é útil a relação da banda solicitada durante o estabelecimento da conexão. O número de solicitações de conexão, correspondendo ao número de tentivas de chamadas nas redes de telefonia, o número de fluxos e outras entidades podem ser medidas em intervalos pré-determinados para caracterizar o tráfego.

A caracterização de caminhos para engenharia de tráfego em redes MPLS pode ser feita utilizando as seguintes entidades de medição: retardo de estabalecimento de caminho, probabilidade de erro no estabalecimento de caminho, probabilidade de falha no estabelecimento do caminho, retardo de liberação do caminho, probabilidade de desconexão do caminho, tempo de restauração do caminho e etc.

As principais entidades relacionadas ao tráfego e ao desempenho estão listadas a seguir (LAI, 2003a; LAI, 2003b). Algumas destas entidades, como por exemplo retardo e variação do retardo, são relacionadas às respectivas métricas definidas pelo IPPM, ou aos parâmetros de desempenho definidos pelo ITU-T, na recomendação I.380/Y.1540 (ITUT, 2002a).

- Volume de tráfego: sua média e variância, em bits, bytes ou pacotes, contados em um dado intervalo de tempo por classe de serviço e em vários níveis de agregação (prefixo de endereço IP, interface, enlace, nó, par de nós, caminho, entrada/saída de rede, cliente ou AS).
- Tempo médio de alocação (*holding*): tempo de vida ou duração de um fluxo, duração de uma conexão ou caminho (MPLS) por classe de serviço.
- Banda disponível de um enlace ou caminho: útil para balanceamento da carga e para controle de admissão baseado em medições, entre outras atividades.
- Vazão (*Throughput*): medida em bits, bytes ou pacotes por segundo, é a taxa a que os dados são enviados entre dois pontos da rede. A condição da rede, por exemplo normal, altamente carregada ou congestionada, deve ser observada. Também são definidos *goodput* e *badput*, significando respectivamente a taxa a que os dados são transferidos com sucesso e a taxa de erros, perda e corrupção dos dados.
- Retardo: retardo fim a fim unidirecional, retardo bidirecional (*round trip time*), retardo inserido por um elemento de rede (*queueing* e retransmissão) e etc. Assim como para a vazão, a condição da rede deve ser observada.
- Variação do retardo (*jitter*): diferença entre o retardo fim a fim de pacotes selecionados de um mesmo fluxo. Existem diversos métodos de medição do *jitter* especificados pelo ITU-T (ITUT, 2002a) e pelo IPPM (DEMICHELIS, 2002).
- Perda de pacotes: a maioria das medições ativas não distingue a causa da perda de pacotes. Entretanto é desejável fazer a distinção entre perdas causadas por congestionamento da rede e perdas devidas ao policiamento. Perdas causadas por congestionamento são uma medida muito útil para o gerenciamento da capacidade da rede e da utilização dos recursos. Perdas relativas a erros de protocolo e/ou de transmissão não devem ser relacionadas ao tráfego, entretanto uma perda excessiva inesperada pode ser usada como uma forma de detecção de falhas.

A tabela 6.1 apresenta uma correlação entre as entidades de medição relacionadas ao tráfego e ao desempenho e as bases de medição. As medições feitas com base em fluxos, interfaces, enlaces e nós são passivas. Já as medições feitas entre pares de nós e em caminhos podem ser tanto ativas como passivas.

	FLUXOS	INTERFACE, ENLACES E NÓS	PARES DE NÓS	CAMINHOS
Volume de tráfego	x	x	x	x
Tempo médio de alocação	x			x
Banda disponível		x		x
Vazão			x	x
Retardo		x	x	x
Variação do retardo		x	x	x
Perda de pacotes		x	x	x

Tabela 5.1. - Entidades relacionadas ao tráfego e ao desempenho x Bases de medição (LAI, 2003a)

As entidades de medição relacionadas à utilização de recursos compreendem um conjunto de métricas que descrevem a utilização de diferentes recursos da rede, como roteadores (processador e memória), enlace e *buffer*. Devem ser estabelecidos limiares de utilização para a operação normal da rede. É necessária a configuração de mecanismos de alerta quando estes valores são ultrapassados. É importante também monitorar o compartilhamento dos recursos pelas diferentes classes de tráfego, relacionadas abaixo:

- Tráfego de controle: gerado pelo estabelecimento/liberação de uma conexão ou caminho e/ou para o encaminhamento do pacote, por exemplo tráfego gerado por protocolos de roteamento (OSPF, IS-IS), policiamento (COPS), distribuição de *labels* (LDP) e etc.
- Tráfego de sinalização: gerado por exemplo para a reserva de recursos para uma conexão ou caminho (RSVP).
- Tráfego de usuário: gerado pelos usuários da rede e subdividido em diferentes classes de serviço.

A quantidade de tráfego de controle e sinalização transportado por uma rede é função de muitos fatores, entre eles o tamanho e a topologia da rede, os protocolos de controle e sinalização usados, a quantidade de tráfego de usuário transportado, o número de falhas e eventos na rede, e etc.

5.3.4. Matriz de Tráfego

Um importante conjunto de dados para a engenharia de tráfego é a demanda ponto a ponto ou ponto multiponto. Estas informações são importantes para o provisionamento de caminhos intra-domínio e para a configuração de pontos de interconexão da rede. Também são significantes para o gerenciamento da capacidade, com o planejamento e o dimensionamento de novos enlaces, roteadores ou pontos de interconexão (LAI, 2003a).

Estimativas da demanda do tráfego são usualmente determinadas a partir de uma combinação de projeções do tráfego, solicitações dos clientes e SLAs. Não é fácil obter a demanda de tráfego de toda a rede a partir de medições feitas nas interfaces locais de diferentes roteadores. A informação obtida a partir de diferentes arquivos de configuração e coletada por diferentes medições na rede são necessárias para inferir o volume do tráfego (FELDMANN, 2000a; FELDMANN, 2000b). Além dos dados das medições, informações como dados da topologia da rede e dados de configuração dos roteadores, são utilizados para obter uma visão geral da rede. Adicionalmente o roteamento e encaminhamento IP baseado no destino proveêm ao operador da rede um controle primitivo e limitado sobre o roteamento dos fluxos de tráfego. É preciso a associação de uma seqüência no tempo de tabelas de encaminhamento de diferentes roteadores para reconstruir as diferentes rotas utilizadas pela rede ao longo do tempo.

5.4. Conclusão

A engenharia de tráfego representa um tipo de decisão que os gerentes de rede devem tomar. É necessário que se faça a monitoração da rede e o estabelecimento de políticas operacionais, como por exemplo para o roteamento e o policiamento do tráfego, que garantam o cumprimento das diretrizes definidas pela estratégia da empresa.

O gerenciamento do desempenho envolve a medição e a monitoração do funcionamento de diferentes segmentos da rede e assegura o bom desempenho fim a fim. Outras importantes atividades que também envolvem medição são a gerência de configuração e gerência de falhas. A gerência de falhas identifica o local da falha na rede, determina a causa raiz do problema e inicia atividades do subsistema de recuperação, tanto de proteção como de restauração. A gerência de configuração inclui a implantação de novos equipamentos na rede e o provisionamento de novos clientes. A verificação das políticas que estão sendo utilizadas na rede, como por exemplo controle de admissão de conexões ou fluxos, também é parte da gerência de configuração.

Os gerentes de rede dispõem de dados limitados e pouco detalhados para realizar estas atividades, sendo que apenas parte dos processos é automatizada. A engenharia de tráfego em redes IP permanece semimanual e dependente da *expertise* dos técnicos. As estatísticas mostram o congestionamento de um enlace, porém em geral não é fácil determinar a causa do congestionamento, quais clientes estão sendo afetados e uma possível solução. Os dados existentes não provêem informação sobre qual tráfego utiliza o enlace com problemas e nem se os clientes estão sofrendo degradação no desempenho de seus serviços como conseqüência. (GREENBERG, 2003).

O IETF, através de seu grupo de trabalho de engenharia de tráfego, identificou os principais requisitos para medições em engenharia de tráfego (LAI, 2003a; LAI, 2003b):

- Medições específicas de engenharia de tráfego:
  - Aumentar a utilização e a abrangência de medições baseadas em pares de nós, principalmente para derivar estatísticas da matriz de tráfego da rede por classe de serviço.
  - Estatísticas do tráfego transportado versus desempenho.
  - Mecanismos padronizados para facilitar a coleta de dados do tráfego entre pares de nós em redes MPLS.
- Métodos de coleta de dados do tráfego
  - Necessidade de definições de métricas uniformes entre fabricantes e operadoras.
  - Distinção entre a carga de tráfego oferecido e a vazão alcançada.
  - Necessidade de estatísticas de mais alto nível para assegurar a qualidade dos serviços.
  - Necessidade de medições por amostragem que preservem os detalhes do tráfego e que gerem volumes de dados reduzidos.
  - Interligação entre mecanismos de policiamento e medições de engenharia de tráfego.
  - Padronização dos modelos de informação para medições de engenharia de tráfego.

O atendimento a estes requisitos, a automatização dos processos e a interligação com informações detalhadas do tráfego (usuários, SLAs, interconexão, e etc) e com a política de QoS fazem com que a engenharia de tráfego seja mais eficiente, atingindo a sua meta de otimização da rede.

Capítulo 6

Ferramentas para monitoração, medição e geração de tráfego

6.1. Introdução

Um imenso número de atividades em redes de computadores envolve medições de naturezas diversas tais como: medições de retardo unidirecional e de ida e volta (RTT), variação destes tempos (jitter), medições de vazão, de capacidade instalada (largura de banda) em um enlace ou caminho, dentre outras. Para proceder a estas medições, utiliza-se ferramentas de medição. Este capítulo trata das ferramentas utilizadas para monitoração, medição e geração de tráfego. Serão apresentados os tipos de ferramentas usadas na operação de redes e serão listados exemplos de ferramentas de geração e medição de tráfego que permitem uma enorme flexibilidade para a realização de medições de desempenho. Também estão relacionados os principais projetos de medição ativa, passiva e de infra-estrutura de medição sendo desenvolvidos internacionalmente para redes de grande alcance, mais especificamente para a Internet, e um levantamento das ferramentas utilizadas comercialmente por duas importantes empresas provedoras de serviços de telecomunicações e Internet do mercado brasileiro.

Uma grande variedade de ferramentas está disponível para medir muitos aspectos da rede, em especial aqueles relacionados ao seu desempenho. As ferramentas variam desde simples comandos incluídos nos sistemas operacionais comuns, passando por aplicações gratuitas de código aberto, até sistemas e pacotes comerciais. Apesar do grande número de ferramentas disponíveis, não há estudo sobre a precisão e exatidão das medições obtidas, as faixas de medição de cada ferramenta, sua confiabilidade e demais características desejáveis a qualquer instrumento de medida. Em geral, os únicos resultados conhecidos para demonstrar as possibilidades de uma ferramenta são os publicados pelos próprios proponentes da mesma, em número bastante restrito, e apresentados nos documentos em que são propostas. Não existe método nem procedimento para certificação da medição e aferição ou calibração da ferramenta.

O desenvolvimento e a implementação de novas aplicações de rede, com crescentes exigências de serviço, fez com que surgisse a demanda por novas arquiteturas de rede com capacidade para atender a estes novos requisitos e conseqüentemente por uma infra-estrutura de medição que suporte a sua operação e gerência. Para atingir estes objetivos é importante o entendimento das características do tráfego e a sua modelagem para permitir a predição do desempenho das redes (Qualidade de Serviço(QoS), definição de Service Level Agreements (SLAs), e etc) e para o desenvolvimento de ferramentas de desenho, dimensionamento e monitoração e medição de redes.

6.2. Ferramentas

Estão descritos nos tópicos a seguir alguns dos tipos de ferramentas mais comumente utilizados para a obtenção de medidas em redes de comunicação de dados.

Ping

Ping é uma aplicação simples que roda em uma máquina cliente, normalmente fornecida como parte do sistema operacional do cliente. Ping envia um pacote ICMP (POSTEL, 1981a) echo request para uma máquina servidora especificada que envia em resposta um pacote ICMP echo reply, e o programa ping exibe o round trip time. O servidor não precisa executar qualquer software especial uma vez que o pacote ICMP é tratado pelo kernel do sistema operacional.

Os pacotes ICMP echo request/reply são informalmente referidos como pacotes de ping. A maioria dos programas de ping permite ao usuário enviar um único pacote ou uma série de pacotes a intervalos especificados. Ping provê um teste simples de conectividade para o site do servidor, ao menos para pacotes ICMP. Entretanto ser capaz de “pingar” uma máquina não significa que seja possível acessar seus outros serviços. As informações retornadas pelo ping incluem porcentagem de perda de pacotes, bem como informações sobre latência (rtt). Roteadores entretanto usualmente executam seus servidores de ping com baixa prioridade, de forma que usar ping para medir a latência um roteador irá produzir valores maiores de latência do que o experimentado por outras aplicações.

Traceroute

Traceroute (JACOBSON, 1989) é provavelmente a ferramenta de diagnóstico mais comumente utilizada para determinar porque uma máquina não responde a um ping. Da mesma forma que o ping, traceroute é normalmente fornecida como parte do sistema

operacional e não requer qualquer software especial instalado em outras máquinas. Traceroute produz uma lista enlace a enlace identificando cada roteador ao longo do caminho para a máquina alvo. Para cada enlace é impressa a latência (rtt) para o roteador ou * se não há resposta. Entretanto traceroute exibe apenas o caminho a partir da origem até a máquina alvo, ou seja, o caminho de ida dos pacotes. Para obter informações sobre o caminho de retorno traceroute deve ser executado na máquina remota. Uma forma de fazer isto é usando um servidor de traceroute reverso.

Para funcionar corretamente traceroute necessita receber pacotes ICMP *time exceeded* enviados pelos roteadores ao longo do caminho. Se estes pacotes forem bloqueados por um *firewall*, traceroute irá considerar como se os roteadores não tivessem respondido.

Monitoração via SNMP

SNMP, Simple Network Management Protocol (CASE, 1990) , é um protocolo padrão para gerenciamento de redes IP. Atualmente equipamentos como hubs, switches e roteadores saem de fábrica com agentes SNMP embutidos. Um agente SNMP mantém uma base de dados de informações especificadas na MIB (Management Information Base) (MCCLOGHRIE, 1991) do equipamento. Máquinas na rede podem descobrir informações sobre o equipamento a partir de objetos na sua MIB, e até mesmo mudar a sua configuração escrevendo novos valores em alguns destes objetos, caso tenha autorização. Um servidor central age como sistema de gerenciamento da rede, ou NMS (Network Management System), coletando os dados e permitindo ao gerente da rede monitorar informações de rede de diversos equipamentos, exibindo estes dados em uma tela e informando problemas no momento em que aparecem, como por exemplo perda de conectividade. Também é possível monitorar informações SNMP através de APIs, disponíveis para diversas linguagens de programação. Escolhida a forma de monitoração é preciso decidir que objetos da MIB serão monitorados. Existem muitas MIBs disponíveis, sejam proprietárias ou padrão, porém a mais simples é a Internet Standard MIB-II, implementada em praticamente qualquer equipamento de rede. Esta MIB permite monitorar cada interface do equipamento e obter informações sobre o tráfego. São feitas medições passivas para obter por exemplo as taxas de dados de entrada e de saída em cada interface.

Medição de fluxos de tráfego

Monitorar o tráfego nos enlaces, através da utilização do SNMP em suas interfaces é fácil e direto, porém não permite a obtenção de informações mais detalhadas. Para isto é necessário um sistema de medição de fluxos. Uma possibilidade é a arquitetura de

medição de tráfego RTFM (BROWNLEE, 1999) do IETF, que recomenda a utilização de medidores em cada ponto em que é necessário monitorar os fluxos de tráfego. Estes medidores são configurados através de arquivos de configuração que especificam os fluxos de interesse. Um programa gerente envia os arquivos de configuração para os medidores e lê os dados dos fluxos em intervalos especificados.

Monitoração de Aplicações

A maioria das ferramentas de monitoração de aplicações consiste de softwares ou serviços comerciais e tendem a ser altamente sofisticados. A forma mais simples entretanto de monitorar uma aplicação ou serviço é a utilização de *scripts* e *cron jobs*, que são pequenos programas que permitem a execução periodica de uma aplicação, medem seu tempo de resposta e armazenam os resultados.

Medição Ativa

A medição ativa de parâmetros da rede consiste, conforme apresentado mais detalhadamente no capítilo três, na geração e no envio por uma fonte de um fluxo de dados sintético e na medição do fluxo recebido em um detino especificado. Por este motivo as ferrametas que implementam a medição ativa são conhecidas como ferramentas de geração e medição de tráfego. Estas ferramentas permitem obter informações importantes da rede e/ou de seus elementos simulando uma determinada carga de tráfego. Têm a desvantagem de interferir na rede, podendo vir a alterar a grandeza que se pretende medir ou até mesmo degradar o desempenho da rede, quando mal utilizadas.

Usualmente estas ferramentas também permitem algum tipo de medição passiva, seja utilizando a monitoração via SNMP ou a medição de fluxos de tráfego apresentadas anteriormente.

Visualização

Ferramentas de medição são a base de um esforço de monitoração de rede de sucesso, porém para que seja possível lidar com os dados é necessário utilizar ferramentas que coletem os dados medidos e arquive-os de forma a produzir relatórios fáceis de obter e fáceis de entender. Estas informações serão usadas pelo pessoal técnico de suporte à rede. Para facilitar todos estes procedimentos é recomendável a utilização de boas ferramentas de visualização.

Uma ferramenta largamente utilizada é o MRTG (OETIKER, 2004), que lê variáveis SNMP, como por exemplo contadores de tráfego, e produz relatórios no formato http (páginas web), com informações diárias, semanais, mensais e anuais.

6.3. Comparação de ferramentas de geração e medição

Foi realizado um estudo comparativo entre diversas ferramentas de domínio público para a geração e medição de tráfego de rede em redes IP, visando identificar quais facilidades e funcionalidades estão sendo desenvolvidas nos diferentes projetos em andamento na comunidade internacional de pesquisa.

6.3.1. Ferramentas Avaliadas

DITG

O Distributed Internet Traffic Generator – DITG (AVALLONE, 2004) é uma ferramenta desenvolvida pela Universidade Frederico II (Universita' degli Studi di Napoli), cuja proposta é ser usada facilmente para gerar conjuntos de experimentos que possam ser repetidos utilizando uma mistura confiável e realista dos tipos de tráfego disponíveis.

O DITG pode gerar tráfego de acordo com várias distribuições de probabilidade (exponencial, uniforme, constante, pareto, cauchy, normal, etc) para as variáveis aleatórias IDT (Inter Departure Time) e PS (Packet Size). Esta ferramenta foi desenhada para a geração de tráfego de camada 7, camada de aplicação, suportando os seguintes protocolos: TCP, UDP, ICMP, DNS, Telnet, VoIP (G.711, G.723, G.729, Voice Activity Detection, Compressed RTP). Com o DITG é possível a reprodução de condições de rede muito complexas sob diferentes cargas e configurações de tráfego, permitindo também a investigação de efeitos de escala. O DITG é capaz de gerar tráfego a altas taxas, atingindo até 612 Mbps para gerador e receptor em máquinas separadas.

O DITG pode ser implementado em PDAs e laptops possibilitando realizar a caracterização completa de uma rede móvel heterogênea real. O DITG permite a avaliação de desempenho de equipamentos heterogêneos (Laptop, PC desktop, IPAH,…) sobre redes heterogêneas (LAN, WLAN,…). Outra característica inovadora do DITG é a possibilidade de armazenar informação tanto da origem como destino. Adicionalmente o DITG habilita ambas as pontas a delegar a operação de log para um servidor remoto. Esta opção é muito útil quando o nó de destino tem capacidade de armazenamento limitada – por exemplo, PDAs, Palmtops, etc. – e quando a informação de log deve ser analisada "on-the-fly", por exemplo,

no caso do nó de origem ser solicitado a adaptar a taxa de transmissão baseado em informações de congestionamento do canal ou na capacidade de recebimento do destino.

DITG permite a marcação dos campos TOS (DS) e TTL. Tanto a duração do experimento como o retardo em relação ao tempo de início do experimento podem ser configurados. Além disso, o nó origem pode ser remotamente controlado, iniciado no modo daemon e aguardar pelo comando para iniciar o experimento (a geração de fluxos de tráfego é controlada remotamente).

Para analisar os resultados dos experimentos é utilizado o ITGDec, um decodificador desenvolvido para a plataforma de geração DITG. A partir dos arquivos de log gerados pela origem (ITGSend) e pelo destino (ITGRecv) o ITGDec calcula os valores médios da taxa de transmissão, retardo e jitter de todo o experimento ou de um intervalo.

Iperf

O Iperf (TIRUMALA, 2004) é um software para análise de desempenho de redes, que foi desenvolvido pela Universidade de Illinois, para ser uma alternativa moderna para a medição de desempenho e utilização de banda de conexões TCP e UDP. Iperf pode ser compilado com facilidade em diversos OSs: Windows, Linux, SGI IRIX, HP-UX, Solaris, AIX, e Cray UNICOS.

O Iperf assim como a maioria das ferramentas de geração de tráfego e medição ativa utiliza o modelo cliente/servidor respectivamente para geração e recebimento dos pacotes. O servidor pode ser executado como um daemon (sistema Unix, ou um Windows NT Service) e é capaz de manipular múltiplas conexões, ao invés de encerrar a execução após um único teste.

Para realizar as medições o Iperf envia pacotes do cliente para o servidor tão rápido quanto possível. A informação é enviada diretamente da memória do cliente para a memória do servidor numa tentativa de eliminar um pouco as limitações de velocidade causadas pelo hardware. Porém para redes de alta capacidade, freqüentemente é necessário utilizar múltiplos fluxos para maximizar a banda.

O Iperf pode utilizar fluxos de dados representativos para testar como a compressão da camada de enlace afeta a banda a ser utilizada por uma aplicação. O tempo de execução pode ser determinado através de um intervalo específico ou da quantidade de dados a ser transmitida.

Ao final do experimento ou periodicamente a intervalos especificados, são gerados relatórios de perda de pacotes, jitter e banda. São relatórios em texto, utilizando o

múltiplo de unidade de dados mais adequado. O produto Jperf provê um front-end gráfico para o Iperf e produz uma representação gráfica do experimento.

As principais características do Iperf para cada protocolo disponível são:

- TCP
  - Medição da banda
  - Detecção da MSS/MTU *(maximum segment size/maximum transmission unit)*
  - Suporte à detecção do tamanho da janela TCP através de socket buffers.
  - Cliente e servidor podem ter múltiplas conexões simultâneas.
- UDP
  - Cliente pode criar fluxos UDP que utilizem uma banda especificada.
  - Medir perda de pacotes
  - Medir variação do retardo
  - Multicast
  - Cliente e servidor podem ter múltiplas conexões simultâneas. (exceto para Windows.).

Mgen

O Mgen (ADAMSON, 1999) é um conjunto de ferramentas desenvolvidas pelo NRL – Navy Research Laboratory, que permite gerar e medir tráfego UDP, tanto unicast quanto multicast. Possui suporte para o protocolo RSVP (BRADEN, 1997) e permite a criação de scripts utilizando o campo TOS do cabeçalho IP. É multi-plataforma, sendo atualmente suportado pelos seguintes sistemas operacionais: SunOS 4.1.x e Solaris 2.x, Linux, Solaris-i386, NetBSD e FreeBSD. Existe ainda uma versão para a plataforma Win32.

O Mgen é constituído basicamente por duas aplicações principais, mgen e drec, e pelos utilitários mcalc, allcalc, EZ e Txdelay. O mgen (Multi-generator) gera padrões de tráfego e o drec (Dynamic-receiver) recebe e armazena o tráfego gerado. O mcalc (Multi-calculator) mostra estatísticas do tráfego recebido. O rcalc é um visualizador gráfico dos níveis de tráfego por fluxo. O allcalc gera fluxo estatístico incluindo a taxa média de pacote, a taxa média de bit e a taxa média de atraso. O script EZ, ao ser executado, gera um arquivo em formato gif para ser utilizado pela ferramenta gnuplot1. O Txdelay produz um arquivo texto que registra o atraso de transmissão em função do tempo.

A geração do tráfego é realizada através de um arquivo de script que define padrões de tráfego que simulam o funcionamento de uma aplicação UDP/IP unicast e/ou multicast, de forma periódica ou através de uma função de Poisson. Também é possível

estabelecer a taxa de transmissão de pacotes por segundo e o tempo que irá durar a geração de tráfego. As estatísticas obtidas a partir da geração de tráfego pelo Mgen e de sua subseqüente recepção pelo drec podem ser visualizadas de duas formas: em modo texto ou modo gráfico. Em modo texto, deve-se executar o utilitário mcalc para a geração de um relatório com as estatísticas do tráfego recebido, separado por fluxo, e com um sumário de todos os fluxos transmitidos. Nesta estatística são exibidas informações sobre a identificação, a origem e o destino do fluxo, a quantidade de pacotes recebidos, a taxa de pacotes e dados recebidos, as taxas média, máxima e mínima do atraso, a variação do atraso e o número de pacotes descartados. Para a visualização gráfica do tráfego, devem ser utilizados o script EZ e a ferramenta gnuplot. O gráfico gerado dessa forma exibe as taxas médias de pacotes, de bits e de atraso.

Netperf

O Netperf (JONES, 2003) é uma ferramenta de benchmark, desenvolvida e informalmente suportada pelo grupo de desempenho de rede da HP (Hewlett Packard), utilizando o protocolo TCP ou UDP.

Ela foi projetada segundo o modelo cliente/servidor, composta pelos executáveis netperf e netserver. Quando o netperf é executado, é estabelecida uma conexão TCP com o sistema remoto. Essa conexão será utilizada para a passagem da informação de configuração dos testes e resultados para/do sistema remoto. Posteriormente uma outra conexão será aberta para a medição utilizando o protocolo apropriado para o teste e APIs. Contudo, o Netperf não permite a utilização do campo TOS para especificação do tipo de tráfego.

O Netperf oferece a possibilidade de medir o desempenho da transferência de dados, isto é, a velocidade em que um determinado sistema pode transmitir ou receber dados. Ele oferece ainda a possibilidade de medir o tempo de resposta entre um par de máquinas, ou seja, o tempo entre uma requisição e a resposta a esta requisição, o que possibilita seu emprego em testes de ambientes de rede e não apenas como ferramenta de avaliação de máquinas isoladas.

O teste TCP_CRR (TCP Connect/Request/Response) simula n operações TCP compostas por: estabelecimento de sessão, uma mensagem de request, uma mensagem de response e a finalização da sessão. As informações fornecidas pelo relatório gerado são: tamanho dos buffers da estação local (geradora) e da estação remota (receptora), tamanho das mensagens enviadas e recebidas, duração do teste e o resultado do teste, na forma de taxa de transmissão, em segundos.

O Netperf gera ainda um segundo relatório, que corresponde aos testes de fluxos TCP e UDP. Neste relatório são apresentadas a vazão da conexão e a quantidade de mensagens enviadas. Para tráfego UDP é exibida também a quantidade de mensagens com erro (não recebidas). A partir da recompilação do programa, é possível ativar uma opção de relatórios em histogramas.

Netprobe

O NetProbe (SAMIDI, 2002) é uma ferramenta específica para gerar tráfego de voz entre dois pontos da Internet. A meta deste projeto é medir o desempenho fim a fim de uma conexão no nível de aplicação. Esta medição é particularmente importante para aplicações de voz em tempo real que possuem requisitos de perda e atraso muito restritos. O NetProbe foi desenhado para ser um gerador de tráfego que emula o tráfego de voz em tempo real na Internet.

O NetProbe é uma ferramenta multi-threaded baseada em UDP cujo desenho segue a metodologia cliente/servidor. Para obter o comportamento do desempenho fim a fim, o cliente deve rodar localmente e o servidor remotamente. O cliente envia um pacote para o servidor remoto que instantaneamente envia o mesmo pacote de volta para o cliente. O cliente gera pacotes UDP que contém identificador de sessão (session ID), número de seqüência e três time-stamps. Estes pacotes são enviados a intervalos regulares para o servidor remoto. Os time-stamps são gerados cada vez que o pacote é enviado ou recebido pelo NetProbe e então são armazenados session ID, número de seqüência e os quatro time-stamps relacionados ao pacote em particular no arquivo de log, para análises futuras. Session ID, número de seqüência e três time-stamps compõem os 24 bytes adicionados aos 28 bytes do cabeçalho IP/UDP.

NetSpec

O NetSpec (JONKMAN, 1997) é uma ferramenta de avaliação de redes desenvolvida pela Universidade de Kansas. Atualmente existem versões para Digital Unix, Solaris, SunOS, Irix, Linux e FreeBSD.

O NetSpec suporta uma ampla variedade de testes com diversos modelos e tipos de tráfego emulado (FTP, http, MPEG, etc) e três modos de tráfego: full stream, burst e queued burst.

No modo de tráfego full stream, as máquinas em teste transmitem os dados o mais rápido que puderem. No modo burst, as máquinas transmitem os dados num intervalo específico de tempo através da opção de período e tamanho da rajada. No modo queued burst,

uma variação do algoritmo de rajada, as máquinas também transmitem dados num intervalo de tempo específico. Este modo tem como desvantagem o atraso da fila na caracterização do tráfego.

O NetSpec permite a execução distribuída de testes. Através de um único ponto de controle é possível executar testes em outras máquinas. Para isso é necessário escolher no arquivo de configuração da ferramenta uma dentre as três opções disponíveis: serial, paralela e cluster. Os arquivos de configuração do NetSpec são constituídos por uma linguagem específica, estruturada em blocos, e definem as características do tráfego a ser gerado.

A opção serial permite a execução de dois processos A e B, ou seja, processo B será iniciado depois da finalização do processo A. A opção paralela permite que o processo B seja iniciado durante a execução do processo A. Na opção cluster, os processos executam também em paralelo, mas a execução de A começa apenas depois que a execução do processo B é iniciada. O NetSpec não possui interface gráfica e seu relatório é gerado direto na saída padrão do Linux, ou seja, o terminal de vídeo. Ele pode, entretanto, ser direcionado para um arquivo-texto. A ferramenta não possui opção de geração de relatório gráfico.

Nettimer

Nettimer (LAI,K., 2002) é um projeto para medição do desempenho de redes fim a fim. As medições podem ser feitas passivamente, ouvindo o tráfego existente na rede, ou ativamente, inserindo tráfego na rede. Fim a fim significa que a ferramenta não depende de qualquer informação especial sobre a rede, bem como não depende de qualquer protocolo de transporte em particular.

O Nettimer é uma ferramenta para medição da largura de banda dos enlaces da rede. Podem ser medidos todos os enlaces ao longo de um caminho ou apenas o enlace que representa um gargalo. A medição fim a fim de banda é difícil porque o congestionamento pode fazer com que um enlace de alta capacidade pareça ter uma pequena banda. Medições passivas também apresentam problemas, uma vez que é preciso filtrar o comportamento de qualquer protocolo de transporte em particular.

Algumas das aplicações a que o Nettimer se destina:

- Benchmarking: Um usuário pode determinar se sua rede, equipamento ou serviço realmente suporta a taxa especificada.
- Seleção de *Web cache*: Dados diversos servidores proxy de cache, o cliente poderia usar medidas de banda na seleção do *cache* que lhe daria o melhor desempenho.
- Construção de árvore de multicast: Roteadores multicast poderiam usar medidas de banda na seleção do caminho a ser incorporado à árvore de multicast.

- Ajuste do protocolo: A medição de banda pode ser usada como um guia para obtenção da vazão máxima de um protocolo de transporte.
- Adaptação da camada de aplicação da rede: Uma aplicação pode modificar seus dados baseada nas condições atuais da rede. Por exemplo, as aplicações de vídeo de tempo real reduzem suas taxas de quadros quando a rede apresenta degradação da sua qualidade de serviço e servidores web que reduzem a qualidade de seu conteúdo (ex. jpegs) quando a banda disponível diminui.

Network Traffic Generator

O Network Traffic Generator (SANDILANDS, 2001) é usado para verificar a quantidade de tráfego de determinado tipo que uma rede, serviço ou equipamento pode suportar. Esta ferramenta não se destina a medir vazão ou tempo de resposta. O Network Traffic Generator foi desenvolvido para responder ao seguinte tipo de pergunta: Meu roteador irá suportar se 100 clientes simultaneamente fazem transferência de arquivos via TCP por 2 dias? Ou, posso configurar meu firewall para permitir que 50 pessoas façam grandes transferências TCP através deste equipamento? Para isto o Network Traffic Generator gera tráfego a partir de um ou mais clientes com destino a um ou mais servidores para realizar teste de sobrecarga em roteadores ou firewalls em redes altamente utilizadas.

Ntop

Ntop (DERI, 2004) é um *software* que faz a amostragem do tráfego e exibe a utilização da rede, retornando as informações em um formato similar ao do comando top, popular na maioria dos sistemas unix. Esta ferramenta funciona capturando pacotes da rede, realizando análise do tráfego e armazenando informações. Ntop possui duas aplicações:

Ntop clássico, que suporta um servidor web embutido: Usuários ntop podem usar um browser (ex. netscape) para navegar através da informação de tráfego gerada pelo ntop e obter um levantamento do estado da rede.

Intop (interactive ntop): é uma interface texto, semelhante ao *shell* dos sistemas unix, baseado no algoritmo do ntop. Intop provê uma interface poderosa e flexível para o ntop. Intop implementa uma interface baseada em linha de comando, com uma aparência simples, porém com muitas funcionalidades implementadas.

As principais características do ntop são:

- Classificação do tráfego da rede de acordo com diversos protocolos
- Exibe o tráfego classificado de acordo com vários critérios

- Mostra estatísticas do tráfego para domínio na Internet, AS (Autonomous Systems) ou VLAN (Virtual LAN).
- Passivamente, ou seja, sem enviar pacotes de teste identifica o OS e a identidade dos usuários de um computador.
- Mostra a distribuição do tráfego IP entre os vários protocolos
- Analisa o tráfego IP e classifica segundo origem/destino
- Exibe a matriz de tráfego IP de uma subnet
- Emite relatório de utilização do protocolo IP, classificado por tipo de protocolo de camada de aplicação encapsulado.
- Age como um coletor NetFlow/sFlow para fluxos gerados por roteadores (ex. Cisco e Juniper) ou comutadores (ex. Foundry Networks).
- Suporta múltiplas interfaces de rede e interfaces virtuais
- Gera gráficos através do utilitário gdchart

Pathchar

Pathchar (JACOBSON, 1997b) é uma abreviação para "path characteristics". Esta ferramenta permite a qualquer usuário descobrir as principais características de qualquer enlace na Internet enviando pacotes ICMP (pings) de tamanho variável. O pathchar mostra as seguintes informações: banda, retardo, tamanho médio das filas e taxa de perda.
Servidores pathchar estão em uso atualmente em diversos sites vBNs (VBNS, 2004) obtendo estatísticas para uso futuro na determinação de tendências.

Pathload

Pathload (DOVROLIS, 2004a) é uma ferramenta para estimar a banda disponível de um caminho fim a fim, entre uma máquina emissora e uma receptora. A idéia básica do pathload é que o retardo unidirecional de fluxos periódicos de pacotes UDP mostra uma tendência para aumentar quando a taxa do fluxo é maior do que a banda disponível. O algoritmo de medida é iterativo e requer a cooperação tanto do emissor como do receptor. Pathload é não-intrusivo, ou seja, não causa aumento significante da utilização da rede, retardos ou perdas.
Pathload consiste de um processo rodando em uma máquina emissora S e um processo rodando em uma máquina receptora R. S envia periodicamente fluxos de pacotes UDP para R a uma certa taxa. Pathload não determina se uma taxa em particular (Tr) é maior do que a banda disponível (A) baseado em apenas um fluxo. Em vez disto envia um conjunto de N fluxos, de forma que são utilizadas N amostras para decidir se Tr > A, ou não. Uma vez completa a recepção de todos os N fluxos, R verifica se há uma tendência de aumento no

retardo unidirecional relativo de cada fluxo. Se uma grande parte dos fluxos mostrar uma tendência de aumento então é dito que todo o conjunto possui a mesma tendência e que o próximo conjunto deve ser enviado a uma taxa menor do que Tr. Caso uma grande parte dos fluxos não possuam nenhuma tendência, então todo o conjunto é dito sem uma tendência e o próximo conjunto deve ser enviado a uma taxa maior do que Tr. Um certo conjunto cai em uma região cinza quando menos de f x N fluxos do conjunto mostram tendência de aumento e menos de f x N fluxos não mostram uma tendência consistente quando a banda disponível foi maior do que a taxa do conjunto para alguns fluxos e menor para outros. Em outras palavras a banda disponível durante o tempo de transmissão dos fluxos variou, estando acima da taxa de alguns fluxos, causando uma tendência de aumento, e abaixo de outros, que não demonstraram nenhuma tendência.

O algoritmo de estimativas iterativo Pathload termina quando a taxa de dois conjuntos sucessivos é menor do que a resolução especificada pelo algoritmo, ou quando a banda disponível varia em uma região cinza que é maior do que a resolução especificada pelo usuário.

Pathrate

Pathrate (DOVROLIS, 2004b) é uma ferramenta para estimar a capacidade fim a fim de um caminho. São usados métodos de dispersão de pacotes (*packet-pairs* e *packet-trains*) em conjunto com técnicas estatísticas para estimar a capacidade do enlace de menor capacidade do caminho. A capacidade de um caminho, ou seja, a banda do gargalo, é a vazão máxima que um fluxo de camada IP pode obter no caminho de rede entre um emissor S e um receptor R. A capacidade não depende da carga da rede. A rota seguida pelo caminho deve ser única e deve permanecer constante durante a medição. A capacidade do caminho é determinada pelo enlace com a menor taxa de transmissão.

Uma importante característica do pathrate é que esta ferramenta é robusta em relação aos efeitos do tráfego de fundo , ou seja, a medida da capacidade de um caminho pode ser feita mesmo que este se encontre significantemente carregado. Isto é crucial, uma vez que os caminhos mais difíceis de medir são os mais pesadamente carregados.

Pathrate requer que o usuário tenha acesso às duas pontas do caminho (é necessário executar o pathrate tanto em S como em R). São usados pacotes UDP para dispersão, assim como uma conexão TCP para a troca de informação de controle.

Pchar

Pchar (MAH, 2001) é uma nova implementação do utilitário pathchar, escrito por Van Jacobson. Ambos programas tentam caracterizar a banda, jitter, latência e perda de enlaces ao longo de um caminho fim a fim na Internet. Pchar pode ser usado tanto em redes IPv4 como Ipv6.

Pchar, assim como o pathchar, envia pacotes de teste de tamanhos variáveis e analisa as mensagens ICMP produzidas pelos roteadores intermediário ou pela máquina de destino. Através da medição do tempo de resposta para pacotes de diferentes tamanhos pchar pode estimar a banda e o round-trip delay fixo ao longo do caminho. Pchar varia o valor do campo TTL dos pacotes a serem enviados para obter respostas dos diferentes roteadores intermediários. Podem ser usados pacotes UDP ou ICMP como pacotes de teste. Tanto um como outro podem ser úteis em diferentes situações.

Os roteadores são implementados para encaminhar pacotes muito mais rapidamente do que para retornar mensagens de erro ICMP em resposta aos pacotes enviados pelo pchar. Devido a este fato, é possível obter tempos de resposta mais rápidos para partes mais longas do caminho. O resultado parece então uma estimativa negativa sem sentido do round-trip time para cada hop. Flutuações transitórias na rede também podem causar maus resultados.

Rude/Crude

O Rude/Crude (LAINE, 2002) é composto de duas ferramentas desenvolvidas pela Universidade de Tampere, na Finlândia e distribuído sob a licença GPL2. O código fonte das ferramentas está incluído no pacote. Não existe a possibilidade de utilização de interface gráfica, porém existe ajuda na linha de comando.

O Rude é o módulo gerador de tráfego. Ele utiliza um arquivo de configuração em formato texto por meio do qual é possível configurar os fluxos a serem gerados e mesmo modificar o comportamento destes fluxos depois de iniciada sua transmissão. Permite também o assinalamento do byte TOS do cabeçalho IP e a criação de novos tipos de fluxo e tráfego. Porém, o Rude/Crude só é capaz de gerar e medir tráfego UDP. Não existe opção de execução dos parâmetros utilizados no arquivo de script diretamente pela linha de comando.

O Crude é a ferramenta que irá receber os dados gerados pelo Rude e, na sua forma padrão, exibe informações sobre o tráfego recebido na tela, ou em um arquivo binário. São armazenadas neste arquivo informações sobre a identificação do fluxo, os números de

seqüência dos pacotes transmitidos, o tempo de transmissão e recepção e o tamanho dos pacotes em bytes.

Apesar de não fazer parte do pacote do Rude/Crude, existe um utilitário denominado gosplot, desenvolvido também pela Universidade de Tampere, que pode ser utilizado em conjunto com a ferramenta gnuplot para fazer uma conversão dos arquivos gerados pelo Crude em um arquivo em formato HTML, onde são apresentados o percentual de perda de pacotes, a vazão, a latência, a variação e distribuição da latência, além de um sumário destas características.

TG

TG (DENNY, 2003) e seus utilitários associados foram originalmente desenvolvidos pela SRI International (SRI, 2004) com subseqüentes melhorias suportadas por USC/ISI *Postel Center for Experimental Networking* (POSTEL CENTER, 2004). TG é um programa gerador de tráfego que cria fluxos unidirecionais UDP ou TCP entre uma fonte e um sumidouro. O tráfego é descrito em termos de intervalo de chegada e comprimento de pacotes. As informações relativas à fonte e sumidouro, por exemplo, tempo de transmissão e recebimento de pacotes, é gravado em um arquivo de log binário para ser processado posteriormente pelo utilitário dcat. Dcat, a partir do arquivo de log binário, produz uma representação ascii. Um script em perl chamado gengraph transforma estes dados em um formato apropriado para visualização através de ferramentas gráficas de domínio público, como por exemplo, xplot, xgraph, e gnuplot.

UDPGen/UDPCount

UDPgen/UDPCount - UDP kernel traffic generator (ZANDER, 2002) é composto por duas ferramentas que têm sido desenvolvidas para obter desempenho máximo na geração e recepção de tráfego, principalmente para uso em redes Gigabit Ethernet. A maioria das ferramentas compostas por softwares não possui um bom desempenho em termos de vazão de pacotes quando comparadas aos equipamentos de teste implementados em hardware. A razão para isto é que estas ferramentas sofrem restrições por rodarem no espaço do usuário, como por exemplo, o compartilhamento do kernel e a necessidade dos pacotes atravessarem toda a pilha de protocolos de rede. A proposta deste projeto foi construir ferramentas que enviam e recebem pacotes UDP o mais perto possível do driver de hardware.

Udpgen é um emissor de pacotes UDP. É um módulo do kernel do Linux que envia pacotes tão rápido quanto possível diretamente do driver de hardware evitando assim a pilha. O udpgen pode gerar taxas muito altas de pacotes para uma solução por software e

pode ser usado para testar o desempenho do conjunto hardware+driver de roteadores, comutadores, middleboxes e etc.

Udpcount é um receptor de pacotes UDP. É um módulo do kernel do Linux que pode ser associado ao protocolo UDP ou diretamente à rotina de recebimento que obtém pacotes a partir do driver de hardware. Esta ferramenta irá contar os pacotes recebidos e medir o intervalo entre a chegada dos pacotes. O udpcount pode receber e avaliar altas taxas de pacotes e pode ser utilizado em conjunto com o udpgen para vários testes de desempenho.

6.4. Comparação

A seguir estão tabuladas as informações mais importantes das ferramentas avaliadas para que seja possível sua comparação de forma simples e sistemática. Entretanto não é feito nenhum julgamento quanto à melhor ferramenta, uma vez que cada uma pode ser a mais indicada para determinado tipo de medição e de ambiente. As informações, que são na sua maioria auto-explicativas ou se referem a métricas já discutidas no capítulo 3, estão divididas em blocos de acordo com a sua utilização e/ou seu tipo.

Estas tabelas foram baseadas no trabalho "Laboratório para Avaliação de Modelos com Suporte a QoS em Redes IP" de MSc. Sheila Monteiro Bianchini, ex-aluna desta instituição (BIANCHINI, 2002).

Interface de Entrada

	DITG	Iperf	Rude Crude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPGen UDPCount
Gui	N	N	N	S	N	N	N	N	N	S	N	N	N	N	S*	N
Linha de Comando	S	S	N	S	S	S	N	S	S	S	S	S	S	S	N	S
Script	S	N	S	S	N	N	S	N	N	N	N	N	N	N	S	N
Execução em Modo Daemon	S	S	N	N	S	N	S	N	N	N	N	N	N	N	N	N
Execução Remota	S	N	N	N	N	N	N	N	N							

* Apenas para visualização dos resultados

Tabela 6.1 - Interface de Entrada

Características Gerais

	DITG	Iperf	Rude Crude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPGen UDPCount
Ipv6	N	S	S	S	S	*	N	N	N	N	N	N	N	N	S	N
RSVP	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N	N
DS/TOS	S	S	S	S	N	N	N	N	N	N	N	N	N	N	S	N
Múltiplos fluxos	S	S	N	S	S	N**	S	N	S	N	N	N	N	N	S	S
Fontes disponíveis	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Log remoto	S	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Taxa máxima gerada		Mb					Mb			N						Gb
Sistema Operacional	Linux Win	Linux Win	Linux	Linux Win	Linux	Linux	Linux	Linux	Linux Win	Linux Win	Linux	Linux	Linux	Linux	Linux	Linux

Tabela 6.2 Características Gerais

Tipos de Tráfego

	DITG	Iperf	Rude Crude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPGen UDPCount
TCP	S	S	N	N	S	N	S	N	S	S	N	N	N	N	S	N
UDP	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
ICMP	S	N	N	N	N	N	N	N	N	S	S	N	N	S	S	N
Multicast	N	S	N	S	N	N	S	N	N	S	N	N	N	N	S	N
Rajadas	N	N	S	S	S	N	S	N	N	S	N	N	N	N	S	N
Tráfego de fundo	N	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N
Telnet	S	N	N	N	N	N	S	N	N	S	N	N	N	N	N	N
FTP	N	N	N	N	N	N	S	N	N	S	N	N	N	N	N	N
VoIP	S	N	N	N	N	S	S	N	N	S	N	N	N	N	N	N
DNS	S	N	N	N	S	N	N	N	N	S	N	N	N	N	N	N
HTTP	N	N	N	N	N	N	S	N	N	S	N	N	N	N	N	N
Texto	N	N	S	N	S	N	S	N	N	N	N	N	N	N	N	N
Gráficos	N	N	S	N	N	N	N	N	N	N	N	N	N	N	N	N
Vídeo	N	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N
Outros	N	S	N	N	N	N	N	N	N	S	N	N	N	N	N	N

Tabela 6.3 Tipos de Tráfego

Tipos de Medição

	DITG	Iperf	Rude Crude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPGen UDPCount
Owdm	S	S	S	S	S	S	N	N	N	N	S	N	N	S	S	N
Rttm	S	S	S	S	S	S	N	N	N	N	S	S	S	S	S	N

Tabela 6.4 Tipos de Medição

Parâmetros de Entrada

	DITG	Iperf	Rude Crude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPCount
Início da transmissão	S	S	S	S	N	S	N	N	N	N	N	N	N	N	S	S
Help	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Endereço destino	S	S	N	S	S	S	S	S	S	S	S	S	S	S	S	S
Porta destino	S	S	N	S	N	S	S	S	S	S	N	N	N	N	S	S
Tamanho do pacote	S*	S	S	S	S	S	S	S	S	S (saída)	S (saída)	S (saída)	S (saída)	S (saída)	S (entrada e saída)	S
Intervalo entre pacotes	S*	N	N	S	N	S	N	N	S	S (saída)	N	N	N	N	S	S
Tamanho das rajadas		N	S	S	S		N	S	N	N	N	N	N	N	S	N
Intervalo entre rajadas	?	N	S	S	S	S	S	S	N	N	N	N	N	N	S	N
Tamanho da janela TCP	N	S	N	N	N	N	S	N	N	N	N	N	N	N	S	N
Taxa de transmissão UDP	N	S	N	N	N	N	N	N	N	N	N	N	N	N	S	N
Duração	S	S	S	S	S	S	S	N	S	N	N	N	N	N	S	S
Meio físico	N	N	N	N	N	N	N	N	N	S	N	N	N	N	N	N

Múltiplas CPUs	N	N	N	N	S	N	N	N	N	S (múltiplos hosts ou subredes)	N	N	N	N	N	N
Total de pacotes	N	S	S	S	N	N	S	N	N	S (saída)	S	S	S	S	S	N
TTL	S	S	N	N	N	N	N	N	N	N	N	N	N	N	S	N
Total de bytes			S	S	N		N	S	N	S (saída)	N	N	N	N	S	N

Tabela 6.5 Parâmetros de Entrada

Informações de Saída

		DITG	Iperf	RudeCrude	Mgen	Netperf	Netprobe	NetSpec	Nettimer	Network Traffic Generator	Ntop	Pathchar	Pathload	Pathrate	Pchar	TG	UDPGen UDPCount
Identificação das máquinas		S	S	N	S	N	S	S	S	S	S	S	S	S	S	S	S
identificação dos fluxos		S	S	S	S	N	N	N	N	S	S	N	N	N	N	S	S
Separação por fluxo		S	S	S	S	N	N	N	N	S	S	N	N	N	N	S	N
Consolidada		S	N	N	S	S	S	S	N	N	S	S	S	S	S	N	S
Por intervalo	Tempo	S	S	N	N	N	N	N	N	N	S	N	N	N	N	N	N
	Qtd de pacotes	S	N	N	N	N	N	N	N	N	S	S	S	N	S	N	N
Pacotes TX		S	N	S	S	S	S	S	S	S	S	S	S	N	S	S	S
Pacotes RX		S	N	S	S	S	S	S	S	S	S	S	S	N	S	S	S
Bytes TX			N	S	S	N	N	N	N	S	S	S	S	N	S	S	S
Bytes RX			N	S	S	N		N	N	S	S	S	S	N	S	S	S
Taxa de transmissão	Max	S	N	S	N	N	S	N	N	N	N	N	N	N	N	S	N
	Min	S	N	N	N	N	S	N	N	N	N	N	N	N	N	S	N
	Média	S	S	S	S	S	S	S	S	N	S	N	N	N	N	S	S
	Periódica	N	S	N	S	N	N	N	N	N	N	N	N	N	N	S	N
Atraso	Max	S	N	S	N	N	S	N	N	N	N	N	N	N	N	S	N
	Min	S	N	N	N	N	S	N	N	N	N	N	N	N	N	S	N
	Média	S	N	S	S	N	S	N	N	N	N	S	N	N	S	S	N
	Periódico	N	N	N	S	N	N	N	N	N	N	N	N	N	N	S	N
Jitter	Máx	S	N	S	S	N	S	N	N	N	N	N	N	N	N	S	N
	Min	S	N	S	S	N	S	N	N	N	N	N	N	N	N	S	N
	Média	S	S	S	S	N	S	N	N	N	N	N	N	N	N	S	N
	Periódico	N	S	N	S	N	N	N	N	N	N	N	N	N	N	S	N

TCP_MSS		N	S	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Tempo de resposta		N	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N
Bandwidth		N	S	S	S	S	N	N	S	N	S	S	S	S	S	S	N
Descarte	Total	S	S	S	S	N	S	N	N	N	N	S	S	N	S	N	N
	Periódico	N	S	N	S	N	N	N	N	N	N	N	N	N	N	N	N
Pacotes errados	Total	S	S	S	S	N	N	N	N	N	N	N	N	N	N	N	N
	Periódico	N	N	S	S	N	N	N	N	N	N	N	N	N	N	N	N

Tabela 6.6 Informações de Saída

6.5. Ferramentas Selecionadas

As tabelas 6.1 a 6.6 mostram informações importantes sobre cada ferramenta que permitem traçar um panorama do que está atualmente disponível ou em desenvolvimento na comunidade internacional de pesquisa, identificando quais facilidades devem consideradas chave e quais poderiam ser adicionadas. A seguir estão listadas algumas das principais facilidades que auxiliam a avaliar e selecionar a ferramenta mais adequada para cada tarefa.

Características Principais

A seguir estão apresentadas brevemente as principais características consideradas durante a avaliação das ferramentas. Estas características foram escolhidas por sumarizar informações importantes para a utilização prática das ferramentas em diferentes cenários.

- GUI: A presença de uma interface gráfica auxilia a rapidez e a clareza da execução, bem como da visualização e da interpretação dos resultados. Contrariamente à tendência de utilização de interfaces gráficas, este não é um item contemplado pela maioria das ferramentas. A sua importância depende do grau de familiaridade do usuário com scripts e ambiente texto.
- QoS: A geração de tráfego que simulem pacotes de reserva de recursos por fluxo (RSVP) ou com marcação de DS/TOS permite a geração de tráfego para testes dos principais mecanismos de QoS (IntServ e DiffServ). Também contrariando o esperado, muitas das ferramentas estudadas não permitem a geração de tráfego com características que simulem os principais mecanismos de QoS.
- Tipos de tráfego: A geração de diferentes tipos de tráfego permite o estudo e a avaliação de um número maior de variáveis da rede, monitorando o seu comportamento sob dieferentes cargas de tráfego e simulando diferentes aplicações. Isto pode ser extremamente útil em redes convergentes que suportam serviços variados. Da mesma forma que em relação à QoS, a geração de diferentes tipos de tráfego não é conemplada pela maioria das ferramentas. Quase todas as ferramentas permitem a geração de tráfego TCP e/ou a UDP com um perfil genérico, que em alguns casos pode ser ajustado modificando tamanho e intervalo de pacotes e rajadas. Apenas duas das ferramentas estudadas, DITG e NetSpec, apresentam a possibilidade de gerar tráfego com o perfil de várias aplicações comuns em redes IP.
- Tipos de medição: A possibilidade de realizar tanto medidas de ida e volta como unidirecionais dá flexibilidade à realização dos testes. Embora haja um movimento no sentido de utilizar medidas unidirecionais, que são inclusive recomendadas pelo IETF,

as dificuldades envolvidas na sua obtenção fazem com que praticamente todas as ferramentas priorizem a realição de medidas de ida e volta.

A possibilidade de configurar parâmetros de entrada e informações de saída também pode acrescentar flexibilidade à ferramenta. Configurar os parâmetros de entrada permite controlar o experimento e modelar o tráfego para obter melhores resultados em diferentes situações. É interessante que seja possível utilizar padrões de tráfego pré-configurados, auxiliando o usuário que não possua grande experiência e/ou agilizando a realização de testes com padrões recorrentes. De forma similar, quanto mais informações de saída sejam possíveis de obter, maior a flexibilidade na realização de experimentos. Também é útil a possibilidade de reduzir as informações disponibilizadas e/ou utilizar configurações prévias para diminuir a quantidade de dados ou a complexidade dos resultados, quando necessário. Boa pare das ferramentas apresenta restrições em seus parâmetros de entrada e informações de saída e apenas algumas permitem configurar mais do que tamanho do pacote e endereço IP e porta de destino. As informações de saída, na maioria dos casos, são pouco detalhadas, não podendo ser adaptadas para a geração de relatórios personalizados.

Outras informações importantes, como por exemplo método de medição utilizado e impacto na rede esperado pelos fluxos gerados não foram disponibilizadas pela grande maioria das ferramentas, embora sejam fundamentais para inferir a precisão das medidas obtidas e para verificar a sua adequação para monitorar redes operacionais.

Cenários de Utilização

A seguir estão descritos cinco cenários de utilização que descrevem situações práticas em que é necessário empregar fermentas de geração e/ou medição de tráfego. As grandes diferenças entre os cenários ilustra a variedade de situações encontradas pelos técnicos envolvidos na implantação, operação, gerência e manutenção de redes e demonstra a dificuldade de obter uma ferramenta única. Assim, é necessário avaliar cada caso utilizando informações como as disponibilizadas nas tabelas 6.1 a 6.6 sobre cada ferramenta para que seja possível definir qual mais se aproxima do “ideal” para cada tipo de atividade.

- Cenário 1 – Medições em laboratório para simulação ou homologação de redes e equipamentos

As atividades deste cenário são comuns durante as fases de implantação e de aceitação de redes, bem como testes de homologação e certificação de equipamentos. Para este tipo de aplicação é importante que a ferramenta utilizada seja capaz de gerar tráfego de diferentes perfis, não dependendo da existência de uma rede com tráfego real para realizar as medições. Outra característica desejável é a flexibilidade para configurar os parâmetros de

entrada e as informações de saída de modo que um mesmo experimento possa realizar diversas medições em conjunto e/ou em paralelo.

Para este cenário as ferramentas DITG e Iperf foram consideradas as mais adequadas por permitirem a geração de tráfego com diversos perfis, em especial a DITG, que também perimte simular aplicações como VoIP e DNS. Estas ferramentas foram utilizadas em ambos os estudos de caso que serão apresentados no capítulo 8. Para testes específicos de capacidade máxima de roteamento e encaminhamento de pacotes pode ser utilizada a ferramenta UDPGen/UDPCount desenvolvida especificamente para alcançar altas taxas de geração de pacotes utilizando um micro.

- Cenário 2 – Monitoração de uma rede operacional

Este cenário descreve o dia a dia da operação e da gerência de redes. Todas as tarefas desde o provisionamento até a recuperação de enlaces e serviços envolvem a monitoração da rede em operação. Para a realização de medições em uma rede operacional, deve-se limitar ao máximo o impacto no tráfego dos clientes, seja em relação à qualidade do serviço, seja em relação à segurança e privacidade dos dados. Esta preocupação supera a necessidade de simular diferentes tipos de tráfego. Idealmente deve-se realizar medições passivas, como as obtidas utilizando SNMP e RMON. Muitos fabricantes provêem um sistema de gerência proprietário que realiza as medições e a monitoração da rede.

As melhores ferramentas para este cenário são Ntop, utilizada em conjunto com Pathrate/Pathload e com Pathchar (Pchar). Estas ferramentas fazem medições passivas ou utilizam técnicas que realizam medições ativas com o mínimo de interferência na rede. Ntop monitora a utilização da rede e mostra estatísticas do tráfego, tendo suas informações complementadas pelas outras ferramentas citadas, que fornecem dados sobre os enlaces e/ou caminhos utilizados, como capacidade, vazão, utilização entre outros.

- Cenário 3 – Verificação das garantias de QoS

A verificação das garantias de QoS em uma rede pode ser feita durante o provisionamento de enlaces e serviços com qualidade garantida ou durante a recuperação destes serviços. Esta é uma atividade difícil de ser realizada rotineiramente e abrangendo a rede como um todo. Em geral esta verificação é feita sob demanda e pontualmente, seja em um ponto de acesso de cliente ou de interconexão (peering). É preciso manter as restrições do cenário anterior, acrescentando a geração de tráfego com diferentes perfis de QoS. Assim a ferramenta DITG é recomendada pela geração de tráfego DiffServ, em conjunto com Ntop que faz medições passivas, sem interferência na rede.

- Cenário 4 – Diagnóstico de problemas de desempenho na Internet ou em grandes redes IP

O diagnóstico de problemas de desempenho pode ser parte de um processo de otimização da rede, como a engenharia de tráfego, ou da recuperação de um enlace. É necessário utilizar ferramentas que façam a análise fim a fim dos enlaces, identificando gargalos e pontos de falha. No caso da Internet, a medição fim a fim pode ser a única forma de avaliar o enlace, uma vez que provavelmente este atravessa vários AS com administrações distintas. Em grandes redes IP, mesmo nas que possuem uma única administração, a análise de desempenho fim a fim pode auxiliar a diagnosticar, isolar e seccionalizar problemas de desempenho.

Assim como nos dois cenários anteriores estas medições são feitas em redes operacionais, portanto deve-se reduzir ao mínimo a interferência na rede, sempre que possível. A ferramenta Nettimer, assim como o *suite* Pathrate/Pathload se adequam bem a estes requisitos por levantarem várias informações sobre a rede gerando pouco ou nenhum tráfego. Estas ferramentas podem ser usadas em conjunto ou não.

- Cenário 5 – Ajuste (Tunning) de conexões TCP

Recentemente a implantação de redes de alta velocidade vem revelando que freqüentemente a limitação no *throughput* de uma aplicação não se deve a problemas da rede WAN, mas sim a erros de configuração da própria aplicação, da LAN e de outros equipamentos envolvidos. A determinação de parâmetros como MSS permite uma melhor utilização das redes. A ferramenta Iperf foi desenhada para realizar esta tarefa, podendo ser utilizada em conjunto com outras ferramentas, como a Web100, para obter o melhor desempenho possível das aplicações de rede.

Ferramentas Selecionadas

Dentre as ferramentas avaliadas foi selecionado um conjunto de ferramentas considerado como adequado para a realização dos testes necessários ao estudo de caso apresentado no capítulo 7. Avaliando os aspectos apresentados acima e os cenários prováveis de utilização, foram selecionadas as ferramentas DITG, pela sua flexibilidade, capaz de gerar tráfego segundo diversos perfis, UDPGen/UDPCount, por alcançar a geração de altas taxas, e Iperf, por também permitir a medição ativa das principais métricas de desempenho e por ser uma ferramenta bem aceita em termos de confiabilidade de resultados.

6.5.1. Hardware

Existem vários aspectos da arquitetura do hardware utilizado para geração e medição de tráfego que devem ser avaliados para verificar a sua adequação para ser utilizado em diferentes testes. Testes que necessitem a geração de tráfego a altas taxas (gigabit ou mais)

devem utilizar recursos especiais para evitar que gargalos na capacidade computacional do gerador/monitor comprometam a realização do experimento. Neste caso é recomendada a utilização de máquinas com um ou mais processadores de alta velocidade e barramento com alta capacidade de transmissão. O acesso à memória, bem como a memória em si também devem ser de alto desempenho. É interessante que a interface de alta velocidade seja *on board*, eliminando mais um gargalo. Seguem abaixo algumas sugestões, com a observação de que os preços informados são de agosto de 2004, coletados via Internet:

Servidor montado:

Estes dois servidores são comercializados já montados e possuem garantia de seus fabricantes. Ambos atendem aos requisitos para a geração de tráfego a taxa de gigabit.

- Modelo - dsIBM x Series 205 - modelo 8480 42XLM
  - 1 porta Gigabit on board
  - Pentium 4 - 2,66Ghz
  - Barramento PCIX
  - Memória 256MB a 2 GB
  - Linux Red Hat
  - Preço - R$ 4.238,51
- Modelo - Sun Fire B100x Blade Server
  - 2 porta Gigabit on board
  - Athlon XP1800+
  - Barramento PCIX
  - Memória 2 GB
  - Preço - *U$* 4.795,00

Componentes

É possível também montar um computador com capacidade para a geração à taxa de gigabit utilizando componentes adquiridos separadamente. A seguir estão algumas opções, relembrando porém que os preços foram coletados via Internet em agosto de 2004.

HD	PREÇO US	PREÇO BR
Winchester SCSI 36GB		R$ 798,00
Samsung UltraDMA33 40GB		R$ 349,00

Tabela 6.7 Opções de HD

MEMÓRIA DDR.400/PC3 200	PREÇO US	PREÇO BR
256MB		R$ 224,00
512MB		R$ 351,17

Tabela 6.8 Opções de memória

PLACA DE VÍDEO	PREÇO US	PREÇO BR
Radeon 7000 AGP 64Mb		R$ 279,99
GeForce MX4000 PCI 64Mb		R$ 235,54

Tabela 6.9 Opções de placa de vídeo

PROCESSADOR	PREÇO US	PREÇO BR
AMD Athlon 64 3200+ 2GHz		R$1.429,00
AMD Opteron		R$
Pentium 4 3.0 GHz		R$ 1.215,00
Xeon 3.06 GHz		R$ 3.188,97

Tabela 6.10 Opções de processador

COOLER	PREÇO US	PREÇO BR
Máster Aero 7 p/AMD até 3200		R$ 95,00
p/Pentium 4 até 3.2GHz		R$ 35,00

Tabela 6.11 Opções de cooler por processador

PLACA MÃE PARA AMD ATHLON 64 3200+ (2GHZ)		
MSI K8T Neo	U$140,00	R$ 632,00
Gigabyte K8NNXP	U$185,00	R$ 1069,00

Tabela 6.12 Opções de placa mãe por processador

PLACA MÃE DUAL PARA AMD OPTERON		
MSI K8D Master - F	U$519,19	R$ 1935,00
Tyan Thunder K8S s 2880	U$549 ,00	

Tabela 6.13 Opções de placa mãe por processador

PLACA MÃE PARA PENTIUM 4		
ASUS P4 C800-E Deluxe		R$ 838,32
Gigabyte GA - SINXP 1394	U$205,00	
MSI 865 PE Neo FIS 2R	U$170,00	R$ 694,00
Aopen AX4C-6	U$ 150,00	
Aopen AX4S Plus - U	U$179,00	

Tabela 6.14 Opções de placa mãe dual por processador

PLACA MÃE PARA XEON		
ASUS PP-DLW	U$ 304,63	
Aopen AXPS-U	U$ 172,00	
Aopen AXPS Plus - U	U$ 216,00	

Tabela 6.15 Opções de placa mãe por processador

PLACA MÃE DUAL PARA XEON		
Iwill DJ800		
Aopen DXPN-U	U$ 258,00	
Aopen DXPS-U	U$ 329,00	

Tabela 6.16 Opções de placa dual mãe por processador

6.6. Comparação de projetos de medição ativa de desempenho fim a fim na Internet

Existem diversos projetos que fazem medições ativas de desempenho fim a fim na Internet. A principal diferença destes projetos para as ferramentas avaliadas na seção anterior é sua utilização distribuída na Internet e a sua grande abrangência geográfica, delegando as tarefas de medições entre um grande número de pontos. Outra diferença importante é a limitação em definir os parâmetros de transmissão e dos pacotes de teste. Na maioria dos projetos a medição é baseada em ferramentas já conhecidas, como ping e traceroute, ou na implementação das recomendações do IETF. Esta lista não pretende ser exaustiva, apenas apresenta alguns projetos de relevância acadêmica de forma a ilustrar o cenário internacional da pesquisa em desempenho de redes.

6.6.1. Projetos avaliados

AMP – Active Measurement Program

O AMP (AMP, 2004)é um projeto do NLANR – National Laboratory for Applied Network Research (NLANR, 2004) cujo objetivo é aumentar o entendimento de como redes de alto desempenho funcionam, segundo a visão dos usuários e dos sites participantes, e auxiliar no diagnóstico de problemas tanto para usuários como para provedores da rede. A comunidade de interesse deste projeto compreende os sites participantes do programa HPC – *High Performance Computing* (HPC, 2003) da NSF – *National Science Foundation* (NSF, 2004). Neste projeto, os sites do HPC e outros colaboradores que participam de atividades de redes de alto desempenho, são encorajados a hospedar um monitor de medições ativas que executa medidas de conectividade, perda de pacotes e retardo de ida e volta. Também é feita, sob demanda, a medição de vazão para outros sites do HPC.

PingER

PingER (PINGER, 2002) é um projeto do IEPM – Internet End-to-end Performance Measurement para prover monitoração ativa do desempenho fim a fim de enlaces da Internet utilizando ping. Existem três comunidades de interesse que implementam projetos separados: Esnet – Energy Sciences Network (ESNET, 2004) e HENP – High Energy & Nuclear Physics (HENP, 2004), e XIWT – Cross Industry Working Team (XIWT, 2003).

A sua arquitetura de monitoração inclui três componentes: sites monitorados remotamente, sites de monitoração e sites de armazenamento e análise de dados. As medidas

são coletadas utilizando uma variação do ping, portanto os sites monitorados remotamente necessitam apenas disponibilizar uma máquina que irá responder passivamente aos pacotes ICMP. Os sites de monitoração devem ter uma máquina com as ferramentas PingER instaladas e configuradas, encarregadas de realizar as medições e de disponibilizar seus resultados via Web para os sites de armazenamento e análise. Os sites de armazenamento e análise são responsáveis pela coleta das informações dos sites de monitoração e seu armazenamento e pela disponibilização dos relatórios via Web.

RIPE

O serviço de medição de tráfego de teste (TTM – *Test Traffic Measurement*) é uma parte do projeto RIPE (RIPE, 2004) cujo objetivo é fazer medições independentes de parâmetros de qualidade de serviço na Internet. Sua comunidade de interesse é composta por provedores de serviço de acesso à Internet, em especial os europeus, e seus usuários.

As medições feitas pelo TTM-RIPE incluem retardo unidirecional, perda de pacotes, variação do retardo (*jitter*), banda e informação do caminho (*traceroute*). Os dados podem ser acessados em gráficos ou em seu formato bruto.

O projeto TTM-RIPE é compatível com os padrões desenvolvidos e mantidos pelo grupo de trabalho IPPM (IP *Performance Metrics*) do IETF (RFCs 2330 e 2678 a 2681) (IPPM, 2004).

Skitter

Skitter (SKITTER, 2004) é um projeto desenvolvido para testar a Internet ativamente de forma a analisar topologia e desempenho. Skitter determina o caminho unidirecional entre a sua localização, definida como origem, e um ou mais destinos utilizando um método semelhante ao do traceroute, ou seja, testando cada enlace ao longo do caminho através do envio de vários pacotes e incrementando o campo TTL (time-to-live) do cabeçalho IP. Desta forma são mapeados caminhos unidirecionais e seu retardo de ida e volta. Também são identificadas mudanças de roteamento persistentes.

Skitter foi desenvolvido e é suportado pela CAIDA – Cooperative Association for Internet Data Analysis (CAIDA, 2004). A comunidade de interesse e em grande parte financiadora do projeto é a DARPA – Defense Advanced Research Project Agency em conjunto com a NSF – National Science Foundation.

Surveyor

Surveyor (SURVEYOR, 2004, KALINDINDI, 1999) é um projeto encabeçado por duas organizações ligadas à pesquisa: Advanced Network Services – ANS (ADVANCED, 2004) e Common Solutions Group – CSG (COMMON, 2004). Seu objetivo é criar tecnologia e infra-estrutura de medição que permita aos usuários e provedores de serviços ter um entendimento preciso, comum a ambos, do desempenho e da confiabilidade de determinados caminhos na Internet, bem como determinar qual segmento que causa limitações. Utiliza testes ativos de retardo e perda de pacotes unidirecionais ao longo de caminhos entre máquinas dedicadas à realização de medições. Estas máquinas ficam localizadas nos sites CSG e alguns sites associados. A comunidade de interesse são os centros de pesquisa e de educação superior dos Estados Unidos, ligados ao CSG e à ANS.

O projeto também desenvolve metodologias e ferramentas para análise dos dados de desempenho.

Assim como o RIPE , o Surveyor utiliza as métricas padronizadas pelo grupo de trabalho IPPM (IP Performance Metrics) do IETF (RFCs 2330 e 2678 a 2681) (IPPM, 2004).

6.6.2. Comparação

Os projetos podem ser divididos entre o tipo de medição que executam (unidirecional ou ida e volta), a necessidade de uma máquina dedicada para as medições e a capacidade de monitorar sites remotos. Estas e outras informações estão tabuladas abaixo para que seja possível a comparação entre os projetos apresentados.

Projetos de Medição Ativa

	SURVEYOR	RIPE	PINGER	AMP	SKITTER
Método	Retardo e perda unidirecional	Retardo e perda unidirecional	Ping	Ping	Traceroute
Máquina	Dedicada	Dedicada	Selecionada	Dedicada	Dedicada
Sincronização	GPS	GPS	NTP	NTP	NTP
Freqüência (carga média)	~2*2/s (~2kbps)	~3/min (0.330kbps)	~0.01/s (~0.1kbps)	~ 1/minuto	1/hora
Escalonamento	Poisson <2/s>	Poisson <1/min>	Rajadas (30 min)	Linear randômico entre o 1º e o 15º segundo do minuto	~30 min.
Tamanho do pacote	~ 40 Bytes	100 Bytes	100 Bytes e 1000 Bytes	64 Bytes	53 Bytes
Locais	US, CA, CH, NL e NZ	EU, IL e US	~ 33 países	US, NZ, NO	Ásia, CA, UK e US
Pairs	~ 1000	1024	~ 1200	~ 4600	35000
Nº de monitores em julho/99	~ 51	~ 32	18	~ 70	20
Data de início	1997	1998	1995	1999	1998
Disponibilidade dos dados	Sob pedido	Sob pedido	Acesso público via web	Acesso público via web	?
Armazenamento dos dados	~38MB/pair/mo	2Mbytes/pair/mo	~0.6MB/pair/mo	~1.3MB/pair/mo (0.5MB zipped)	?
Parceiros/ Comunidade	CSG/ Advanced	RIPE/ Sites de pesquisa e ensino europeus	DOE/ Esnet/ HENP/ XIWT	NSF/ NLANR/ Internet 2	DARPA/ NSF/ CAIDA

Tabela 6.17 Projetos de Medição Ativa

Na tabela 6.17 acima a carga média citada na linha de Freqüência é o número de bytes enviados e recebidos nos pacotes de teste durante uma hora e expresso em bps. Esta informação não retrata a carga instantânea, que pode ser bem maior, ou a banda usada para coletas os dados das máquinas de monitoração.

Os cinco projetos devem ser considerados complementares, já que têm diferentes metas e há colaboração ativa entre os projetos. Uma vez que os projetos frequentemente possuem caminhos sobrepostos, por exemplo, existem vários sites com máquinas AMP, RIPE e Surveyor instaladas concorrentemente com máquinas PingER (p. ex. SLAC – Stanford Linear Accelerator, CERN), comparações e correlações são possíveis e encorajadas. Estas

comparações ajudam a assegurar a correção dos dados, pois os projetos usam diferentes mecanismos e códigos, e também a identificar a aplicabilidade dos dados obtidos com cada projeto. (COTTRELL, 1999)

6.7. Outros projetos de medição

Nesta seção são apresentados outros projetos de medição que complementam os projetos da seção 6.4. Estão relacionados alguns projetos de medição passiva, sendo um deles voltado para a área de segurança, e outros projetos mais complexos que envolvem o desenvolvimento de uma infra-estrutura de medição, com medições ativas e passivas em conjunto. Da mesma forma que na seção anterior não há a intenção de cobrir todos os trabalhos em curso, dada a sua grande quantidade, apenas traçar o cenário internacional da pesquisa em medição e monitoração de redes.

6.7.1. Projetos de medição passiva

Telescope Analysis - CAIDA

Um telescópio de rede (TELESCOPE, 2004) é uma parcela do espaço de endereçamento IP no qual pouco ou nenhum tráfego legítimo existe. A monitoração do recebimento de tráfego inesperado em um telescópio de rede permite a visão de certos tipos de eventos de rede remotos. Entre os eventos visíveis estão várias formas de ataques DoS, infecção de máquinas por worms e varreduras (scanning) de rede. Este trabalho é desenvolvido pela CAIDA com a cooperação da UCSD – University of California, San Diego, Network Operations (UCSD, 2004) e suporte da DARPA, NSF e Cisco Systems.

PMA – Passive Measurement and Analysis

O projeto PMA - Passive Measurement and Analysis é um dos dois projetos de pesquisa que formam o núcleo da Infra-estrutura de Análise de Redes (NAI – Network Analysis Infraestructure) (NAI, 1998) do Grupo de Medição e Análise de Redes (MOAT, 2004) do NLANR. O outro projeto é o AMP – Active Measurement Project, já discutido na seção 6.4.

O PMA (PMA, 2004) disponibiliza publicamente, via Web e FTP, dados de monitoração passiva que permitem o estudo de perfis de carga para um conjunto de pontos de medição estrategicamente localizados.

Sua infra-estrutura de coleta de dados consiste em um número cada vez maior de monitores localizados em pontos dentro de redes dos projetos HPC – *High Performance Computing* (HPC, 2003), VBNS – *Very High Performance Backbone Service* (VBNS, 2004) e Internet2/Abilene (INTERNET2, 2004). Atualmente são feitas medições diárias em enlaces com velocidades que vão de OC3 a OC48. Tipicamente são gerados gigabytes de dados por dia.

A USCD – University of California, San Diego também é parceira deste projeto através do San Diego Supercomputer Center (SDSC).

Enable

Este é um projeto de pesquisa do DOE (Department of Energy) , desenvolvido pelo LBNL - Lawrence Berkeley National Laboratory (LBNL, 2004) Data Intensive Distributed Computing Group e pelo ITTC – Information and Telecommunication Technology Center da Universidade de Kansas(KANSAS, 2004). O Enable é parte de outro projeto, o Distributed Monitoring Framework apresentado na subseção 6.5.2.

O Enable network advice server ou Enable server(ENABLE, 2000) pode ser instalado em qualquer máquina que seja fonte de dados, por exemplo um servidor FTP, e configurado para monitorar os caminhos que interligam esta máquina a um conjunto de clientes. No caso de um servidor FTP podem ser monitoradas uma lista de máquinas clientes selecionadas do arquivo de log. O servidor Enable monitora os valores de vazão e retardo.

6.7.2. Projetos de Infra-estrutura

IQoM

O projeto IQoM (IQOM, 2003) é parte das atividades do GT-QoS da RNP2 (RNP2, 2004). O GT compreende três linhas de trabalho principais: Estudo de métricas e métodos de medição, Infra-estrutura de medição e Implantação de serviços diferenciados. O projeto IQoM envolve o estudo, a definição e a implantação da infra-estrutura de medição para o GT-QoS.

A Infra-estrutura de medições consiste num conjunto de equipamentos e ferramentas que visam coletar dados sobre as métricas de interesse relacionadas à QoS das aplicações. São utilizados três tipos de medições: medições por fluxo de tráfego (RTFM – Real Time Flow Measurement) (BROWNLEE, 1999), medições ativas e medições passivas. Também podem ser efetuadas medições para os tráfegos dos PHBs da arqutetura DiffServ .

No projeto IQoM são utilizadas as seguintes ferramentas: NeTraMet, (NETRAMET, 2002) para medições passivas, AMP (AMP, 2004) e OWAMP (SHALUNOV, 2004), para medições ativas, e QAME (QAME, 2004), para monitoração.

NIMI – National Internet Measurement Infrastructure

NIMI (ADAMS, 2000) é um sistema para construir infra-estruturas de medição de redes. Uma infra-estrutura NIMI consiste de um conjunto de monitores e um software de controle e configuração de medição que executam em máquinas separadas.

Escalabilidade é uma das metas principais no desenvolvimento do NIMI, de forma a permitir uma visão potencialmente global da rede. Para isso o NIMI foi especificamente desenhado para ignorar as ferramentas de monitoração. As ferramentas de monitoração são agregadas em módulos, que podem conter diversas ferramentas diferentes, para serem utilizadas pelo NIMI na obtenção das medidas. Isto permite uma grande flexibilidade na realização das medições. Assim, o NIMI não é uma ferramenta de medição, mas um sistema de comando e controle para gerenciar ferramentas de medição. Atualmente as medições incluem:

- FTP: um wrapper para FTP – *File Transfer Protocol* (POSTEL, 1981c).
- Mtrace: uma ferramenta para medir rotas de multicast (MTRACE, 2004).
- *Traceroute*: uma ferramenta para identificar rotas (JACOBSON, 1989).
- Tráfego/Descarte: ferramentas para medir a vazão do TCP – Transmission Control Protocol (POSTEL, 1981b).
- TReno: uma ferramenta para medir a capacidade de transferência de grandes volumes de tráfego (Bulk Transfer Capacity) (MATHIS, 1996)
- Zing: uma ferramenta, variante do *ping*, para medir retardo unidirecional, *jitter* e perda .

Observatório Abilene

O observatório Abilene (OBSERVATORY, 2004) é um projeto que suporta a coleta e disseminação de dados das redes associadas com a rede Abilene. Este projeto provê informações operacionais de larga escala e também informações voltadas para a pesquisa de protocolos e outros mecanismos de redes de alta capacidade.

O observatório Abilene consiste de dois componentes:

- Dados coletados pelos engenheiros da Abilene, usando equipamentos localizados nos nós de roteamento e operados pelo centro de operações da rede (NOC) Abilene.

- Dados coletados por projetos de pesquisa separados usando equipamentos instalados nos nós Abilene. Atualmente cerca de quinze projetos utilizam o observatório.

Tequila

O objetivo do projeto Tequila – Traffic Engineering for Quality of Service in the Internet, at Large Scale (TEQUILA, 2002) é estudar, especificar, implementar e validar um conjunto de definições de serviços e de ferramentas de engenharia de tráfego, utilizadas para obter garantias de QoS fim a fim na Internet, como por exemplo no modelo DiffServ. Ou seja o projeto Tequila se destina a prover engenharia de tráfego para qualidade de seviço na Internet em larga escala.

As seguintes áreas são contempladas:

- Especificação de acordos de níveis de serviço, estáticos e dinâmicos, para suportar usuários fixos e móveis inter e intradomínio.
- Protocolos e mecanismos para negociação, monitoração e aplicação de acordos de níveis de serviço.
- Esquemas de engenharia de tráfego inter e intradomínio para assegurar a cooperação da rede com os acordos de níveis de serviços contratados entre diferentes provedores e na Internet como um todo.

DMF – Distributed Monitoring Framework

O objetivo do DMF (DMF, 2004) é melhorar a vazão fim a fim para aplicações que utilizam grande quantidade de dados em ambientes de redes WAN de alta velocidade. Outro objetivo é prover a capacidade de diagnóstico de problemas e análise do desempenho em Grids. Os dados coletados pela monitoração da rede e dos demais componentes de computação são disponibilizados para ferramentas de análise em tempo real.

Este projeto é constituído por diversos componentes, muitos dos quais já foram implementados separadamente. Fazem parte do DMF:

- NetLoger Toolkit: inclui monitores de aplicações, de rede e de sistema. Possui uma poderosa ferramenta para visualização de eventos e um sistema de armazenamento.
- Network Characterization Service: realiza a monitoração de rede enlace a enlace.
- Projeto Enable: discutido anteriormente na subseção 6.5.1, provê um serviço de aconselhamento para ajuste da rede.

6.8. Ferramentas utilizadas comercialmente

Complementando o panorama traçado pelas seções anteriores a respeito dos projetos desenvolvidos pela comunidade acadêmica e de pesquisa internacional, foi realizado um levantamento das ferramentas utilizadas comercialmente por três das principais empresas provedoras de serviços de telecomunicações e Internet do mercado brasileiro. Foram pesquisadas duas operadoras que atuam no mercado brasileiro a longos anos, derivadas da privatização do sistema Telebrás, e uma empresa instalada recentemente, cerca de 10 anos. Atendendo às solicitações os nomes das empresas não serão citados.

Em todas as empresas foi detectada a falta de ferramentas que se adeqüem ao perfil das operadoras de rede, tanto pelo alto custo das possíveis soluções como pelo seu atendimento apenas parcial às necessidades das empresas. As ferramentas disponíveis comercialmente, como por exemplo HP OpenView (HPOV, 2004), CiscoWorks (CISCO, 2004) e IBM Tívoli (IBM, 2004), se destinam a gerenciar redes com perfil coorporativo e apresentam limitações inconcebíveis para uma ferramenta "*carrier-class*" , tanto de endereçamento IP, como de monitoração de alarmes, geração de relatórios entre outras.

Em uma das empresas foi desenvolvida internamente uma ferramenta que faz interface com as plataformas de dados, tanto de transmissão como de comutação e de roteamento. A plataforma de transmissão é implementada utilizando equipamentos SDH do fabricante Newbridge/Alcatel, enquanto a comutação é feita por duas plataformas diferentes: ATM com switches Ascend/Lucent e Frame Relay usando equipamentos Nortel e Ascend/Lucent. A plataforma de roteamento, que suporta o *backbone* Internet, é composta por roteadores Cisco.

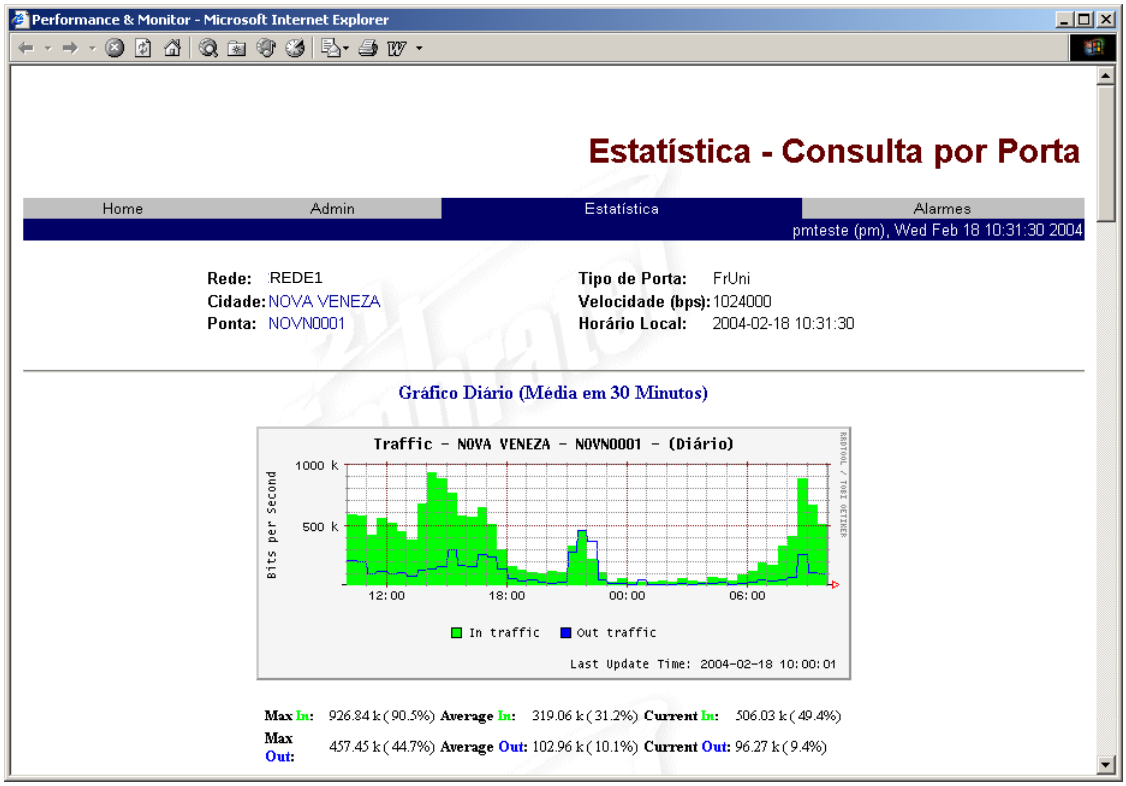
Esta ferramenta obtém informações diretamente dos equipamentos de cada plataforma e/ou da sua gerência proprietária e as utiliza para a geração de alarmes, monitoração dos elementos e obtenção de estatísticas históricas ou *on-line*. Como módulos adicionais, a ferramenta também provê suporte ao processo de diagnóstico através de um sistema de *trouble ticket* e apoio às rotinas operacionais internas, como por exemplo escala de plantão dos operadores.

A monitoração dos elementos permite consultas voltadas para o *backbone*, de forma a verificar o estado operacional ou estatísticas de utilização de um entroncamento entre switches, de uma porta, de uma placa ou do switch inteiro, e consultas voltadas para redes de clientes, informando dados por porta, por circuito ou da rede como um todo. Também é possível a verificação de erros em cada um dos elementos descritos acima e a determinação dos maiores ofensores, ou seja, dos elementos que estão inserindo mais erros na rede.

Completando a monitoração de elementos é possível obter informações sobre o consumo de recursos dos elementos do backbone, por exemplo utilização de memória ou CPU, por placa e por switch.

Os resultados obtidos podem ser visualizados graficamente, em tabelas ou incluídos em relatórios, com intervalos de medição variando entre 15 e 30 minutos e periodicidade diária, semanal, mensal e anual.

As figuras abaixo tiveram o logotipo da empresa removido a pedido dos profissionais entrevistados e exemplificam a interface da ferramenta para os usuários, que são os operadores da rede e as equipes de suporte e planejamento.



Id	Mnemonico	Data	Status	Fecham	Rede	Cidade	Ponta
1300036	QUEDA LMI	2004-03-18 14:58:20	A	-	REDE1	ALFENAS	AFN 828347
1300026	QUEDA LMI	2004-03-18 14:56:22	A	-	REDE1	RIO DE JANEIRO	RJO 814566
1300018	QUEDA LMI	2004-03-18 14:54:50	A	-	REDE1	MANAUS	MNS 817506
1299990	QUEDA LMI	2004-03-18 14:50:34	A	-	REDE1	GUARAPARI	GRI 827232
1299981	QUEDA LMI	2004-03-18 14:49:12	A	-	REDE1	MOITA BONITA	MOB 827569
1299929	QUEDA LMI	2004-03-18 14:42:27	A	-	REDE1	RIO DE JANEIRO	RJO 814565
1299865	QUEDA LMI	2004-03-18 14:33:11	A	-	REDE1	BRASILIA	BSA 827887
1299842	QUEDA LMI	2004-03-18 14:29:47	A	-	REDE1	LONDRINA	LDA 816407
1299809	QUEDA LMI	2004-03-18 14:25:42	A	-	REDE1	VILA VELHA	VVA 833813
1299801	QUEDA LMI	2004-03-18 14:24:14	A	-	REDE1	ARIPUANA	AYP 818733
1299795	QUEDA LMI	2004-03-18 14:23:22	A	-	REDE1	BRASILIA	BSA 825057
1299778	QUEDA LMI	2004-03-18 14:20:19	A	-	REDE1	SAO BENTO DO SUL	SBS 819026
1299739	QUEDA LMI	2004-03-18 14:14:24	A	-	REDE1	UBERLANDIA	ULA 816735
1299713	QUEDA LMI	2004-03-18 14:13:04	F	F	REDE1	MANAUS	MNS 819177
1299698	QUEDA LMI	2004-03-18 14:10:21	F	F	REDE1	IJUI	IJI 813974
1299686	QUEDA LMI	2004-03-18 14:08:41	F	F	REDE1	MANAUS	MNS 817506
1299670	QUEDA LMI	2004-03-18 14:03:49	F	F	REDE1	ITAPORANGA D`AJUDA	IJD 828106

Nas outras duas empresas encontramos a mesma carência por soluções de monitoração e medição, entretanto não foi feito nenhum desenvolvimento interno. A gerência da rede é feita utilizando as ferramentas proprietárias de cada plataforma. Estas ferramentas provêm um bom suporte à detecção e diagnostico de falhas, apesar da dificuldade de visualização devido ao grande número de elementos representados nos mapas de monitoração e à repetição de alarmes no log. Estas ferramentas possuem limitações ainda maiores em relação à avaliação de desempenho e à formatação e emissão de relatórios.

Assim a falta de integração entre as diferentes plataformas e a falta de ferramentas adequadas levaram à redução da análise das características da rede ao mínimo, impossibilitando a realização de tarefas importantes da engenharia de tráfego, com a conseqüente falta de otimização das redes destas duas empresas.

6.9. Conclusão

A avaliação das informações apresentadas neste capítulo sobre as diversas ferramentas disponíveis nos permite afirmar que não há uma ferramenta ideal, uma vez que cada uma pode ser a mais indicada para determinado tipo de medição e de ambiente.

Isto foi percebido especialmente no levantamento feito no mercado de operadores de rede. Apesar da existência de vários pacotes comerciais de ferramentas de medição e monitoração percebeu-se uma enorme carência. As ferramentas existentes possuem alto custo e não atendem aos requisitos de escala e de qualidade das empresas, bem como apresentam relatórios distantes das necessidades do seu ambiente. Assim foram encontradas duas situações diferentes resultantes desta carência:

- O desenvolvimento interno de ferramentas capazes de interfacear com as plataformas de rede, obter e formatar as informações conforme necessário;
- A redução da análise das características da rede ao mínimo, relegando ao abandono tarefas importantes da engenharia de tráfego.

As informações levantadas neste capítulo demonstram a importância e a utilidade de ferramentas de monitoração, medição e geração de tráfego visto o grande número e a variedade de projetos em curso na comunidade de pesquisa internacional e a carência encontrada no mercado brasileiro de operadores.

Capítulo 7
Estudo de caso

7.1. Introdução

A geração e medição de tráfego possuem várias utilidades, como por exemplo a monitoração de redes para conhecer as suas características de desempenho e qualidade, a coleta de dados históricos e em tempo real para atividades de engenharia de tráfego, e a realização de testes de aceitação de redes e homologação de equipamentos. Neste capitulo serão apresentados dois estudos de caso em que foram realizados testes que permitiram avaliar a funcionalidade da utilização de ferramentas de geração e medição de tráfego em testes reais de equipamentos.

Como parte das atividades desenvolvidas para esta dissertação, foi realizado um estudo comparativo entre diversas ferramentas disponibilizadas publicamente para a geração e medição de tráfego de rede. Este estudo teve o objetivo de identificar quais são as ferramentas mais adequadas para utilização em cada tipo de trabalho, bem como quais facilidades e funcionalidades estão sendo desenvolvidas nos diferentes projetos em andamento na comunidade internacional de pesquisa.

A possibilidade de simulação de fontes de tráfego complexas, permitindo a repetição diversas vezes exatamente do mesmo padrão de tráfego e obtendo informações não apenas sobre os pacotes recebidos, mas também sobre os pacotes enviados, é uma característica altamente desejável em uma ferramenta de geração e medição de tráfego utilizada em testes de aceitação e homologação. Esta capacidade da ferramenta permite a realização de experimentos simulando eventos reais repetidamente, o que facilita a detecção e o diagnóstico de problemas na rede ou equipamento em teste.

Cada vez mais as simulações devem refletir não apenas a grande escala dos cenários reais mas também a enorme variedade das fontes de tráfego, em termos tanto de protocolos como de padrões de geração de dados. A simulação de tráfegos de camada 4 a 7 (VoIP, FTP, Telnet, http, DNS, SNMP,...) pode auxiliar na configuração de redes de alto desempenho e na avaliação de equipamentos.

Avaliação e seleção de ferramentas

Foi realizada uma pesquisa para levantar as diversas ferramentas de geração e medição de tráfego disponibilizadas publicamente, segundo a filosofia do *software* livre. Entre estas foram consideradas neste estudo as ferramentas relacionadas abaixo e descritas detalhadamente no capítulo 6.

- D-ITG
- Iperf
- Rude/Crude
- Mgen
- Netperf
- Netprobe
- NetSpec
- Nettimer
- Network Traffic Generator
- Ntop
- Pathchar
- Pathload
- Pathrate
- Pchar
- TG
- UDPGen/UDPCount

Dois critérios foram considerados na seleção, avaliando a geração e a medição de tráfego. O primeiro critério utilizado foi a possibilidade de gerar diferentes perfis de tráfego, controlando seus parâmetros e simulando as principais aplicações utilizadas em redes IP. Também foi considerada a taxa máxima de geração, visando especificamente à geração de tráfego à taxa de Gbps.

O segundo critério foi a capacidade de obter diversas medidas, seja ativa ou passivamente, de forma a permitir a avaliação tanto de redes, incluindo enlaces, equipamentos e serviços, como de equipamentos isoladamente e de seu estado operacional. Foram selecionadas para este estudo as ferramentas DITG e Iperf. O DITG – *Distributed Internet Traffic Generator* é capaz de gerar tráfego segundo diversos perfis, medir as características do tráfego recebido e avaliar equipamentos isolados e ambientes de testes, que não possuem um tráfego real. O Iperf é uma ferramenta que também permite a medição ativa das principais métricas de desempenho em um ambiente de testes, porém não oferece muitas opções de perfil de tráfego a ser gerado. Entretanto é uma ferramenta muito utilizada pela comunidade

de pesquisa internacional, sendo, portanto, bem aceita em termos de confiabilidade de resultados. Assim ambas as ferramentas independem da existência de uma carga de tráfego real para a realização das medidas. Mesmo em ambiente de laboratório é possível a obtenção de medidas, sem a necessidade de utilizar qualquer outro recurso.

DITG

O DITG é uma ferramenta para a geração e medição de tráfego capaz de gerar um conjunto de experimentos que podem ser repetidos utilizando uma mistura confiável e realista dos tipos de tráfego disponíveis. São suportados os seguintes protocolos: TCP, UDP, ICMP, DNS, Telnet, VoIP (G.711, G.723, G.729, *Voice Activity Detection*, *Compressed* RTP). O DITG permite a marcação dos campos TOS (DS) e TTL. Para analisar os resultados dos experimentos é utilizado o ITGDec, que a partir dos arquivos de log gerados pela origem (ITGSend) e pelo destino (ITGRecv) calcula os valores médios da taxa de transmissão, retardo e jitter de todo o experimento ou de um intervalo, e o ITGPlot, que utiliza estes dados para gerar gráficos retratando o experimento.

Iperf

O Iperf é um software para análise de desempenho de redes capaz de gerar tráfego TCP e UDP. Para realizar as medições o Iperf envia pacotes do cliente para o servidor tão rápido quanto possível. A informação é enviada diretamente da memória do cliente para a memória do servidor numa tentativa de eliminar um pouco das limitações de velocidade causadas pelo *hardware*. Porém para redes de alta capacidade, freqüentemente é necessário utilizar múltiplos fluxos para maximizar o uso da banda. Ao final do experimento, ou periodicamente a intervalos especificados, são gerados relatórios de perda de pacotes, jitter e banda utilizada. São relatórios em texto, utilizando o múltiplo de unidade de dados mais adequado. O produto Jperf provê um front-end gráfico para o Iperf e produz uma representação gráfica do experimento.

Sincronismo e métodos de medição

As medições tradicionais de ida e volta, ou r*ound-trip*, como, por exemplo, a obtenção de valores de latência utilizando ping, medem o desempenho em conjunto de dois caminhos diferentes, de ida e de volta dos pacotes IP. Entretanto muitas rotas na Internet são assimétricas e, nestas circunstâncias as diferenças entre estes dois caminhos podem ser importantes a ponto de requerer medições separadas. Para a realização de medições unidirecionais é necessária a utilização de um relógio de referência externo para a

sincronização das máquinas. A precisão desta referência externa varia conforme a natureza da rede que está sendo avaliada.

Percebe-se assim uma das vantagens da utilização de medidas de ida e volta, é a facilidade para sua obtenção. Diferentemente das medidas unidirecionais, é possível com freqüência realizar algum tipo de medida do retardo de ida e volta sem a necessidade de instalar qualquer *hardware* ou *software* específico para medição no destino, porém perdem-se informações sobre a rede e seu desempenho.

Neste trabalho foram realizados experimentos entre máquinas sincronizadas e entre máquinas não sincronizadas, utilizando respectivamente os métodos de medição rttm – *round trip time measurement* e owdm – *one way delay measurement*. Para sincronizar as máquinas envolvidas com a geração e a medição de tráfego foi utilizado o produto NTP – *Network Time Protocol* (NTP, 2004), um *software* livre disponibilizado na Internet. O NTP utiliza servidores de referência de tempo, chamados *stratum*, distribuídos hierarquicamente conforme o seu grau de precisão e sua proximidade em *hops*, da referência de tempo. *Stratum* 1 são os servidores de mais alta precisão, diretamente conectado a uma fonte de referência, *stratum* 2 estão a dois *hops* da referência, *stratum* 3 a três *hops* e etc.. Foram utilizados como referência dois servidores de NTP da UFF, as máquinas marlin.telecom.uff.br, stratum 2, e traíra.telecom.uff.br, stratum 3.

7.2. Estudo de Casos: Homologação de switches Dlink

A Universidade Federal Fluminense iniciou um processo de substituição dos equipamentos do núcleo da sua rede de comunicação de dados, uma vez que os equipamentos atuais se encontram no limite se sua capacidade. Foram selecionados os equipamentos do fabricante Dlink para testes de homologação, certificando-os para a utilização pela UFF. Estes testes visam ratificar as informações prestadas pelo fabricante a respeito das características e funcionalidades dos *switches*, e verificar o seu desempenho em situações que simulam o ambiente de produção. Para isso foi desenvolvido um conjunto de testes simples, porém eficiente, cuja metodologia se baseia em experiências anteriores de outras instituições de ensino e pesquisa.

As ferramentas selecionadas foram utilizadas nos testes de homologação dos *switches* Dlink, tanto para a geração de tráfego com características semelhantes ao real, como para avaliação do desempenho dos equipamentos através da medição do tráfego recebido e da sua documentação na forma de gráficos e relatórios de texto. Estas vantagens tornam a utilização de ferramentas de geração e medição de tráfego essencial para o sucesso deste tipo de teste, principalmente em comparação com os utilitários *ping*, *traceroute* e *tcpdump*

tradicionalmente usados. Assim a utilização das ferramentas DITG e Iperf executando em máquinas com sistema operacional linux, permite a implementação de um laboratório capaz de realizar diversas medições a um custo muito baixo. As limitações encontradas devem-se, em sua maior parte, ao *hardware* utilizado, especialmente no que se refere à velocidade do processador e do barramento PCI, utilizados em computadores do tipo PC.

Estão descritos a seguir os equipamentos, os *softwares* e os procedimentos empregados nos testes de homologação.

7.2.1. Caso 1 – Homologação do switch DES 6300

Inicialmente foi selecionado o switch DES 6300 para avaliação, sendo que o ambiente de testes também utilizou outros dois modelos de switches Dlink, DES 1200 e DES3226 (DLINK, 2004).

DES 6300

Este equipamento é um *switch router* do tipo chassi, que suporta diversos módulos de interface, podendo ser obtidas diferentes configurações. Suas principais características são:

- Backplane de 31.99 Gigabit/sec (Gbps).
- Comutação de camada 2 baseada em endereços MAC e no parâmetro VLAN ID
- Suporte ao padrão IEEE 802.1Q VLAN (*Static* VLAN)
- Suporte ao padrão IEEE 802.1d *Spanning Tree*
- Suporte à priorização de tráfego 802.1p
- Capacidade de agregação de portas (*Port trunking*)
- Espelhamento de portas (*Port mirroring*)
- Suporte a cliente DHCP
- Suporte ao protocolo de roteamento RIP, versões 1 e 2
- Suporte ao protocolo de roteamento OSFP
- Suporte a IGMP, IP Multicast e a mecanismos de QoS (*Quality of Service*)
- Suporte aos protocolos de roteamento multicast: DVMRP, PIM DM
- Suporte a ACL – *Access Control List*

DES 1200 e DES 3226

Os *switches* DES – 1200 e DE – 3226 são equipamentos gerenciáveis, destinados para uso departamental. A diferença fundamental entre eles é o fato de que o DES – 1200 é um *switch* tipo chassi para o qual existem alguns módulos opcionais a serem instalados.

Suas principais características são:

- *Backplane* de 9.6 Gigabit/sec (Gbps). – DES 1200 M
- *Backplane* Gigabit/sec (Gbps). – DES 3226 S
- Comutação de camada 2 baseada em endereços MAC e no parâmetro VLAN ID
- Suporte ao padrão IEEE 802.1Q VLAN (*Static* VLAN)
- Suporte ao padrão IEEE 802.1d *Spanning Tree*
- Suporte à priorização de tráfego 802.1p e a TOS
- Capacidade de agregação de portas (*Port trunking*)
- Espelhamento de portas (*Port mirroring*)

Configuração do laboratório

A topologia desenhada para o laboratório procura simular no ambiente de testes o *backbone* da UFF, utilizando três *switches* DES-6300, interligados entre si por enlaces Ethernet 100Mbps e 1Gbps, e por enlaces Ethernet 100Mbps a *switches* DES-1200M e DES-3226. Entretanto esta especificação teve que ser reduzida para apenas dois DES-6300, um DES-1200M e um DES-3226, devido à dificuldade do fornecedor em entregar a quantidade de equipamentos solicitada.

Adicionalmente duas máquinas PC Linux foram configuradas como cliente e servidor para as ferramentas de medição e geração de tráfego. Estas máquinas também foram usadas para configurar via console os *switches*, testando a interface de linha de comando. Foi utilizado ainda um *laptop* com o *software* Config Master para a configuração e monitoração dos equipamentos via interface gráfica. Faz parte das sugestões para trabalhos futuros a implementação de um ambiente com maior número de equipamentos, tanto PCs como *switches*, e também de um ambiente MPLS para a realização de testes envolvendo engenharia de tráfego.

A figura 7.1 ilustra a configuração pretendida para a realização dos testes, inicialmente em laboratório e em seguida transportando os equipamentos para a rede operacional.

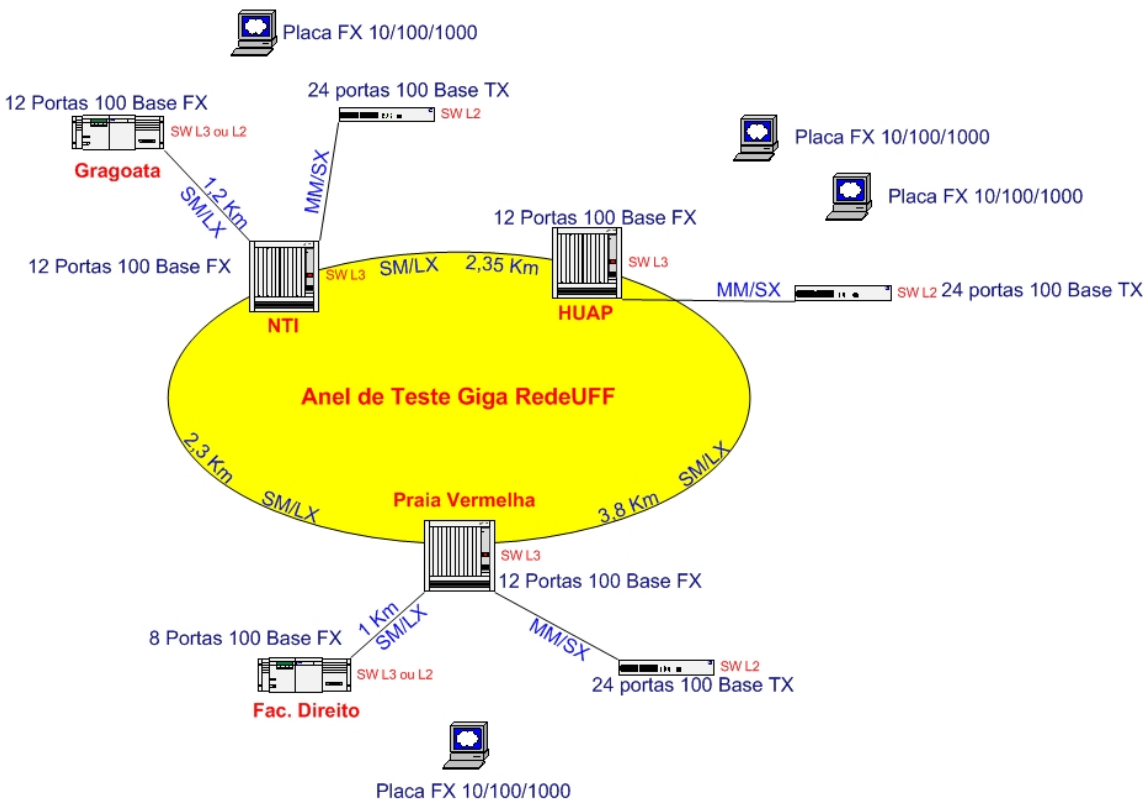


Figura 7.1 - Configuração pretendida do laboratório

A figura 7.2 mostra a configuração realmente utilizada nos testes do caso 1, devido às dificuldades na obtenção de todos os equipamentos necessários à configuração pretendida inicialmente.

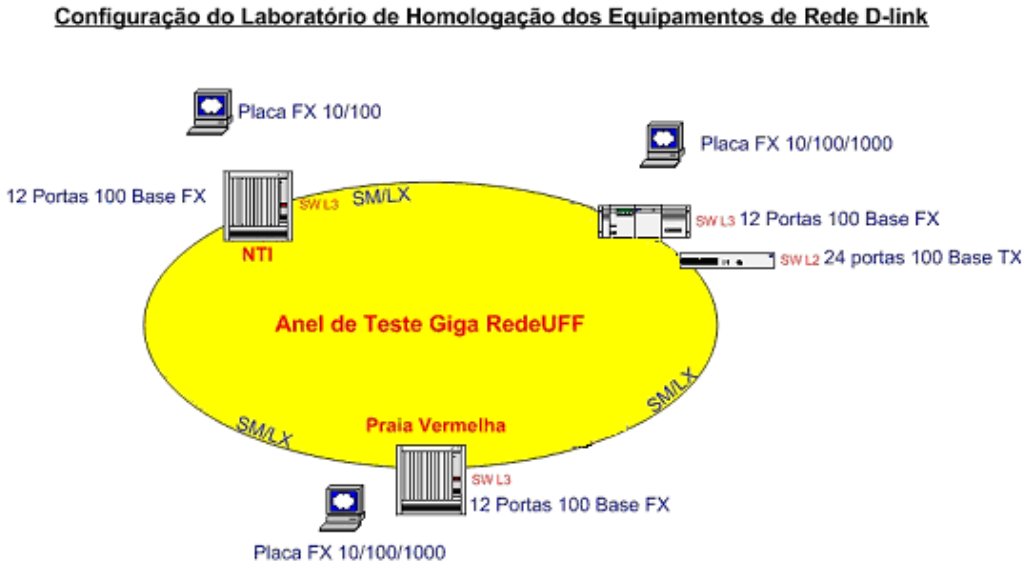


Figura 7.2 - Configuração utilizada do laboratório

As figura 7.1 e 7.2 apresentam a topologia pretendida e utilizada nos testes respectivamente. A seguir está brevemente descrita a configuração dos equipamentos empregados.

Switch NTI

Chassi DES6300

Módulos:

- DES-6305 100BASE-FX (SC) Module: módulo com oito portas de fibra ótica Fast Ethernet.
- DES-6308 1000BASE-T (RJ-45) Module: módulo com duas portas Gigabit Ethernet com interface elétrica RJ-45.
- DES-6309 GBIC Module: módulo com duas portas de fibra ótica Gigabit Ethernet, com interface GBIC

Switch Praia Vermelha

Chassi DES 6300

Módulos:

- DES-6304 100BASE-FX (MT-RJ) Module: módulo com doze portas de fibra ótica com conector MT-RJ.
- DES-6309 GBIC Module: módulo com duas portas de fibra ótica Gigabit Ethernet, com interface GBIC

Switch DES 1200 M

Módulos:

- DES-124F 100BASE-FX (SC) Module: módulo com quatro portas de fibra ótica Fast Ethernet
- DES-121T 1000BASE-T (RJ-45) Module: módulo com uma portas Gigabit Ethernet com interface elétrica RJ-45

Microcomputadores

Foram utilizadas três máquinas para testes e configuração dos equipamentos, sendo dois PCs e um *laptop*. Os PCs foram utilizados para a geração de tráfego, executando o cliente e o servidor das ferramentas avaliadas, e para configuração via console (linha de comando) dos *switches*. O *laptop* foi utilizado para configuração via interface gráfica e para gerenciamento dos *switches*, utilizando o *software* proprietário Config Master.

HOST	PC1	PC2	LAPTOP
Sistema Operacional	Linux	Linux Windows	Linux Windows
CPU	Athlon XP 2000+ (@1667MHz)	Athlon XP 2000+ (@1667MHz)	Athlon XP 1500+ (@1300MHz)
Placa mãe	ASUS A7N266-VM	ASUS A7N266-VM	HP Laptop (chipset Via KT133/KM133
Memória	256 MB DDR400	256 MB DDR400	512 MB PC133
HD	80GB ATA100	80GB ATA100	30GB ATA66
Eth0	Nforce LAN On-board (10/100 Mbps)	Nforce LAN On-board (10/100 Mbps)	Via Rhine II 10/100 Integrada
Eth1	-	Via Rhine III 10/100 Mbps PCI	-

Config Master

ConfigMaster e uma aplicação baseada em SNMP que configura, monitora e realiza diagnostico de problemas nos equipamentos Dlink, seja através da estação de gerência ou seja remotamente utilizando um *web browser* como interface. O ConfigMaster prove gráficos *on line* a partir das variáveis MIB que monitoram a performance do equipamento.

ConfigMaster e acessado através de uma interface gráfica que exibe o painel frontal do equipamento. Os indicadores do painel, como LEDs, são espelhados na interface gráfica e visualizado pelo gerente da rede, conforme exemplificado na figura 7.3.

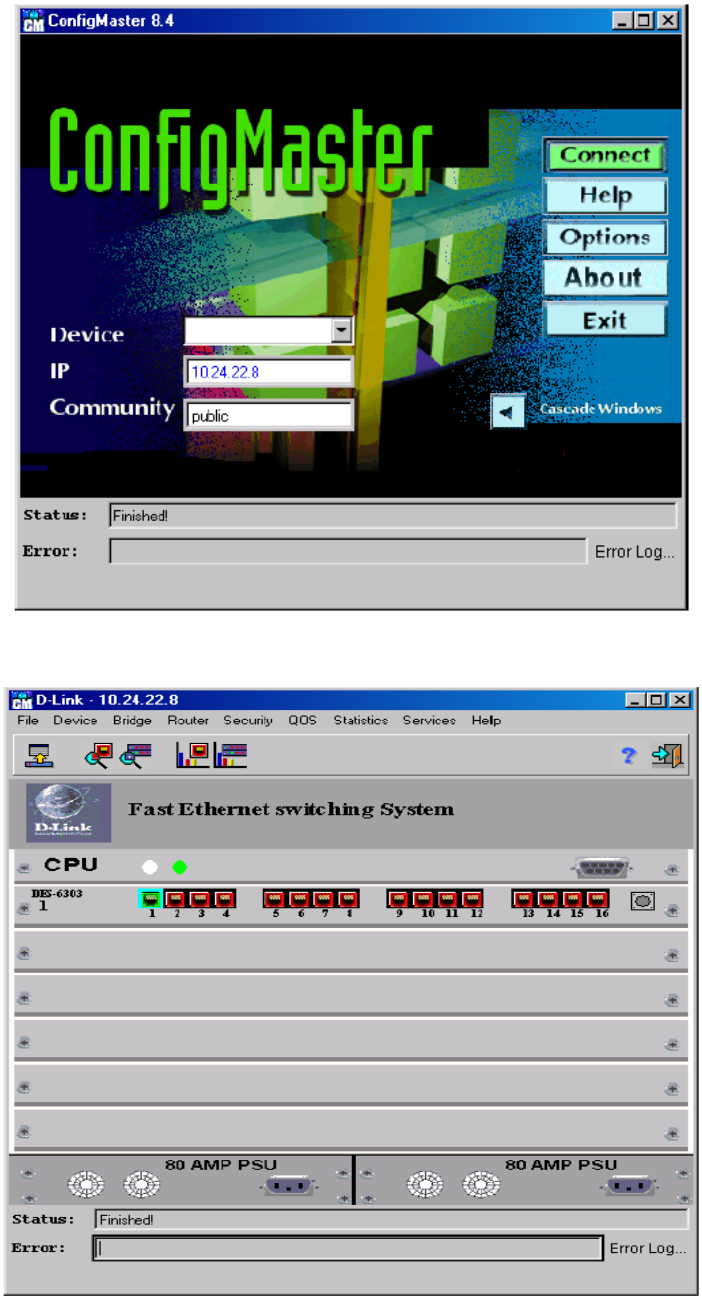


Figura 7.3 Config Master

7.2.2. Caso 2 – Homologação do switch DES 6500

Num segundo momento foi avaliado o *switch* DES 6500 em substituição ao *switch* DES 6300, devido aos muitos problemas apresentados por este equipamento e às grandes dificuldades de configuração derivadas da sua interface de gerenciamento. O DES 6500 é um equipamento de maior capacidade que substitui o DES 6300, retirado do mercado pela Dlink.

DES 6500

O DES 6500, assim como o DES6300, é um *switch router* do tipo chassi, que pode ser configurado com diversos módulos de interface. Suas principais características são:

- Backplane de 160 Gigabit/sec (Gbps).
- Comutação de camada 2 baseada em endereços MAC e no parâmetro VLAN ID
- Suporte ao padrão IEEE 802.1Q VLAN (*Static* VLAN)
- Suporte ao padrão IEEE 802.1d *Spanning Tree*
- Suporte à priorização de tráfego 802.1p
- Capacidade de agregação de portas (*Port trunking*)
- Espelhamento de portas (*Port mirroring*)
- Suporte a cliente DHCP
- Suporte ao protocolo de roteamento RIP, versões 1 e 2
- Suporte ao protocolo de roteamento OSFP
- Suporte a IGMP, IP Multicast e a mecanismos de QoS (*Quality of Service*)
- Suporte aos protocolos de roteamento multicast: DVMRP, PIM DM
- Suporte a ACL – *Access Control List*

Configuração do laboratório

De forma semelhante ao estudo de caso 1 a topologia, mostrada na figura 7.4, procura simular o *backbone* da UFF, utilizando três *switches*. Porém neste caso foi disponibilizado apenas um DES 6500, interligado a *switches* DES-3226S por enlaces Ethernet 100Mbps e 1Gbps.

Foram mantidas as duas máquinas PC Linux utilizadas para configurar via console os *switches*, e como cliente e servidor para as ferramentas de medição e geração de tráfego. Também foi mantido o *laptop* com o *software* ConfigMaster para a configuração e monitoração dos equipamentos via interface gráfica.

A figura 7.4 apresenta a configuração utilizada no caso 2.

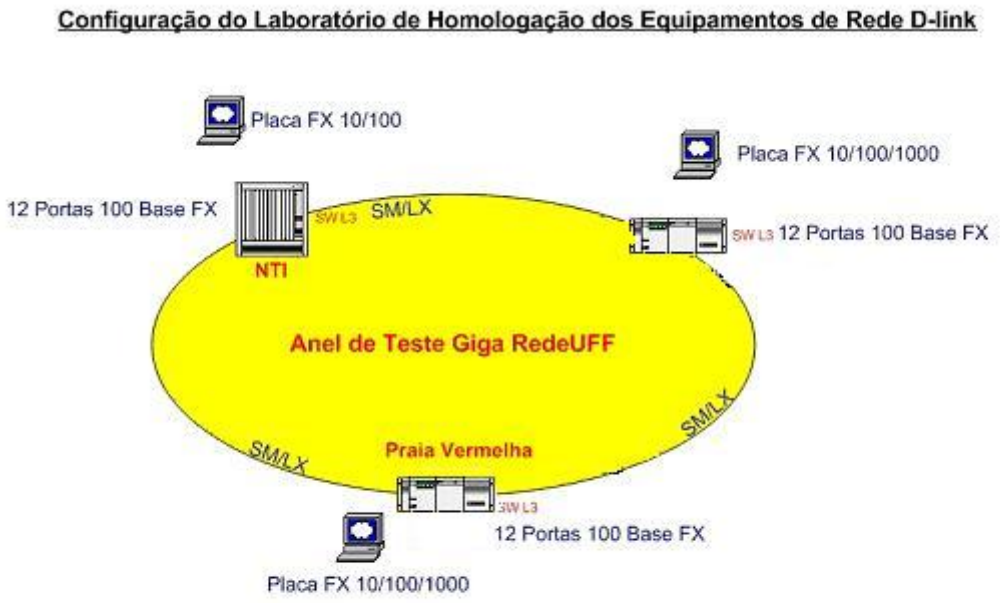


Figura 7.4 Configuração utilizada do laboratório

Switch NTI

Chassi DES6500

Módulos:

- DES-6505 8-port 1000BASE-SX (SC): Módulo com 8 portas de fibra, interface SC, Gigabit Ethernet.
- DES-6507 12-port 10BASE-T/100BASE-TX/1000BASE-T: Módulo com 12 portas Ethernet/Fast Ethernet/Gigabit Ethernet com interface elétrica RJ-45.
- DES-6509 12-port Mini GBIC(SFP): Módulo com 12 portas de fibra ótica Gigabit Ethernet, com interface mini GBIC

Switch DES 3226 S

Chassi 3226 S com 24 portas 10/100BASE-TX e um *slot* livre.

Módulos:

- DES-134T 2-Port Fiber 1000BaseSX (SC-Duplex): Módulo com duas portas de fibra ótica SC, Gigabit Ethernet

Microcomputadores

Foram utilizadas as mesmas máquinas do caso 1, dois PCs e um *laptop*. Os PCs foram utilizados para a geração de tráfego e para configuração via console dos *switches*. O

laptop foi mantido para configuração e gerenciamento utilizando o *software* Config Master, já descrito anteriormente .

7.3. Descrição dos testes

Foram realizados testes de homologação dos *switches* Dlink para sua aquisição e utilização no backbone da UFF. Estes testes se destinam a verificar o correto funcionamento dos equipamentos, tanto em ambiente de laboratório, quando todas as suas funcionalidades e características são testadas individualmente, como em ambiente de produção, aonde é testado o desempenho do *switch* em uma situação de carga real.

Para determinação dos testes foram identificados os itens a serem avaliados através da especificação dos equipamentos, sendo esta a referência para aceitação dos resultados. A partir deste ponto inicial foram definidas as características de interesse dos fluxos de dados a serem gerados de forma que possam fornecer a carga adequada para cada teste e explicitar as informações relevantes mais facilmente.

Dentre os vários tipos de dados possíveis de serem gerados e transmitidos procurou-se utilizar uma mistura que reflita de forma realista o tráfego de redes IP em operação. Para isto foram selecionadas ferramentas capazes de gerar diferentes perfis de tráfego e simular várias aplicações.

Uma primeira etapa envolveu a geração e medição de tráfego utilizando cada uma das ferramentas individualmente. Em um segundo momento foi feita a execução concorrente das ferramentas DITG e Iperf, sendo consideradas respectivamente como fonte de tráfego de teste e fonte de tráfego de fundo. Os ítens a seguir descrevem a metodologia dos testes executados e a seção 7.2.4 apresenta os resultados mais significativos. A íntegra dos resultados de todos os experimentos realizados se encontra no CD fornecido em anexo.

Testes de hardware - falhas

Os *switches* possuem a facilidade de *hot swap* de módulos e fonte redundante, que permitem maior tolerância a falhas e aumentam o tempo de disponibilidade do equipamento. Estes testes simulam situações de falha da fonte de alimentação e de troca de módulos sem o desligamento do *switch* (*hot swap*).

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Hot Swap	Remoção dos módulos durante operação normal do switch	Continuidade da operação do switch e manutenção das configurações após a recolocação do módulo	Retardo e Perda de Pacotes
Fonte Redundante	Remoção da fonte principal durante operação normal do switch para teste da fonte redundante	Continuidade da operação normal do switch	Retardo e Perda de Pacotes

Para execução destes testes foi gerado tráfego com vários fluxos a diferentes taxas com perfil constante, até o máximo da ferramenta, e pacotes com payload de tamanho constante, variando nos diferentes fluxos entre 512 Bytes e um valor máximo em torno de 1400 Bytes (MTU – cabeçalho IP), para verificar se há perda de pacotes, e caso haja a partir de que taxa e tamanho de pacote. Isto permite:

→ No caso de fonte redundante, estimar quanto tempo é gasto na troca da origem da alimentação,

→ No caso de *hot swap* dos módulos, verificar se há algum impacto nos fluxos de outros módulos.

Testes de roteamento

Os equipamentos testados funcionam também como roteadores, encaminhando pacotes de camada 3 – IP, IPX , Apple Talk e outros, utilizando os protocolos de roteamento OSPF e RIP (v.1 e v.2). O DES 6300 também suporta IGMP, IP Multicast e DHCP . Os testes de roteamento verificaram apenas o funcionamento dos protocolos RIP e OSPF.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Roteamento Configuração	Configuração de roteamento estático, RIP e OSPF	Descoberta de rotas e envio das tabelas de roteamento de acordo com cada protocolo	Retardo Perda de Pacotes Jitter
Roteamento Falha	Desligamento de uma ou mais conexões	Estabelecimento de uma nova configuração	Retardo Perda de Pacotes Jitter

Nestes testes foram utilizados fluxos simulando os serviços Telnet, DNS e VoIP, e simulando também o tráfego "genérico" (p2p + http + ftp + outros), com taxa e *payload* de perfis variáveis, de forma a oferecer uma carga realista para os algoritmos de roteamento. Além destes fluxos, foi gerado também um fluxo a taxa constante com os parâmetros máximos das ferramentas e/ou retirados dos testes anteriores para servir como referência para avaliar retardo, perda de pacotes e jitter, especialmente para o teste de falha de roteamento.

Para avaliação destes testes é necessário observar além das métricas de interesse indicadas na tabela acima, as tabelas de rotas dos equipamentos que informam quais as rotas utilizadas em um determinado momento.

Testes de agregação (trunking)

Os *switches* permitem a configuração de portas formando um agregado lógico de camada 2. Utilizando este agregado é possível interligar o *switch* a outro *switch* ou a um servidor, por exemplo, a taxas superiores às das interfaces disponíveis e com balanceamento do tráfego entre as portas.

Entretanto estes equipamentos possuem a limitação de não utilizar portas pertencentes a VLANs nem portas configuradas com endereços IP para a formação dos agregados.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Agregação Configuração	Configuração de enlaces agregados em uma mesma rede e configurar uma rota alternativa ao agregado	Envio de pacotes através do enlace agregado	Vazão Utilização do Enlace Banda disponível
Agregação Falha	Desligamento de uma ou mais conexões	Tempo de resposta de reconfiguração	Retardo Perda de Pacotes Vazão Utilização do Enlace Banda disponível

Para testar a facilidade de trunking foi utilizado tráfego gerado à taxa máxima com tamanho de pacote máximo, de forma a gerar o maior volume de tráfego possível a ser transmitido pelo agregado. A verificação do envio dos pacotes através do enlace agregado é feita através das estatísticas das portas do *switch*.

Testes de spanning tree

A habilitação do protocolo de *spanning tree* entre *switches* evita a formação de anéis, identificando e desabilitando caminhos redundantes. Os caminhos desabilitados passam então a funcionar como sobressalentes (*backups*), sendo utilizados em caso de falha do enlace ativo. As portas configuradas como agregados são exceções para o protocolo de *spanning tree*, sendo tratadas como uma única porta.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Spanning Tree Configuração	Configuração de um anel e habilitação do spanning tree	Desabilitação do anel	Retardo Perda de Pacotes Utilização do Enlace
Spanning Tree Falha	Desligamento de uma ou mais conexões	Reconfiguração do spanning tree e Tempo de reposta	Retardo Perda de Pacotes Utilização do Enlace

De forma semelhante ao teste de hardware, foi gerado tráfego com vários fluxos a diferentes taxas (constante, até o máximo da ferramenta) e pacotes com payload de tamanho constante, variando nos diversos fluxos entre 512 Bytes e máximo 1462 Bytes (MTU – cabeçalho IP), para verificar se há perda de pacotes, e caso haja a partir de que taxa e tamanho de pacote, e estimar em quanto tempo o protocolo de *spanning tree* desabilita o anel e reconfigura um novo caminho em caso de falha.

Testes de VLAN

Através da configuração de VLANs (*Virtual LANs*) é possível delimitar os domínios de *broadcast*, isolando em um grupo apenas as máquinas de interesse em um ou mais segmentos de rede, compartilhando recursos e evitando *broadcast storms*.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
VLAN Configuração	Configuração de VLANs	Conectividade entre os membros da VLAN e isolamento dos não membros.	Conectividade

Para execução deste teste foi gerado tráfego com fluxos com taxa e payload constante entre portas a serem separadas pela criação de uma VLAN de forma a verificar o isolamento dos membros da VLAN. Gerar o mesmo tráfego entre duas portas membros de uma mesma VLAN e verificar a sua conectividade.

Testes de ACL

Access Control Lists – ACLs contribuem para melhorar a segurança da rede, limitando o tipo de tráfego que pode entrar ou sair. ACLs são usadas para evitar que determinados pacotes sejam encaminhados por um roteador, permitindo a restrição de acesso a fluxos com perfis especificados, de forma a implementar políticas de segurança e de utilização de recursos. Os limites podem ser baseados no protocolo e no número da porta utilizados para controlar o tráfego de entrada e de saída.

Na especificação deste equipamento está descrita a utilização de ACL baseada em protocolos apenas para IP, não sendo possível a configuração de ACL baseada em serviço (portas) e em outros protocolos.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
ACL Configuração	Instalação de ACLs baseadas em MAC e porta (física e lógica)	Bloqueio de conexões não autorizadas	Conectividade

Para este teste devem ser gerados diversos fluxos tanto para serem aceitos como para serem recusados, de acordo com os parâmetros avaliados pelo *switch* para permitir o acesso. Entretanto esta facilidade não foi testada devido às inúmeras dificuldades de configuração encontradas pela equipe encarregada da homologação.

Testes de QoS

A possibilidade de implementação dos mecanismos de qualidade de serviço (QoS) está se tornando cada vez mais um requisito importante para os equipamentos de rede, acompanhando a tendência mundial de buscar uma melhor utilização das redes ao mesmo tempo em que é provido ao cliente um serviço diferenciado. Existem mecanismos de QoS que atuam na camada 2 (802.1p) e camada 3 (intserv, diffserv, mpls), priorizando pacotes, realizando controle da banda utilizada, reserva de recursos e controle de admissão de fluxos. Para isto é necessário configurar filtros de pacotes, filas internas e algoritmos de escalonamento de forma a refletir a política de QoS adotada, assegurando a cada classe de serviço o atendimento aos parâmetros de qualidade definidos – retardo, perda de pacotes, jitter e vazão (*bit rate*).

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Classificação e priorização camadas 2 e 3 Configuração	Configurar filtros, filas e escalonamento	Operação dentro dos parâmetros pré-definidos	Retardo Perda de Pacotes Jitter Vazão Tempo de conexão
Classificação e priorização camadas 2 e 3 Falha	Desligamento de uma ou mais conexões	Operação dentro dos parâmetros pré-definidos	Retardo Perda de Pacotes Jitter Vazão
Controle de banda	Configurar policiamento e shapping	Condicionamento do tráfego (descarte e retardo de pacotes)	Retardo Perda de Pacotes Jitter Vazão Utilização do Enlace Banda disponível Tempo de conexão
Controle de admissão de conexões	Configurar cac baseado em parâmetros	Aceitação ou rejeição de conexões	Conectividade Utilização do Enlace Banda disponível Tempo de conexão
RSVP Configuração	Configurar reservas	Estabelecimento e liberação de reservas e operação dentro dos parâmetros pré-definidos	Retardo Perda de Pacotes Jitter Vazão Utilização do Enlace Banda disponível Tempo de conexão
RSVP Falha	Desligamento de uma ou mais conexões	Estabelecimento de uma nova reserva	Retardo Perda de Pacotes Jitter Vazão Utilização do Enlace Banda disponível

Para testes de QoS é necessário gerar fluxos com as características que podem ser identificadas pelos *switches* de modo a fornecer volume de tráfego a ser filtrado e tratado de acordo com as regras de QoS e policiamento. Dentre estas características se encontram os campos DSCP, TOS, endereços de origem e destino, portas de origem e destino e etc. Devem ser configuradas ações incluindo descarte, *shapping* e priorização de pacotes .

Testes de desempenho

Os últimos testes se destinam a verificar o desempenho dos equipamentos em situações que simulam o ambiente de produção, de forma a observar o seu funcionamento em condições de operação normal e de sobrecarga.

TESTE	AÇÃO	RESULTADO	MÉTRICA DE INTERESSE
Módulo	Gerar várias conexões	Saturação	Retardo Perda de Pacotes Vazão Utilização do Enlace
Backplane	Gerar pacotes de tamanho máximo	Saturação	Retardo Perda de Pacotes Vazão Utilização do Enlace
Forwarding camada 3	Gerar pacotes de tamanho mínimo	Saturação	Retardo Perda de Pacotes Vazão Utilização do Enlace
ACL	Configurar (v. testes específicos)	Degradação de desempenho	Conectividade Retardo Perda de Pacotes Vazão Utilização do Enlace
QoS	Configurar (v. testes específicos)	Degradação de desempenho	Retardo Perda de Pacotes Jitter Vazão Utilização do Enlace

Estes testes envolvem a geração do volume máximo possível de trafego, utilizando diversos fluxos, espelhamento de portas (*mirroring*) e roteamento estático de forma a obter a saturação dos componentes em teste. Devem ser monitoradas métricas que indicam alguma degradação no desempenho durante estes testes.

7.4. Resultados do caso 1 – DES 6300

Foram realizados mais de 50 experimentos de geração e medição de tráfego para viabilizar a realização dos testes descritos acima. Alguns destes experimentos estão descritos a seguir, exemplificando a utilização das ferramentas.

1. *Teste de Hot-Swap*

Neste experimento foram gerados múltiplos fluxos de tráfego TCP pela ferramenta DITG com medição rttm para a realização do teste de *hardware – hot swap*, tanto

dos módulos como da fonte redundante. O *switch* se manteve em operação, sem apresentar queda no desempenho nem degradação na qualidade dos fluxos, conforme ilustrado pelos gráficos a seguir.

Tráfego gerado

Foram gerados dois fluxos, TCP e UCP, através da utilização do *script* abaixo.

```
-a 192.168.1.4 -m rttm -rp 9500 -C 100 -c 500 -t 20000
-a 192.168.1.4 -m rttm -rp 9501 -C 1000 -u 500 1000 -t 20000
```

O primeiro fluxo possui as seguintes características:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 9500
- intervalo entre pacotes (-C): constante – 100 pacotes por segundo
- *payload* (-c): constante – 500 bytes
- protocolo: TCP
- duração (-t): 20000 milissegundos

Características do segundo fluxo:

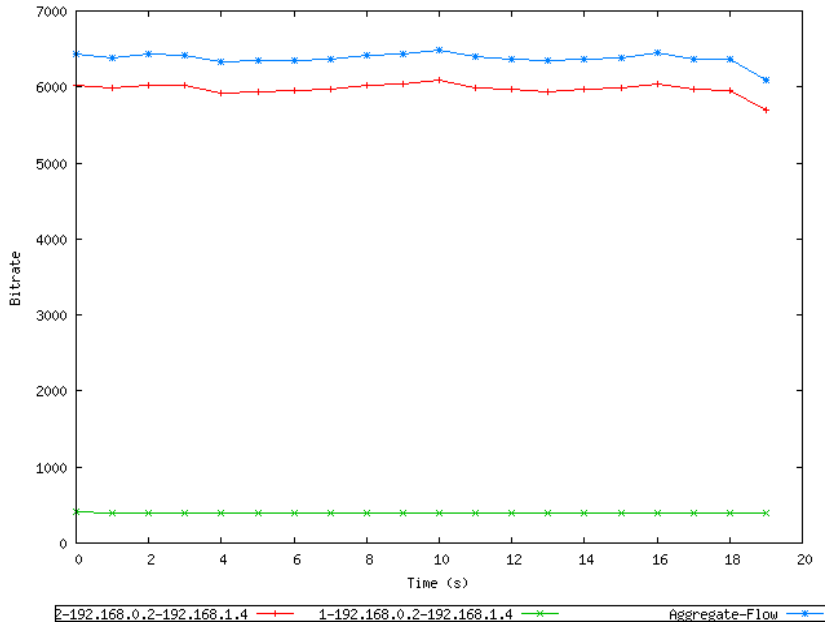
- medição (-m): bidirecional (rttm)
- porta remota (-rp): 9501
- intervalo entre pacotes (-C): constante – 1000 pacotes por segundo
- *payload* (-u): distribuição uniforme de 500 bytes a 1000 bytes
- protocolo: TCP
- duração (-t): 20000 milissegundos

Tráfego recebido

```
bash-2.05b# /usr/src/ditg/ITG/bin/ITGDec receiver1201051930
------------------------------------------------------------
Flow number: 2
From 192.168.0.2:32770
To   192.168.1.4:9501
------------------------------------------------------------
Total time              =     19.949684 s
Total packets           =         19950
Minimum delay           =  45590.721629 s
Maximum delay           =  45590.725880 s
Average delay           =  45590.721866 s
Average jitter          =      0.000116 s
Delay standard deviation =      0.003537 s
Bytes received          =      14940814
Average bitrate         =   5991.398761 Kbit/s
```

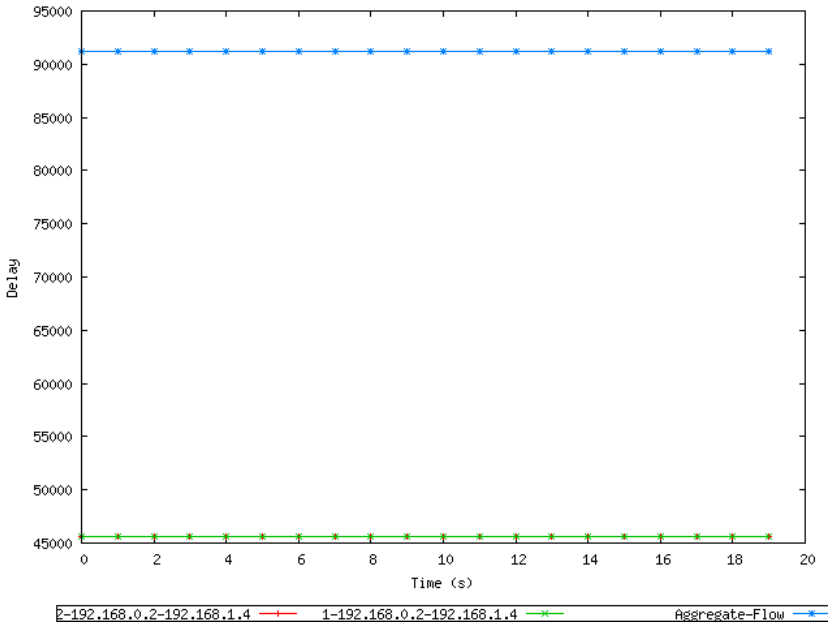
```
Average packet rate      =   1000.015840 pkt/s
Packets dropped          =            1 (0.01 %)
---------------------------------------------------------
---------------------------------------------------------
Flow number: 1
From 192.168.0.2:32769
To    192.168.1.4:9500
---------------------------------------------------------
Total time               =     19.989333 s
Total packets            =          2000
Minimum delay            =  45590.721630 s
Maximum delay            =  45590.725817 s
Average delay            =  45590.721801 s
Average jitter           =      0.000114 s
Delay standard deviation =      0.000915 s
Bytes received           =       1000000
Average bitrate          =    400.213454 Kbit/s
Average packet rate      =    100.053363 pkt/s
Packets dropped          =            0 (0.00 %)
---------------------------------------------------------

_____________________________________________________________
**********  TOTAL RESULTS   **********

_____________________________________________________________
Number of flows          =            2
Total time               =     19.989333 s
Total packets            =         21950
Minimum delay            =  45590.721629 s
Maximum delay            =  45590.725880 s
Average delay            =  45590.721860 s
Average jitter           =      0.000116 s
Delay standard deviation =      0.002841 s
Bytes received           =      15940814
Average bitrate          =   6379.728228 Kbit/s
Average packet rate      =   1098.085664 pkt/s
Packets dropped          =            1 (0.00 %)
Error lines              =            0
---------------------------------------------------------
bash-2.05b#
```

Gráfico bitrate x tempo (Kbps x s)



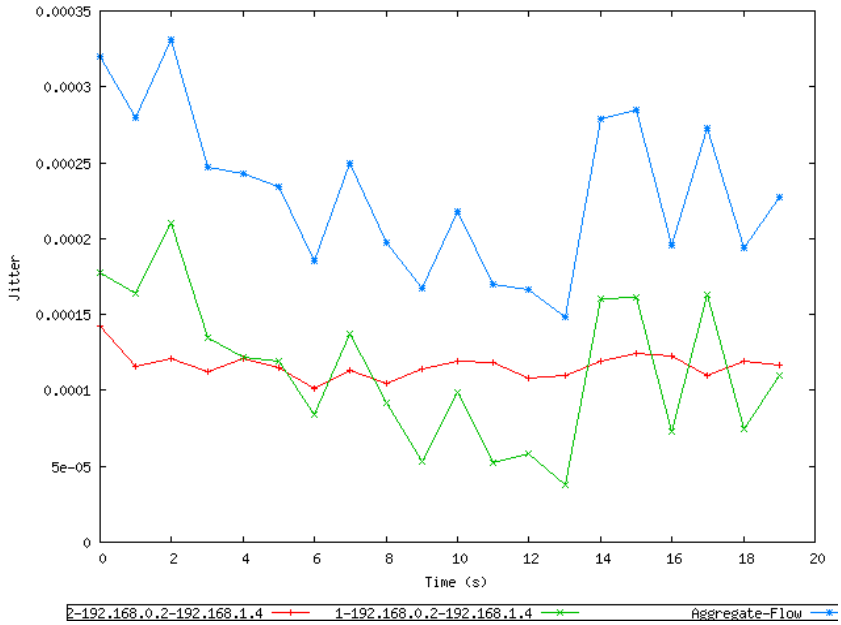
Neste gráfico podemos observar que não há redução da vazão (*bit rate*) de nenhum dos fluxos em função da troca de módulos em *hot swap*.

Gráfico delay x tempo (s x s)



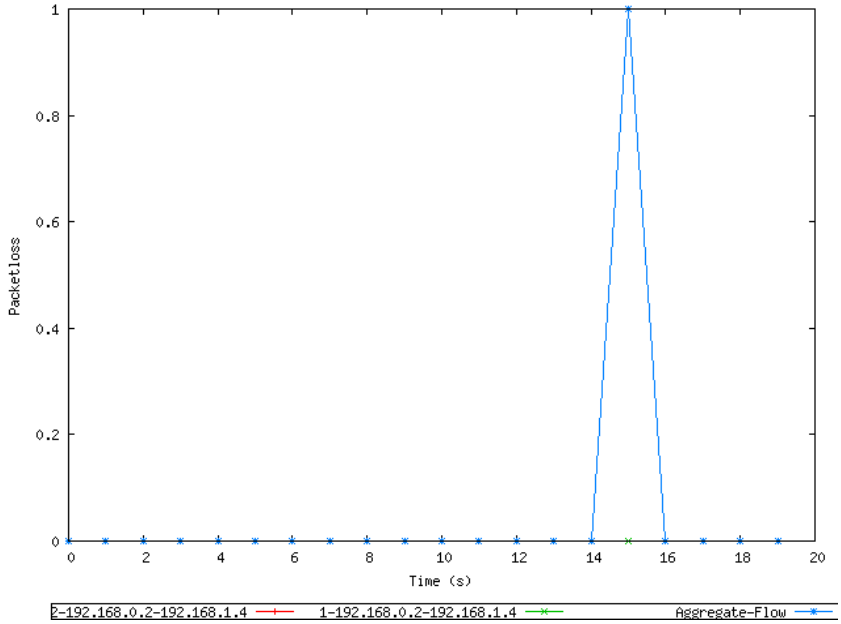
Ambos os fluxos apresentam o mesmo retardo e, como podemos observar neste gráfico, não há aumento do retardo (*delay*) em função da troca de módulos em *hot swap*.

Gráfico jitter x tempo (s x s)



Este gráfico mostra a variação do *jitter* durante a operação de *hot swap*. Observa-se um pequeno aumento no momento da troca dos módulos, cerca de 15 segundos após o início do experimento.

Gráfico packet loss x tempo (pacotes/s x s)



O gráfico acima mostra a perda de um pacote no momento da troca dos módulos, cerca de 15 segundos após o início do experimento.

2. *Teste de roteamento RIP*

Para este experimento foram gerados múltiplos fluxos TCP e UDP pela ferramenta DITG com medição rttm utilizados para teste do protocolo de roteamento RIP, tanto para verificar a descoberta e estabelecimento de rotas, bem como a reconfiguração das rotas no caso de uma falha. Como pode ser observado em todos os gráficos o equipamento em teste não atuou corretamente, causando uma grande perda de pacotes e degradando a qualidade dos fluxos durante o evento da falha.

Tráfego gerado

Foram gerados três fluxos TCP e dois fluxos UDP através da utilização do *script* abaixo.

```
-a 192.168.1.4 -m rttm -rp 9500 -C 100 -c 500 -t 200000
-a 192.168.1.4 -m rttm -rp 9501 -C 1000 -u 500 1000 -t 200000
-a 192.168.1.4 -m rttm -rp 9502 -C 1500 -u 500 1000 -t 200000
-a 192.168.1.4 -m rttm -rp 10001 -C 1000 -c 512 -T UDP -t 200000
-a 192.168.1.4 -m rttm -rp 10002 -C 2000 -c 512 -T UDP -t 200000
```

O primeiro e o segundo fluxo possuem respectivamente características idênticas às dos fluxos 1 e 2 do experimento 1, exceto pela duração de 200000ms deste experimento .

Características do terceiro fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 9502
- intervalo entre pacotes (-C): constante – 1500 pacotes por segundo
- *payload* (-u): distribuição uniforme de 500 bytes a 1000 bytes
- protocolo: TCP
- duração (-t): 200000 milissegundos

Características do quarto fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1001
- intervalo entre pacotes (-C): constante – 1000 pacotes por segundo
- *payload* (-c): distribuição : constante – 512 bytes
- protocolo (-T): UDP
- duração (-t): 200000 milissegundos

Características do quinto fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1002
- intervalo entre pacotes (-C): constante – 2000 pacotes por segundo

- *payload* (-c): distribuição : constante – 512 bytes
- protocolo (-T): UDP
- duração (-t): 200000 milissegundos

Tráfego recebido

```
[root@wefixd expfalharip3]# /root/dlink/ditg/bin/ITGDec receiver1401051702falharip   --
Flow number: 5
From 192.168.0.2:32807
To    192.168.1.4:10002
------------------------------------------------------------
Total time              =    204.160561 s
Total packets           =       182150
Minimum delay           =  45585.934221 s
Maximum delay           =  45587.233131 s
Average delay           =  45585.939991 s
Average jitter          =      0.000111 s
Delay standard deviation =      0.000000 s
Bytes received          =      93260800
Average bitrate         =   3654.410021 Kbit/s
Average packet rate     =    892.189947 pkt/s
Packets dropped         =       226176 (55.39 %)
------------------------------------------------------------
------------------------------------------------------------
Flow number: 2
From 192.168.0.2:32805
To    192.168.1.4:9501
------------------------------------------------------------
Total time              =    205.070955 s
Total packets           =       97100
Minimum delay           =  45585.934232 s
Maximum delay           =  45588.405352 s
Average delay           =  45585.941878 s
Average jitter          =      0.000289 s
Delay standard deviation =      0.012436 s
Bytes received          =      72737019
Average bitrate         =   2837.535681 Kbit/s
Average packet rate     =    473.494650 pkt/s
Packets dropped         =       107972 (52.65 %)
------------------------------------------------------------
------------------------------------------------------------
Flow number: 3
From 192.168.0.2:32809
To    192.168.1.4:9502
------------------------------------------------------------
Total time              =    204.917590 s
Total packets           =       137989
Minimum delay           =  45585.934222 s
Maximum delay           =  45588.396401 s
Average delay           =  45585.940611 s
```

Average jitter = 0.000193 s
Delay standard deviation = 0.010707 s
Bytes received = 103376230
Average bitrate = 4035.816740 Kbit/s
Average packet rate = 673.387775 pkt/s
Packets dropped = 165847 (54.58 %)

Flow number: 4
From 192.168.0.2:32806
To 192.168.1.4:10001

Total time = 205.097058 s
Total packets = 96100
Minimum delay = 45585.934222 s
Maximum delay = 45587.428099 s
Average delay = 45585.941618 s
Average jitter = 0.000236 s
Delay standard deviation = 0.005174 s
Bytes received = 49203200
Average bitrate = 1919.216218 Kbit/s
Average packet rate = 468.558647 pkt/s
Packets dropped = 109000 (53.14 %)

Flow number: 1
From 192.168.0.2:32808
To 192.168.1.4:9500

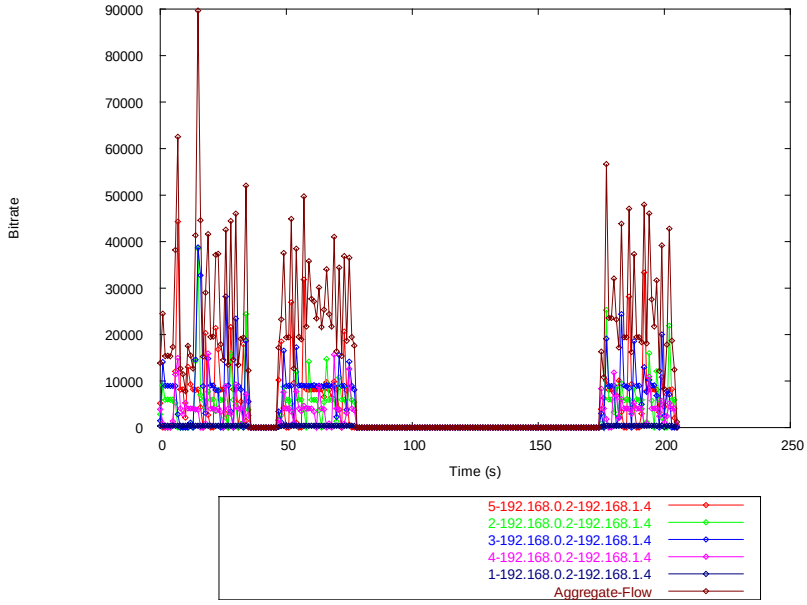
Total time = 204.598078 s
Total packets = 9400
Minimum delay = 45585.934221 s
Maximum delay = 45585.964007 s
Average delay = 45585.936937 s
Average jitter = 0.000479 s
Delay standard deviation = 0.005141 s
Bytes received = 4700000
Average bitrate = 183.774942 Kbit/s
Average packet rate = 45.943736 pkt/s
Packets dropped = 11061 (54.06 %)

********** TOTAL RESULTS **********

Number of flows = 5
Total time = 205.182732 s
Total packets = 522739
Minimum delay = 45585.934221 s
Maximum delay = 45588.405352 s
Average delay = 45585.940749 s
Average jitter = 0.000210 s

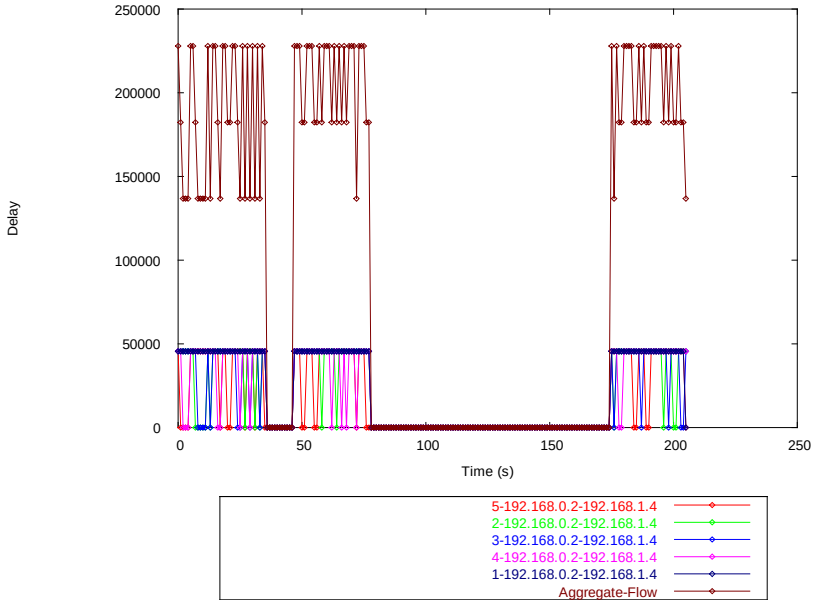
```
Delay standard deviation =      0.006274 s
Bytes received           =     323277249
Average bitrate          =  12604.462212 Kbit/s
Average packet rate      =   2547.675406 pkt/s
Packets dropped          =        620056 (54.26 %)
Error lines              =             0
-------------------------------------------------------------
[root@wefixd expfalharip3]#
```

Gráfico bitrate x tempo



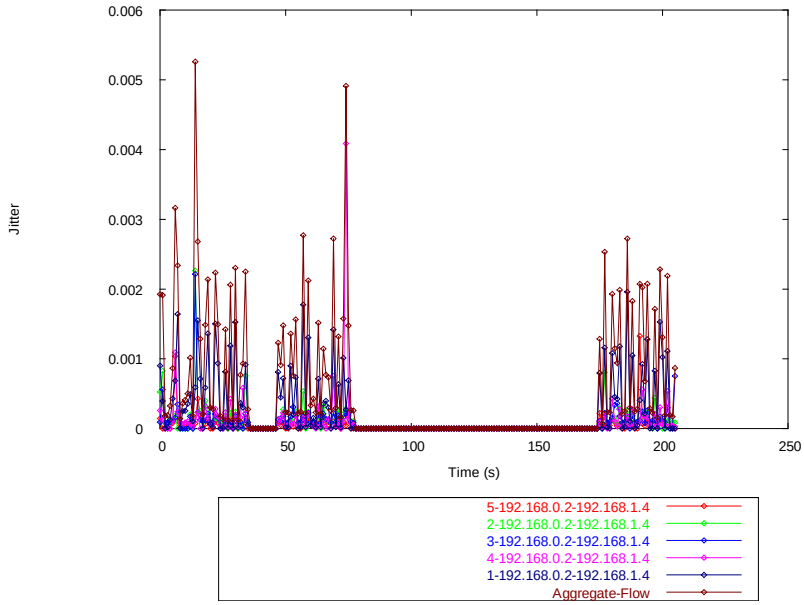
Este gráfico mostra a interrupção de envio de pacotes durante as duas falhas.

Gráfico delay x tempo



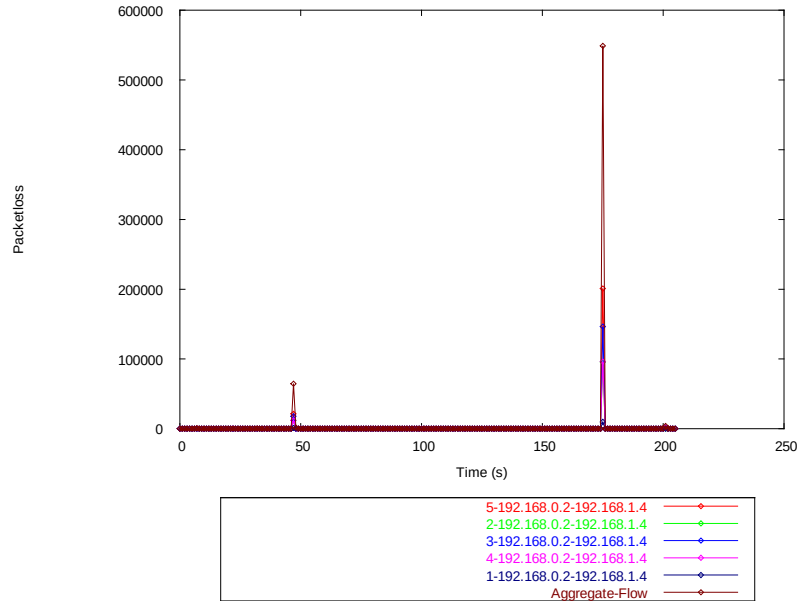
Neste gráfico o valor zero indica que nãohouve o recebimento dos pacotes durante os períodos de falha, não sendo possível o cáculo do retardo.

Gráfico jitter x tempo



De forma semelhante à medição do retardo, não foi possível a medição do *jitter* durante as falhas.

Gráfico packet loss x tempo



Em ambos os momentos de falha observa-se uma grande perda de pacotes, que só pode ser contabilizada no restabelecimento da conexão.

3. Simulação de DNS

Este experimento foi realizado para testar a geração de tráfego com o perfil da aplicação DNS, uma das opções da ferramenta DITG. Podemos observar pelo gráfico *bit rate* x tempo que este padrão de fato se assemelha ao de uma aplicação cliente/servidor, como é o caso do DNS, com períodos de transmissão de dados e períodos de silêncio aguardando o recebimento de pacotes de resposta e processando-os. Da mesma forma os valores máximo e médio estão dentro do esperado para DNS.

Tráfego gerado

Foi gerado fluxo simulando o perfil de tráfego da aplicação DNS através da utilização do script abaixo.

```
-a 192.168.1.4 -m rttm -rp 10006 DNS -t 20000
```

Características do fluxo:

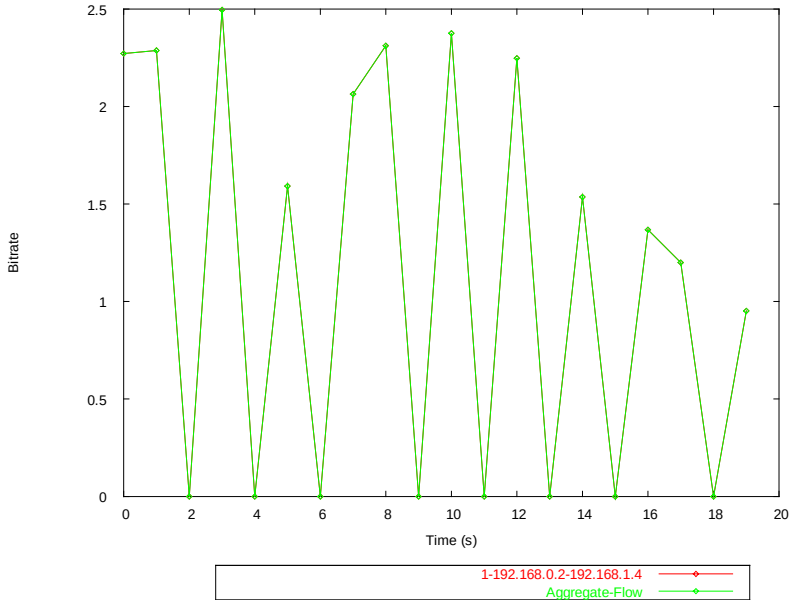
- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1006
- perfil do fluxo: simulação de DNS
- duração (-t): 200000 milissegundos

Tráfego recebido

```
[root@wefixd exp3]# /root/dlink/ditg/bin/ITGDec receiver1401051525
------------------------------------------------------------
Flow number: 1
From 192.168.0.2:32768
To    192.168.1.4:10006
------------------------------------------------------------
Total time              =     19.642594 s
Total packets           =          12
Minimum delay           =  45586.007303 s
Maximum delay           =  45586.007567 s
Average delay           =  45586.007425 s
Average jitter          =      0.000024 s
Delay standard deviation =      0.000000 s
Bytes received          =         2838
Average bitrate         =      1.155855 Kbit/s
Average packet rate     =      0.610917 pkt/s
Packets dropped         =          0 (0.00 %)
------------------------------------------------------------

_____
**********  TOTAL RESULTS   **********
_____
```

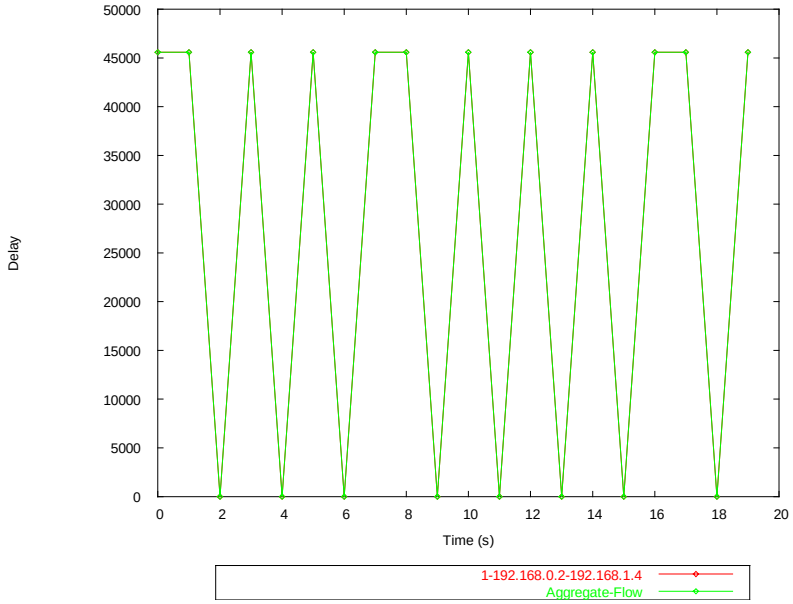
```
Number of flows         =           1
Total time              =     19.642594 s
Total packets           =          12
Minimum delay           =  45586.007303 s
Maximum delay           =  45586.007567 s
Average delay           =  45586.007425 s
Average jitter          =      0.000024 s
Delay standard deviation =      0.000000 s
Bytes received          =         2838
Average bitrate         =      1.155855 Kbit/s
Average packet rate     =      0.610917 pkt/s
Packets dropped         =           0 (0.00 %)
Error lines             =           0
-------------------------------------------------------------
[root@wefixd exp3]#
```

Gráfico bitrate x tempo



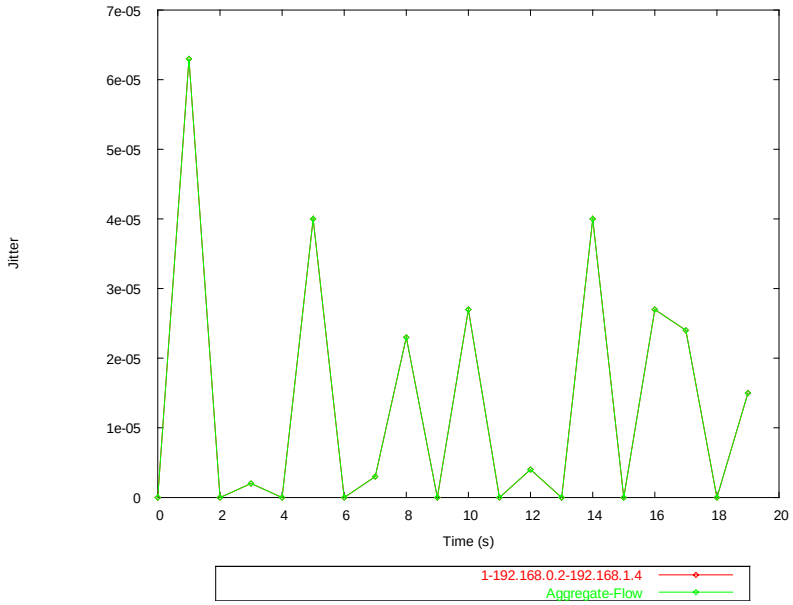
O gráfico mostra um padrão de transmissão típico de aplicações cliente/servidor como o DNS.

Gráfico delay x tempo



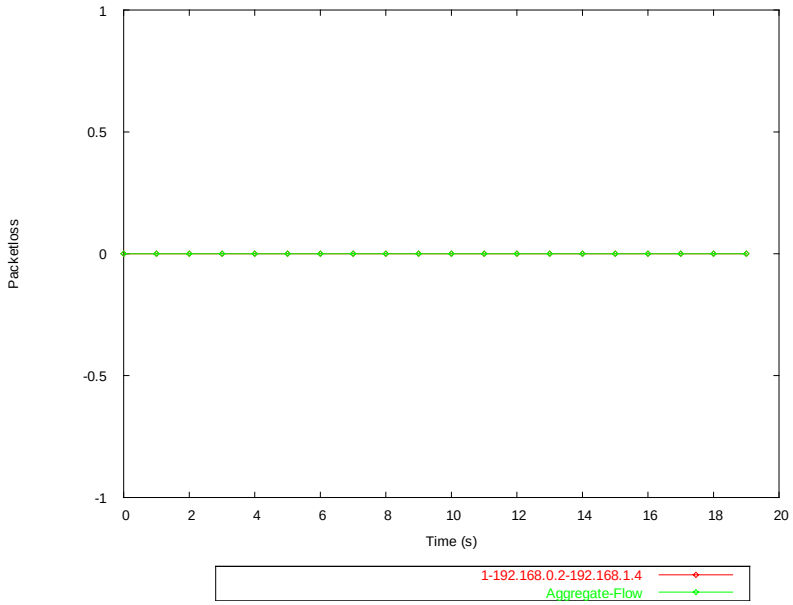
Acompanhando o padrão de transmissão, o retardo cai a zero quando não há envio de pacotes.

Gráfico jitter x tempo



O gráfico apresenta grande variação do *jitter* também devido aos momentos de silêncio.

Gráfico packet loss x tempo



Não há perda de pacotes, pois os momentos de interrupção de envio de pacotes devem-se ao perfil do fluxo e não a falhas ou perdas de qualquer espécie.

4. Teste de VLAN

Neste experimento foi feita a geração de tráfego simultânea por ambas as ferramentas com medição owdm utilizando portas pertencentes a uma mesma VLAN, de modo a verificar a conectividade entre as portas e o compartilhamento de fluxos de tráfego com diferentes perfis.

Tráfego gerado – Iperf

```
bash-2.05b# iperf -c 192.168.1.4 -t 200 -m
------------------------------------------------------------
Client connecting to 192.168.1.4, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 192.168.0.2 port 32771 connected with 192.168.1.4 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-200.0 sec  2.12 GBytes  91.2 Mbits/sec
[  5] MSS size 1448 bytes (MTU 1500 bytes, ethernet)
bash-2.05b#
bash-2.05b#
bash-2.05b# iperf -c 192.168.1.4 -t 200 -m
------------------------------------------------------------
Client connecting to 192.168.1.4, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 192.168.0.2 port 32774 connected with 192.168.1.4 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-200.0 sec  1.46 GBytes  62.5 Mbits/sec
[  5] MSS size 1448 bytes (MTU 1500 bytes, ethernet)
bash-2.05b# iperf -c 192.168.1.4 -t 200
```

Tráfego recebido – Iperf

Estão transcritos abaixo apenas alguns intervalos de medição da ferramenta Iperf, visto que o arquivo total é muito grande.

```
[  6] local 192.168.1.4 port 5001 connected with 192.168.0.2 port 32774
[ ID] Interval       Transfer     Bandwidth
[  6]  0.0- 1.0 sec  6.04 MBytes  50.7 Mbits/sec
[  6]  1.0- 2.0 sec  8.08 MBytes  67.8 Mbits/sec
[  6]  2.0- 3.0 sec  8.31 MBytes  69.7 Mbits/sec
[  6]  3.0- 4.0 sec  6.33 MBytes  53.1 Mbits/sec
[  6]  4.0- 5.0 sec  6.75 MBytes  56.6 Mbits/sec
[  6]  5.0- 6.0 sec  6.63 MBytes  55.6 Mbits/sec
[  6]  6.0- 7.0 sec  7.34 MBytes  61.6 Mbits/sec
[  6]  7.0- 8.0 sec  7.51 MBytes  63.0 Mbits/sec
[  6]  8.0- 9.0 sec  7.39 MBytes  62.0 Mbits/sec
[  6]  9.0-10.0 sec  7.21 MBytes  60.5 Mbits/sec
```

[6] 10.0-11.0 sec 7.56 MBytes 63.5 Mbits/sec
[6] 11.0-12.0 sec 8.09 MBytes 67.9 Mbits/sec
[6] 12.0-13.0 sec 8.66 MBytes 72.7 Mbits/sec
[6] 13.0-14.0 sec 4.78 MBytes 40.1 Mbits/sec
[6] 14.0-15.0 sec 8.62 MBytes 72.3 Mbits/sec
[6] 15.0-16.0 sec 6.53 MBytes 54.8 Mbits/sec
[6] 16.0-17.0 sec 7.69 MBytes 64.5 Mbits/sec
[6] 17.0-18.0 sec 6.36 MBytes 53.4 Mbits/sec
[6] 18.0-19.0 sec 7.05 MBytes 59.2 Mbits/sec
[6] 19.0-20.0 sec 8.00 MBytes 67.1 Mbits/sec

[ID] Interval   Transfer   Bandwidth
[6] 80.0-81.0 sec 8.21 MBytes 68.8 Mbits/sec
[6] 81.0-82.0 sec 8.56 MBytes 71.8 Mbits/sec
[6] 82.0-83.0 sec 4.73 MBytes 39.7 Mbits/sec
[6] 83.0-84.0 sec 7.95 MBytes 66.7 Mbits/sec
[6] 84.0-85.0 sec 8.52 MBytes 71.5 Mbits/sec
[6] 85.0-86.0 sec 5.91 MBytes 49.6 Mbits/sec
[6] 86.0-87.0 sec 8.46 MBytes 71.0 Mbits/sec
[6] 87.0-88.0 sec 8.58 MBytes 71.9 Mbits/sec
[6] 88.0-89.0 sec 6.64 MBytes 55.7 Mbits/sec
[6] 89.0-90.0 sec 5.47 MBytes 45.9 Mbits/sec
[6] 90.0-91.0 sec 7.62 MBytes 63.9 Mbits/sec
[6] 91.0-92.0 sec 7.55 MBytes 63.3 Mbits/sec
[6] 92.0-93.0 sec 7.56 MBytes 63.4 Mbits/sec
[6] 93.0-94.0 sec 7.56 MBytes 63.5 Mbits/sec
[6] 94.0-95.0 sec 7.10 MBytes 59.5 Mbits/sec
[6] 95.0-96.0 sec 7.61 MBytes 63.9 Mbits/sec
[6] 96.0-97.0 sec 7.28 MBytes 61.1 Mbits/sec
[6] 97.0-98.0 sec 7.43 MBytes 62.4 Mbits/sec
[6] 98.0-99.0 sec 7.52 MBytes 63.1 Mbits/sec
[6] 99.0-100.0 sec 7.52 MBytes 63.1 Mbits/sec

[ID] Interval   Transfer   Bandwidth
[6] 180.0-181.0 sec 7.80 MBytes 65.4 Mbits/sec
[6] 181.0-182.0 sec 7.69 MBytes 64.5 Mbits/sec
[6] 182.0-183.0 sec 8.64 MBytes 72.5 Mbits/sec
[6] 183.0-184.0 sec 8.79 MBytes 73.7 Mbits/sec
[6] 184.0-185.0 sec 5.75 MBytes 48.3 Mbits/sec
[6] 185.0-186.0 sec 8.85 MBytes 74.2 Mbits/sec
[6] 186.0-187.0 sec 7.74 MBytes 64.9 Mbits/sec
[6] 187.0-188.0 sec 5.10 MBytes 42.7 Mbits/sec
[6] 188.0-189.0 sec 7.57 MBytes 63.5 Mbits/sec
[6] 189.0-190.0 sec 7.54 MBytes 63.2 Mbits/sec
[6] 190.0-191.0 sec 7.63 MBytes 64.0 Mbits/sec
[6] 191.0-192.0 sec 7.81 MBytes 65.5 Mbits/sec
[6] 192.0-193.0 sec 7.76 MBytes 65.1 Mbits/sec
[6] 193.0-194.0 sec 7.80 MBytes 65.4 Mbits/sec
[6] 194.0-195.0 sec 7.81 MBytes 65.5 Mbits/sec
[6] 195.0-196.0 sec 6.65 MBytes 55.8 Mbits/sec
[6] 196.0-197.0 sec 9.48 MBytes 79.5 Mbits/sec
[6] 197.0-198.0 sec 8.36 MBytes 70.1 Mbits/sec

```
[  6] 198.0-199.0 sec  4.05 MBytes  34.0 Mbits/sec
[  6]  0.0-200.0 sec  1.46 GBytes  62.6 Mbits/sec

[  6] MSS size 1448 bytes (MTU 1500 bytes, ethernet)
[  6] Read lengths occurring in more than 5% of reads:
[  6]  1448 bytes read 848515 times (93.3%)
```

Tráfego gerado - DITG

Foram gerados três fluxos TCP e dois fluxos UDP através da utilização de um *script* semelhante ao já usado no experimento 2, diferindo pela taxa de pacotes por segundo duplicada para todos os fluxos, pela duração que neste experimento foi de 500000ms e pelo tipo de medição owdm.

Tráfego recebido - DITG

```
bash-2.05b# ./ITGDec /usr/dlink/ditg/170105/receiver1701051742iperf
------------------------------------------------------------
Flow number: 3
From 192.168.0.2:32769
To    192.168.1.4:9502
------------------------------------------------------------
Total time              =    499.977231 s
Total packets           =       745000
Minimum delay           =  45568.542309 s
Maximum delay           =  45570.972676 s
Average delay           =  45568.555913 s
Average jitter          =      0.000265 s
Delay standard deviation =      0.008955 s
Bytes received          =     558455058
Average bitrate         =   8935.687841 Kbit/s
Average packet rate     =   1490.067855 pkt/s
Packets dropped         =         4959 (0.66 %)
------------------------------------------------------------
------------------------------------------------------------
Flow number: 2
From 192.168.0.2:32770
To    192.168.1.4:9501
------------------------------------------------------------
Total time              =    498.776415 s
Total packets           =       497050
Minimum delay           =  45568.542302 s
Maximum delay           =  45572.883623 s
Average delay           =  45568.556494 s
Average jitter          =      0.000344 s
Delay standard deviation =      0.009742 s
Bytes received          =     372603787
```

Average bitrate = 5976.285579 Kbit/s
Average packet rate = 996.538700 pkt/s
Packets dropped = 1715 (0.34 %)

Flow number: 5
From 192.168.0.2:32771
To 192.168.1.4:10002

Total time = 499.963501 s
Total packets = 991600
Minimum delay = 45568.542182 s
Maximum delay = 45570.516777 s
Average delay = 45568.555491 s
Average jitter = 0.000200 s
Delay standard deviation = 0.016987 s
Bytes received = 507699200
Average bitrate = 8123.780220 Kbit/s
Average packet rate = 1983.344780 pkt/s
Packets dropped = 8338 (0.83 %)

Flow number: 4
From 192.168.0.2:32772
To 192.168.1.4:10001

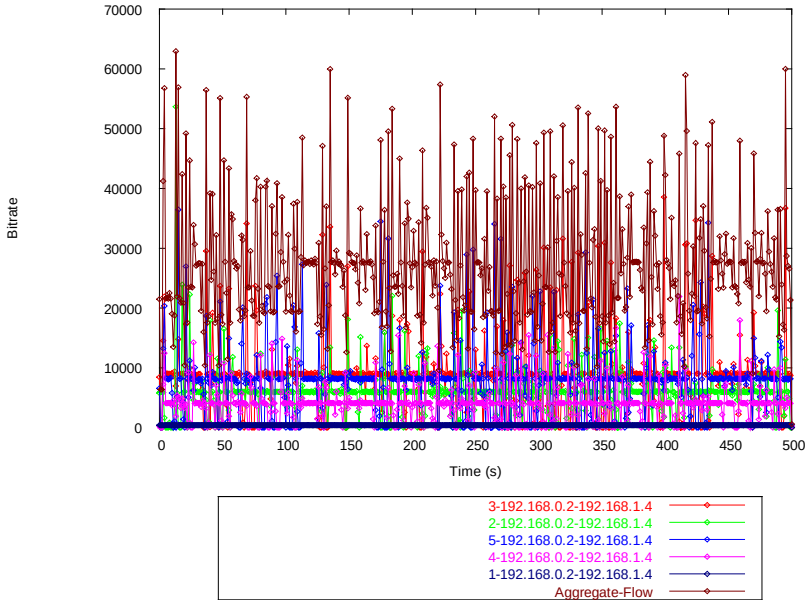
Total time = 499.905416 s
Total packets = 496050
Minimum delay = 45568.542241 s
Maximum delay = 45571.301264 s
Average delay = 45568.557024 s
Average jitter = 0.000293 s
Delay standard deviation = 0.011559 s
Bytes received = 253977600
Average bitrate = 4064.410456 Kbit/s
Average packet rate = 992.287709 pkt/s
Packets dropped = 3867 (0.77 %)

Flow number: 1
From 192.168.0.2:32768
To 192.168.1.4:9500

Total time = 499.986388 s
Total packets = 49935
Minimum delay = 45568.542215 s
Maximum delay = 45568.705187 s
Average delay = 45568.553131 s
Average jitter = 0.001552 s
Delay standard deviation = 0.000000 s
Bytes received = 24967500
Average bitrate = 399.490876 Kbit/s

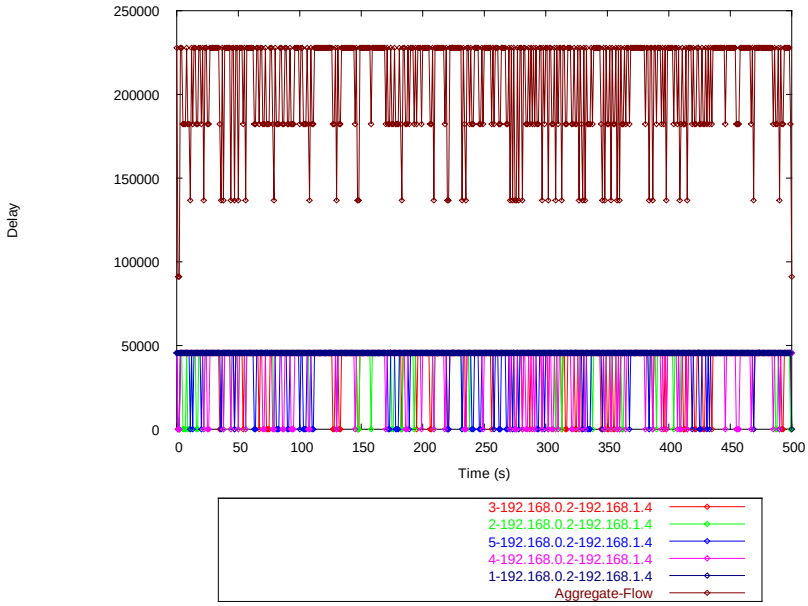
```
Average packet rate      =     99.872719 pkt/s
Packets dropped          =           65 (0.13 %)
-------------------------------------------------------------


************************  TOTAL RESULTS   ********************
_____________________________________________________________
Number of flows          =           5
Total time               =    500.052193 s
Total packets            =       2779635
Minimum delay            =  45568.542182 s
Maximum delay            =  45572.883623 s
Average delay            =  45568.556015 s
Average jitter           =      0.000315 s
Delay standard deviation =      0.016651 s
Bytes received           =    1717703145
Average bitrate          =  27480.381753 Kbit/s
Average packet rate      =   5558.689751 pkt/s
Packets dropped          =        18944 (0.68 %)
Error lines              =           0
-------------------------------------------------------------
bash-2.05b#
```

Gráfico bitrate x tempo



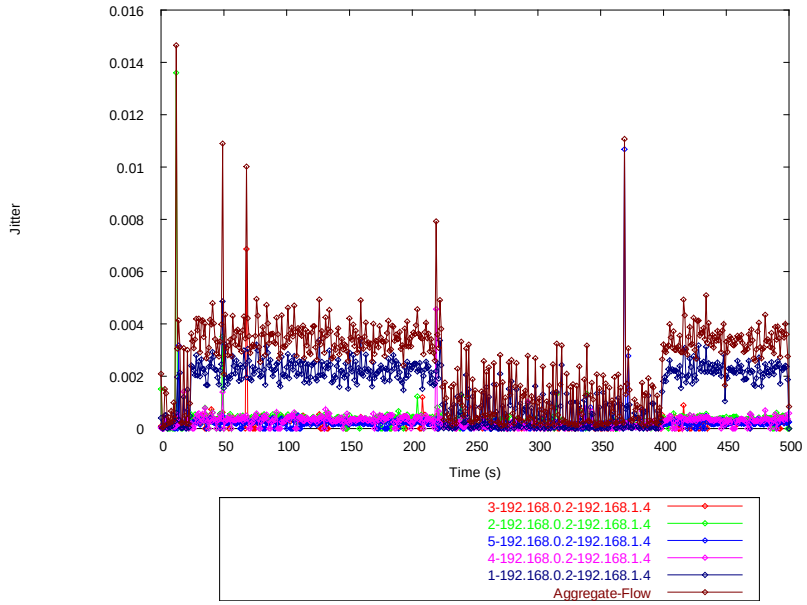
Estes valores de *bitrate* devem ser somados aos valores obtidos pelo fluxo gerado utilizando o Iperf para obter a utilização total da porta.

Gráfico delay x tempo



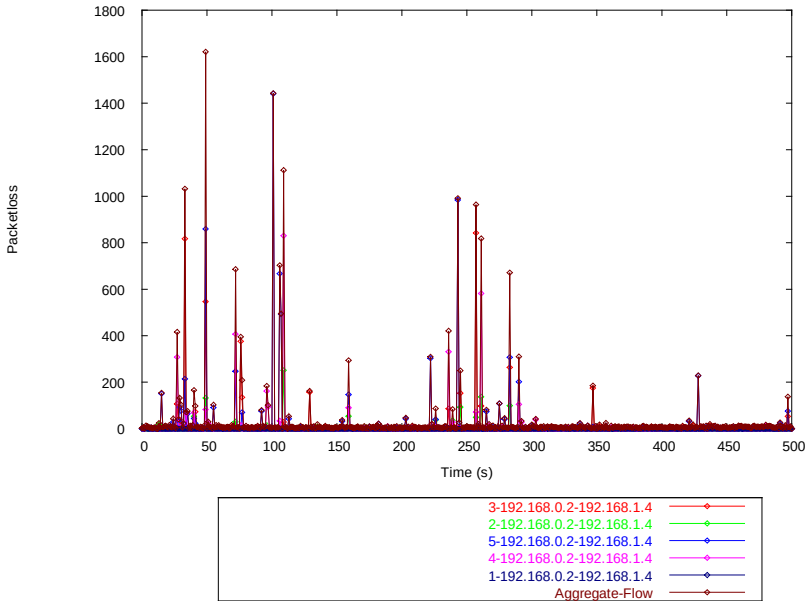
Todos os valores de retardo são semelhantes, indicando que não há priorização para o tráfego.

Gráfico jitter x tempo



O intervalo em que o *jitter* apresenta menores valores corresponde a um período de silêncio da ferramenta Iperf.

Gráfico packet loss x tempo



A perda de pacotes não parece ter sido influenciada pela execução concorrente do Iperf, nem pela sua interrupção.

7.5. Resultados do caso 2 – DES 6500

Neste segundo estudo foram realizados cerca de 30 experimentos de geração e medição de tráfego para permitir a realização dos testes. Estão descritos abaixo alguns destes experimentos.

1. Teste de Spanning Tree

Este teste verificou o funcionamento da facilidade de *spanning tree* e a sua reconfiguração durante uma falha. O *spanning tree* evita a formação de *loops* de camada 2 em uma rede ou VLAN desabilitando os caminhos redundantes. Foi testado o suporte ao protocolo 802.1d padronizado pelo IEEE (IEEE, 2004), habilitando-o e em seguida forçando a determinação de um novo camiho desligando o enlace ativo. Posteriormente este enlace foi reestabelecido.

Tráfego gerado

Foi gerado um fluxo TCP utilizando os parâmetros abaixo.

```
-a 10.90.90.2 -m rttm -rp 9506 -C 1000 -c 512 -t 24000
```

Características do fluxo:

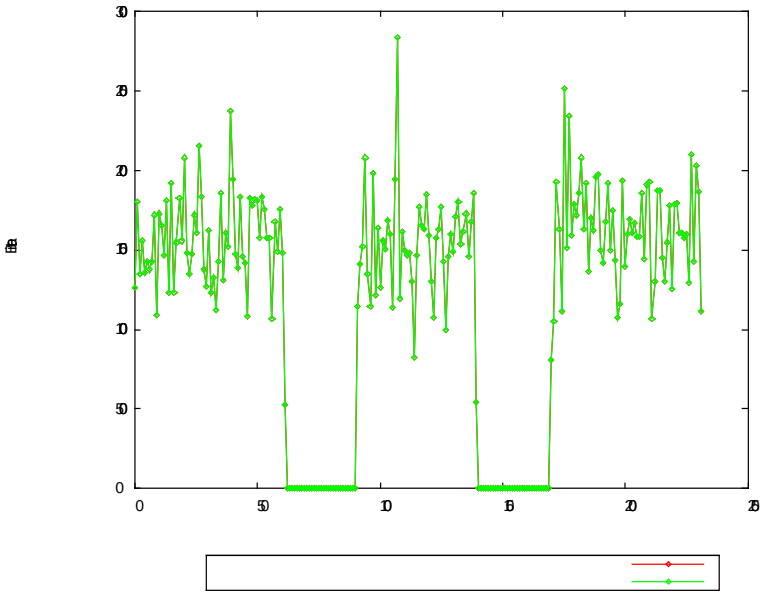
- porta remota: 9506
- intervalo entre pacotes: constante – 1000 pacotes por segundo
- *payload*: constante – 512 bytes
- protocolo: TCP
- duração: 24000 milissegundos

Tráfego recebido

```
[root@wefixd exp6500]# /usr/D-ITG-2.4/bin/ITGDec stpfalha+vlantaxaconstante19020
51050sender
------------------------------------------------------------
Flow number: 1
From 10.90.90.91:32769
To    10.90.90.92:9506
------------------------------------------------------------
Total time              =    240.200741 s
Total packets           =         47384
Minimum delay           =      0.002755 s
Maximum delay           =      1.612773 s
Average delay           =      0.719840 s
Average jitter          =      0.008659 s
```

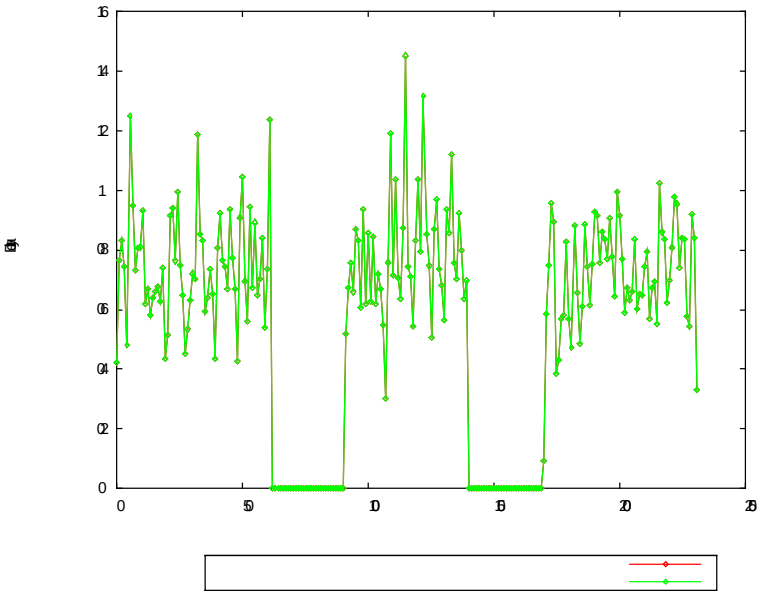
```
Delay standard deviation =      0.252307 s
Bytes received           =      48521216
Average bitrate          =   1616.022192 Kbit/s
Average packet rate      =    197.268334 pkt/s
Packets dropped          =       111084 (70.10 %)
-------------------------------------------------------------

_____________________________________________________________
**********************  TOTAL RESULTS   ********************
_____________________________________________________________
Number of flows          =            1
Total time               =    240.200741 s
Total packets            =        47384
Minimum delay            =     0.002755 s
Maximum delay            =     1.612773 s
Average delay            =     0.719840 s
Average jitter           =     0.008659 s
Delay standard deviation =      0.252307 s
Bytes received           =      48521216
Average bitrate          =   1616.022192 Kbit/s
Average packet rate      =    197.268334 pkt/s
Packets dropped          =       111084 (70.10 %)
Error lines              =            0
-------------------------------------------------------------
[root@wefixd exp6500]#
```

Gráfico bitrate x tempo (Kbps x s)



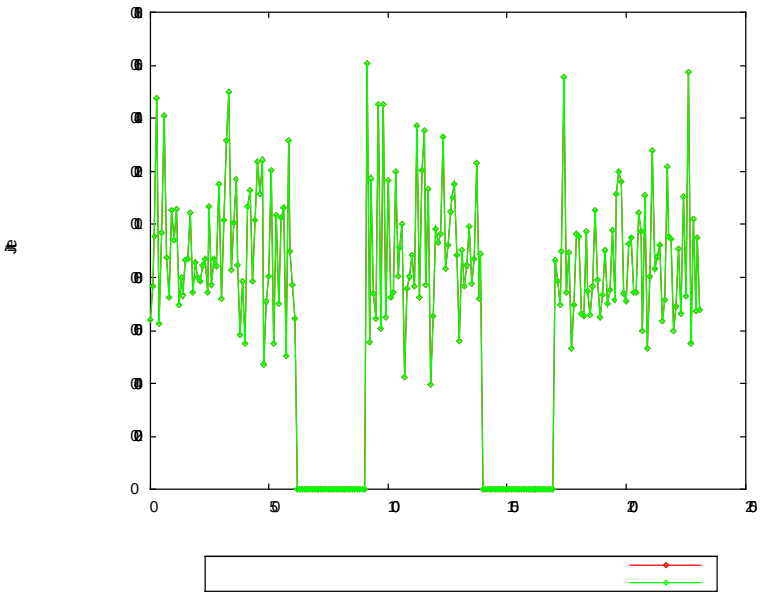
Os intervalos em que a taxa de transmissão cai a zero representam o tempo gasto pelo *switch* para encontrar um novo caminho após a queda do enlace ativo. A descoberta de um caminho e a desabilitação de anéis utilizando o protocolo 802.1d leva cerca de 3s.

Gráfico delay x tempo (s x s)



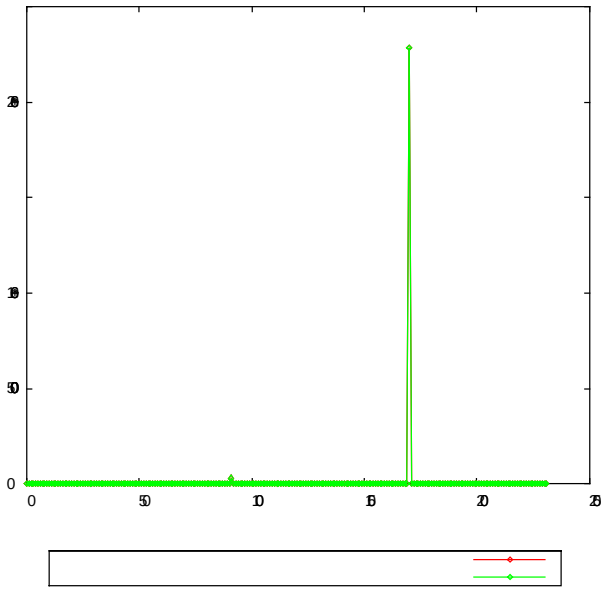
Durante o período em que o protocolo está buscando um novo caminho, o retardo cai a zero, segundo representação da ferramenta para situações em que não há o recebimento dos pacotes. Após este intervalo não há alterações significativas devidas à utilização do novo enlace.

Gráfico jitter x tempo (s x s)



O perfil do gráfico de *jitter* x tempo acompanha os demais, indicando zero quando não é possível o cálculo do valor.

Gráfico packet loss x tempo (pacotes/s x s)



Durante os dois intervalos de reconfiguração houve perda de pacotes, contabilizada no momento em que a conexão é restabelecida.

2. Teste de Vlan

Neste teste verificou-se a conectividade entre as portas pertencentes a uma mesma VLAN e o isolamento das demais portas do switch. Através da configuração de VLANs (*Virtual LANs*) é possível delimitar os domínios de *broadcast*, compartilhando recursos e evitando *broadcast storms*.

Tráfego gerado

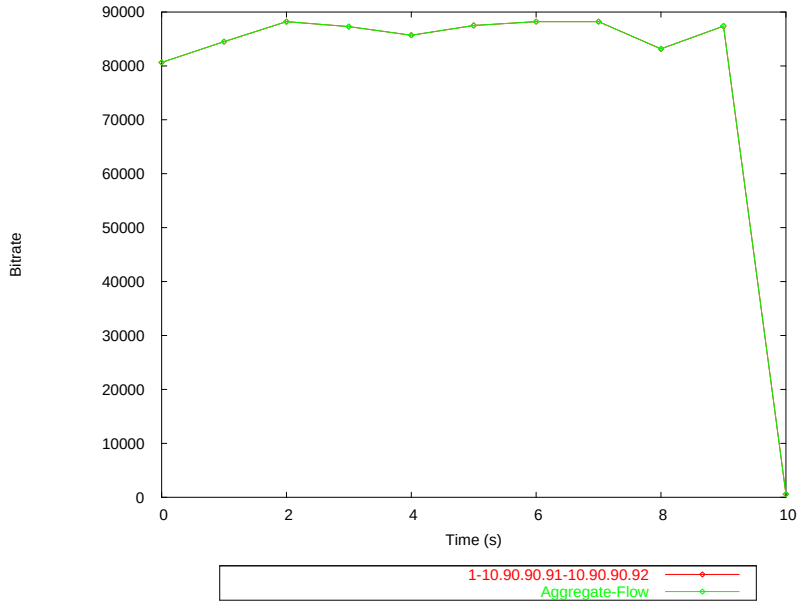
Para execução deste teste foi gerado um fluxo semelhante ao do experimento anterior para testar a conectividade entre duas portas de uma mesma VLAN. Um segundo fluxo entre portas pertencentes a diferentes VLANs não pode ser estabelecido, confirmando o isolamento entre VLANs.

Tráfego recebido

```
[root@wefixd exp6500]# /usr/D-ITG-2.4/bin/ITGDec taxa100000receiver
------------------------------------------------------------
Flow number: 1
From 10.90.90.91:32775
To    10.90.90.92:9506
------------------------------------------------------------
Total time              =     10.006533 s
Total packets           =        210302
Minimum delay           =      0.514071 s
Maximum delay           =      0.532540 s
Average delay           =      0.520186 s
Average jitter          =      0.000034 s
Delay standard deviation =      0.001441 s
Bytes received          =     107674624
Average bitrate         =  86083.460875 Kbit/s
Average packet rate     =  21016.469940 pkt/s
Packets dropped         =            0 (0.00 %)
------------------------------------------------------------

____________________________________________________________
**********  TOTAL RESULTS   **********
____________________________________________________________
Number of flows         =            1
Total time              =     10.006533 s
Total packets           =        210302
Minimum delay           =      0.514071 s
Maximum delay           =      0.532540 s
Average delay           =      0.520186 s
Average jitter          =      0.000034 s
Delay standard deviation =      0.001441 s
Bytes received          =     107674624
Average bitrate         =  86083.460875 Kbit/s
Average packet rate     =  21016.469940 pkt/s
```

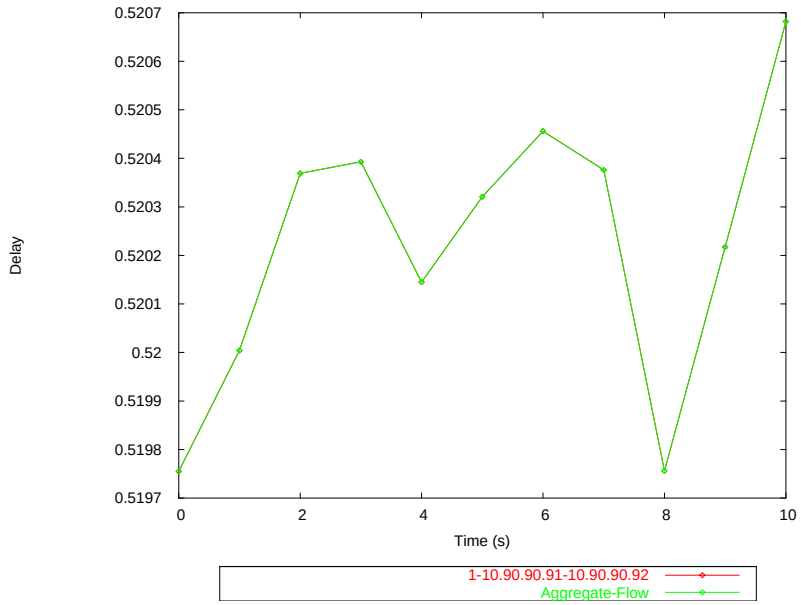
```
Packets dropped          =          0 (0.00 %)
Error lines              =          0
-------------------------------------------------------------
[root@wefixd exp6500]#
```

Gráfico bitrate x tempo (Kbps x s)



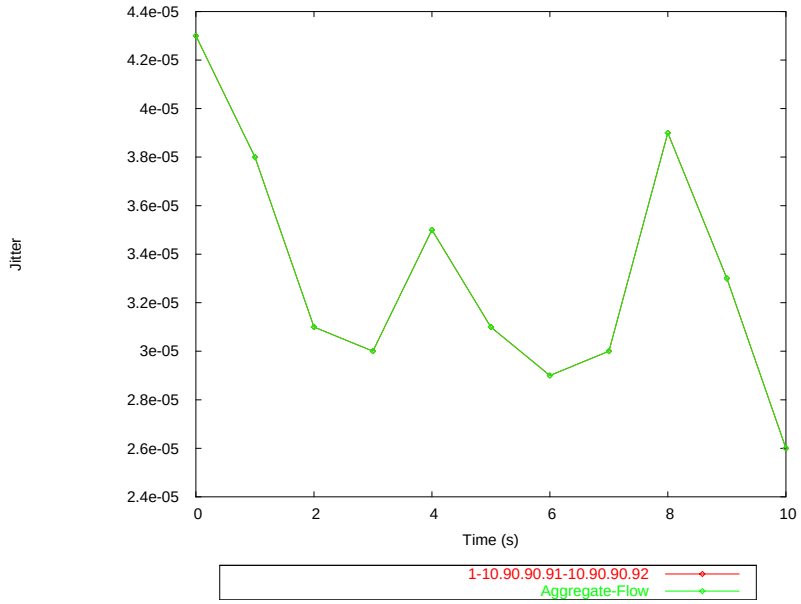
Neste gráfico podemos observar a existência de conectividade entre as portas da VLAN pela não existência de interrupções no fluxo de tráfego, porém com ligeiras alterações da taxa nos momentos de estabelecimento da VLAN.

Gráfico delay x tempo (s x s)



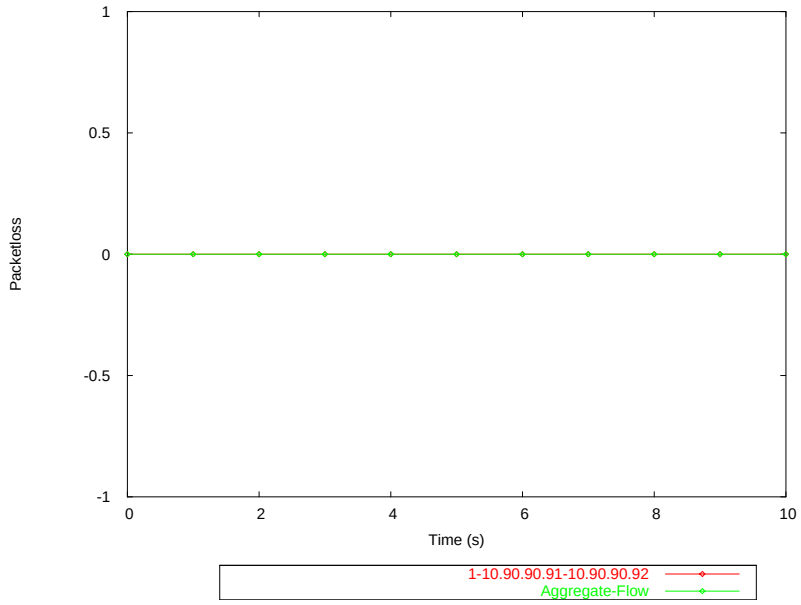
Este gráfico mostra uma pequena variação do retardo, acompanhando o gráfico anterior: nos momentos de queda da taxa também há uma ligeira queda no retardo.

Gráfico jitter x tempo (s x s)



De forma semelhante à medição do retardo o *jitter* não sofreu maiores influências devido ao estabelecimento da VLAN.

Gráfico packet loss x tempo (pacotes/s x s)



O gráfico acima mostra que não houve perda de pacotes durante o experimento.

3. Teste de ACL

Este teste verificou o funcionamento da ACL. Durante o experimento de geração de tráfego foram definidas regras hierárquicas que negaram o acesso ao fluxo e em seguida a regra mais restritiva foi excluída. O equipamento permite a configuração de apenas 8 perfis de tráfegos a serem avaliados, entretanto cada perfil pode conter diversas regras organizadas hierarquicamente, de forma a permitir ou negar o tráfego com uma granularidade mais fina. É preciso um bom planejamento destas regras para que seja possível utilizar esta facilidade corretamente.

Tráfego gerado

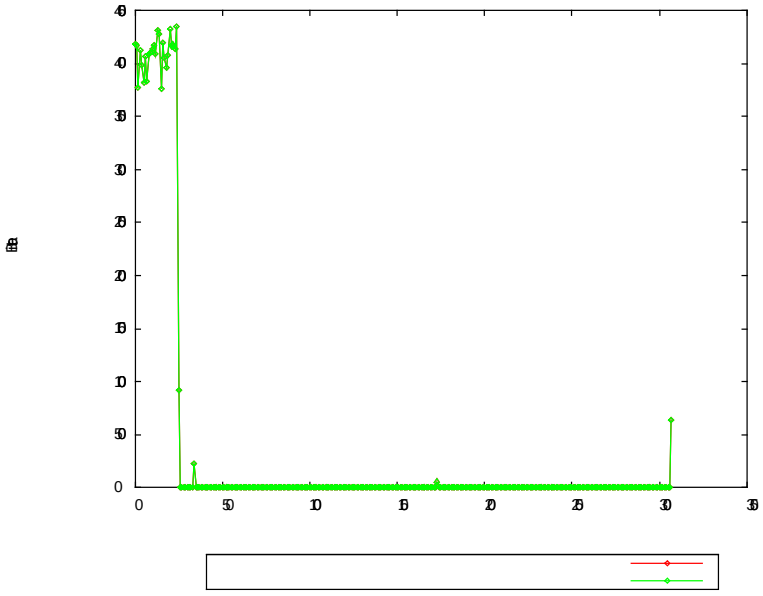
Foi gerado um fluxo com as mesmas características do experimento 1, diferindo pela duração e pela taxa máxima aumentadas.

Tráfego recebido

```
[root@wefixd exp6500]# /usr/D-ITG-2.4/bin/ITGDec payload1400receiver1943170205
------------------------------------------------------------
Flow number: 1
From 10.90.90.91:33879
To    10.90.90.92:9501
------------------------------------------------------------
Total time              =    307.642290 s
Total packets           =         9300
Minimum delay           =   3606.719928 s
Maximum delay           =   3889.236665 s
Average delay           =   3608.749649 s
Average jitter          =      0.034193 s
Delay standard deviation =     22.292478 s
Bytes received          =      13020000
Average bitrate         =    338.575038 Kbit/s
Average packet rate     =     30.229914 pkt/s
Packets dropped         =           91524 (98.63 %)
------------------------------------------------------------

_____________________________________________________________
**********  TOTAL RESULTS   ******************
_____________________________________________________________
Number of flows         =           1
Total time              =    307.642290 s
Total packets           =         9300
Minimum delay           =   3606.719928 s
Maximum delay           =   3889.236665 s
Average delay           =   3608.749649 s
Average jitter          =      0.034193 s
```

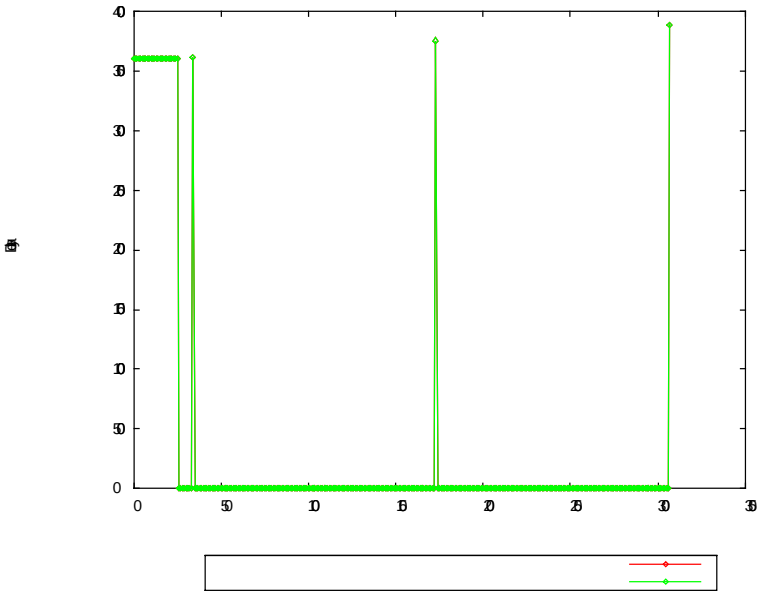
```
Delay standard deviation =     22.292478 s
Bytes received           =      13020000
Average bitrate          =    338.575038 Kbit/s
Average packet rate      =     30.229914 pkt/s
Packets dropped          =           91524 (98.63 %)
Error lines              =           0
-------------------------------------------------------
[root@wefixd exp6500]#
```

Gráfico bitrate x tempo (Kbps x s)



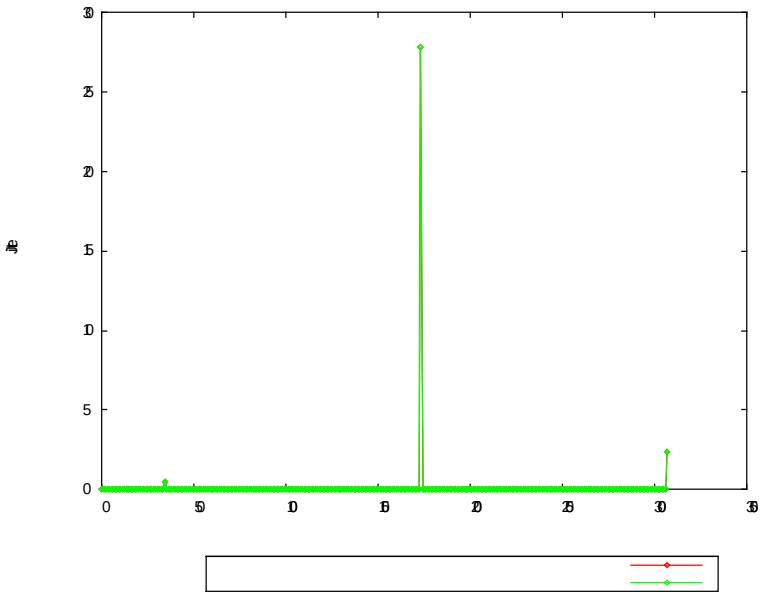
Neste gráfico podemos observar os períodos em que o fluxo foi rejeitado e o seu restabelecimento com a remoção da regra mais restritiva.

Gráfico delay x tempo (s x s)



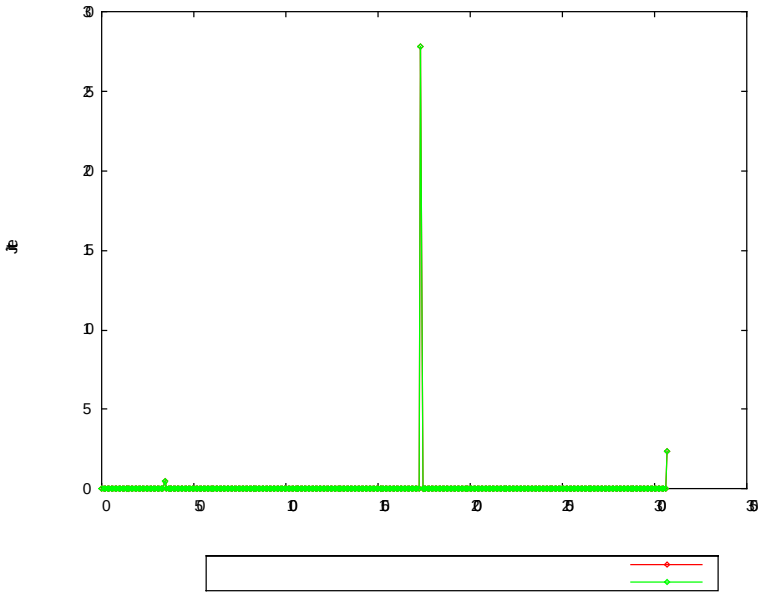
Conforme já relatado anteriormente, os intervalos de retardo zero indicam os períodos em que não houve recebimento de pacotes, informando os valores reais apenas quando existe o restabelecimento do fluxo.

Gráfico jitter x tempo (s x s)



Este gráfico assim como o anterior mostra valores zero para os intervalos em que não é possível a medição do *jitter*.

Gráfico packet loss x tempo (pacotes/s x s)



Durante os intervalos em que o fluxo é rejeitado observa-se uma grande perda de pacotes, que só pode ser contabilizada no restabelecimento da conexão.

4. Teste de VoIP

Este experimento foi realizado para testar o tratamento de tráfegos com o perfil de VoIP, uma das opções da ferramenta DITG. Foram utilizados diferentes algoritmos de compressão de voz em cada fluxo.

Tráfego gerado

Foram gerados cinco fluxos com perfil de VoIP através da utilização do script abaixo.

```
-a 10.90.90.92 -m rttm -rp 10003 VoIP -x G.711.1 -h RTP
-a 10.90.90.92 -m rttm -rp 10004 VoIP -x G.711.2 -h RTP
-a 10.90.90.92 -m rttm -rp 10005 VoIP -x G.723.1 -h RTP
-a 10.90.90.92 -m rttm -rp 10007 VoIP -x G.729.2 -h RTP
-a 10.90.90.92 -m rttm -rp 10008 VoIP -x G.729.3 -h RTP
```

Características do primeiro fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1003
- perfil do fluxo: simulação de VoIP
  - codificação da voz (-x): G.711.1
  - protocolo (-h): RTP – *Real Time Protocol*

Características do segundo fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1004
- perfil do fluxo: simulação de VoIP
  - codificação da voz (-x): G.711.2
  - protocolo (-h): RTP – *Real Time Protocol*

Características do terceiro fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1005
- perfil do fluxo: simulação de VoIP
  - codificação da voz (-x): G.723.1
  - protocolo (-h): RTP – *Real Time Protocol*

Características do quarto fluxo:

- medição (-m): bidirecional (rttm)

- porta remota (-rp): 1007
- perfil do fluxo: simulação de VoIP
  - codificação da voz (-x): G.729.2
  - protocolo (-h): RTP – *Real Time Protocol*

Características do quinto fluxo:

- medição (-m): bidirecional (rttm)
- porta remota (-rp): 1008
- perfil do fluxo: simulação de VoIP
  - codificação da voz (-x): G.729.3
  - protocolo (-h): RTP – *Real Time Protocol*

A seguir estão documentados os parâmetros específicos da codificação de voz de cada fluxo. O primeiro fluxo não foi estabelecido devido a erros no receptor.

bash-2.05b#:/usr/local/src/ITG/experimentos# ITGSend voipscript5fluxos -l voip5sender -x voip5receiver

Primeiro fluxo
Voice Codec: G.711
Framesize: 80.00
Samples: 1
Packets per sec.: 100
VAD: No

Segundo fluxo
Voice Codec: G.711
Framesize: 80.00
Samples: 2
Packets per sec.: 50
VAD: No

Terceiro fluxo
Voice Codec: G.723.1
Framesize: 30.00
Samples: 1
Packets per sec.: 26
VAD: No

Quarto fluxo
Voice Codec: G.729
Framesize: 10.00
Samples: 2
Packets per sec.: 50
VAD: No

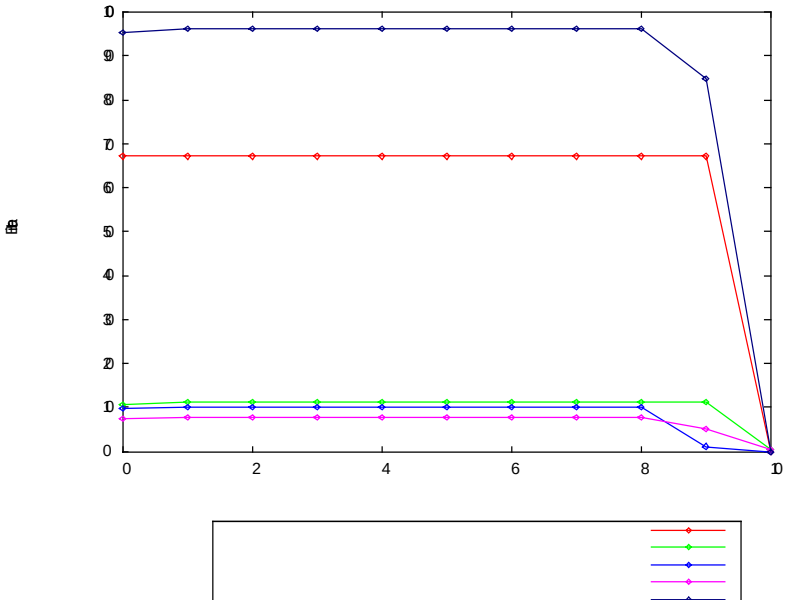
Quinto fluxo
Voice Codec: G.729
Framesize: 10.00
Samples: 3
Packets per sec.: 33
VAD: No

Tráfego recebido

```
[root@wefixd exp6500]# /usr/D-ITG-2.4/bin/ITGDec voip5receiver
------------------------------------------------------------
Flow number: 2
From 10.90.90.91:32770
To    10.90.90.92:10004
------------------------------------------------------------
Total time              =      9.981422 s
Total packets           =           500
Minimum delay           =      0.120823 s
Maximum delay           =      0.121010 s
Average delay           =      0.120898 s
Average jitter          =      0.000007 s
Delay standard deviation =      0.000042 s
Bytes received          =         84000
Average bitrate         =     67.325077 Kbit/s
Average packet rate     =     50.093063 pkt/s
Packets dropped         =            0 (0.00 %)
------------------------------------------------------------
------------------------------------------------------------
Flow number: 4
From 10.90.90.91:32772
To    10.90.90.92:10007
------------------------------------------------------------
Total time              =      9.979848 s
Total packets           =           500
Minimum delay           =      0.120798 s
Maximum delay           =      0.121144 s
Average delay           =      0.120870 s
Average jitter          =      0.000004 s
Delay standard deviation =      0.000044 s
Bytes received          =         14000
Average bitrate         =     11.222616 Kbit/s
Average packet rate     =     50.100963 pkt/s
Packets dropped         =            0 (0.00 %)
------------------------------------------------------------
------------------------------------------------------------
Flow number: 5
From 10.90.90.91:32773
To    10.90.90.92:10008
------------------------------------------------------------
Total time              =      9.069005 s
```

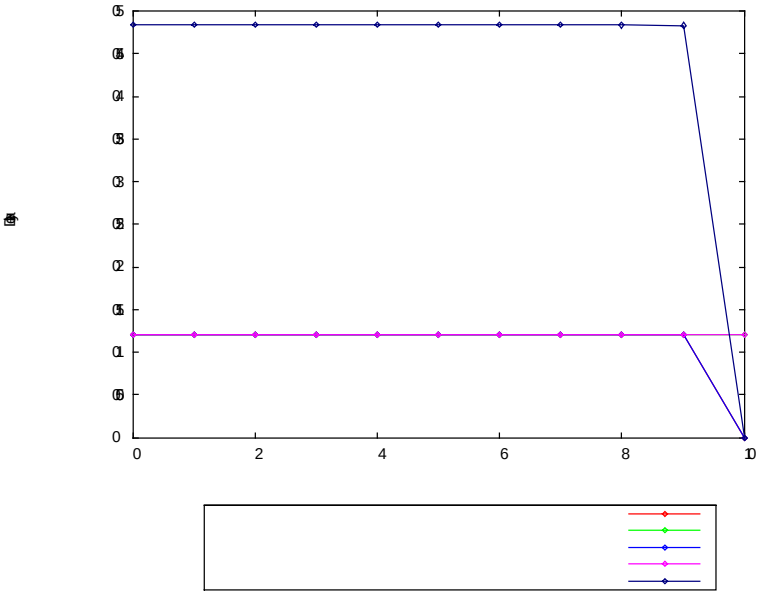
```
Total packets           =         300
Minimum delay           =     0.120811 s
Maximum delay           =     0.121073 s
Average delay           =     0.120892 s
Average jitter          =     0.000028 s
Delay standard deviation =     0.000042 s
Bytes received          =       11400
Average bitrate         =    10.056230 Kbit/s
Average packet rate     =    33.079704 pkt/s
Packets dropped         =           0 (0.00 %)
-------------------------------------------------------
-------------------------------------------------------
Flow number: 3
From 10.90.90.91:32771
To   10.90.90.92:10005
-------------------------------------------------------
Total time              =     9.579291 s
Total packets           =         250
Minimum delay           =     0.120804 s
Maximum delay           =     0.120992 s
Average delay           =     0.120888 s
Average jitter          =     0.000010 s
Delay standard deviation =     0.000042 s
Bytes received          =        9500
Average bitrate         =     7.933781 Kbit/s
Average packet rate     =    26.097965 pkt/s
Packets dropped         =           0 (0.00 %)
-------------------------------------------------------


************************  TOTAL RESULTS   ********************

Number of flows         =           4
Total time              =    10.022204 s
Total packets           =        1550
Minimum delay           =     0.120798 s
Maximum delay           =     0.121144 s
Average delay           =     0.120886 s
Average jitter          =     0.000011 s
Delay standard deviation =     0.000044 s
Bytes received          =      118900
Average bitrate         =    94.909263 Kbit/s
Average packet rate     =   154.656600 pkt/s
Packets dropped         =           0 (0.00 %)
Error lines             =           0
-------------------------------------------------------
[root@wefixd exp6500]#
```

Gráfico bitrate x tempo (Kbps x s)



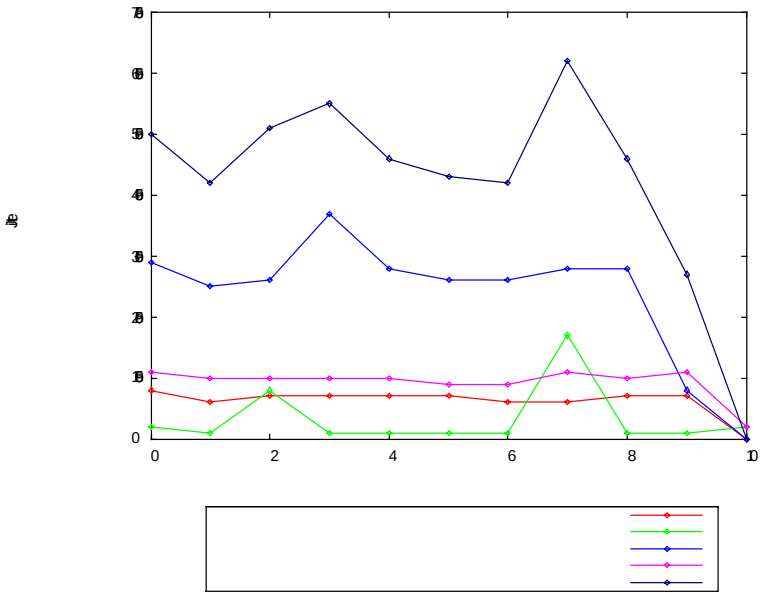
O fluxo nº 2, utilizando o algoritmo G.711, com duas amostras foi o que consumiu maior banda, cerca de 68Kbps. Os demais fluxos tiveram um desempenho semelhante, com o mínimo de 8Kbps.

Gráfico delay x tempo (s x s)



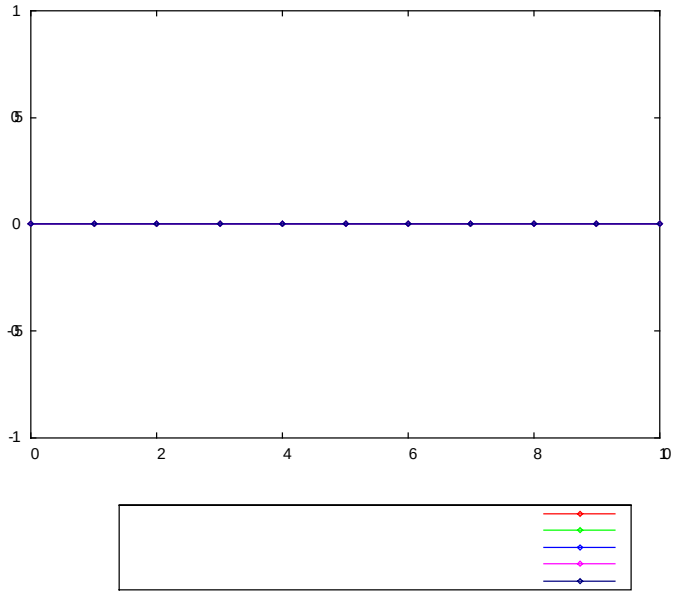
Todos os fluxos apresentam o mesmo retardo, dentro de valores aceitáveis para aplicações de voz.

Gráfico jitter x tempo (s x s)



O *jitter* apresenta valores baixos, adequados para aplicações de voz, variando conforme o algoritmo de compressão.

Gráfico packet loss x tempo (pacotes/s x s)



O gráfico acima mostra que não houve perda de pacotes durante o experimento.

7.6. Conclusão

7.6.1. Avaliação dos testes do caso 1 – DES 6300

Apesar do sucesso dos experimentos de geração e medição de tráfego, que é o objeto deste estudo, os testes do *switch* DES 6300 em processo de homologação pela UFF apresentaram resultados sofríveis. As interfaces de configuração, em especial a interface via linha de comando, não são intuitivas. Este fato, aliado à falta de uma documentação e de suporte técnico de qualidade, gerou dúvidas com freqüência entre a equipe encarregada dos testes, apesar desta ser formada por profissionais com boa experiência em equipamentos de rede.

Os equipamentos apresentaram problemas em ambos os protocolos de roteamento. As falhas não foram tratadas corretamente pelo protocolo RIP, havendo perda de pacotes durante o desligamento da conexão pela qual estavam sendo trafegados os pacotes de teste, mesmo havendo outras conexões disponíveis para a configuração de uma nova rota. No caso do OSPF foram detectados problemas ainda na configuração, não sendo esta intuitiva e nem mesmo amigável.

Assim não foi possível realizar todos os testes inicialmente previstos, que incluíam também testes de ACL, QoS e de desempenho, sendo este último composto por teste de saturação dos módulos e do *backplane*, capacidade agregada das interfaces – *forwarding* camada 3 e degradação de ACL e QoS com sobrecarga.

7.6.2. Avaliação dos testes do caso 2 – DES 6500

Este novo equipamento apresentou um funcionamento satisfatório, tendo sido sanados os problemas da versão anterior. Entretanto também possui limitações, em especial no tratamento de QoS, que é implementado através apenas da priorização dos pacotes provenientes de portas determinadas pela classe a que estão associadas. O *shapping* também não é feito de maneira direta. Para obter o condicionamento do tráfego deve ser utilizado o recurso de ACL, descartando os pacotes especificados. Assim não foram realizados testes de RSVP e de classificação e priorização de tráfego de camada 3, que utilizaria o recurso de geração de pacotes com marcação de DSCP da ferramenta DITG.

A facilidade de ACL existe e funciona corretamente, porém a sua configuração possui alguns problemas uma vez que é limitada a 8 perfis de tráfego, dentro dos quais são estabelecidas hierarquicamente as regras de filtragem.

Também não foram realizados os testes de desempenho em laboratório devido a limitações da ferramenta DITG, cuja taxa máxima é da ordem de 200Mbps, e dos equipamentos disponibilizados pela UFF para os testes, quantidade e tipo dos computadores (PCs), que impossibilitaram a saturação dos módulos e do *backplane*. Foram programados testes de desempenho utilizando o tráfego real da rede da UFF, que por este motivo fugiram ao escopo deste estudo de caso.

7.6.3. Comparação e avaliação das ferramentas

As duas ferramentas avaliadas, DITG e Iperf apresentaram desempenho satisfatório, atendendo às suas especificações e gerando tráfego de acordo com o previsto. Entretanto seria interessante aferir estas ferramentas e outras do mesmo tipo, de forma a corroborar esta percepção comprovando que o tráfego gerado está realmente dentro das especificações (tamanho e intervalo de pacotes e rajadas, distribuição, volume e etc.) e determinando o erro apresentado.

A ferramenta Iperf além de menos flexível do que a DITG na definição de perfis de tráfego, também possui algumas deficiências importantes:

- Armazenamento de dados: não é possível obter facilmente um *log* do experimento. Para isto é preciso usar recursos do sistema operacional, como, por exemplo, redirecionar a saída de dados da ferramenta para um arquivo específico em substituição à saída padrão (tela).
- Geração de gráficos: a geração de gráficos é feita através de um outro produto denominado Jperf. Este produto se encontra disponível no *site* do NLANR, entretanto apresentou erros de compilação, quando utilizada a versão que disponibiliza os arquivos fontes, e erros de execução, quando utilizada a versão pré-compilada. Por este motivo não foram apresentados gráficos dos experimentos envolvendo a ferramenta Iperf.

Uma facilidade que traria contribuições seria a possibilidade de receber em um cliente genérico o tráfego gerado, de forma que este pudesse ser utilizado como uma referência para os resultados das demais ferramentas. Este cliente poderia receber o tráfego gerado pelos servidores das outras ferramentas e apresentar resultados consolidados em um mesmo gráfico ou relatório, facilitando correlacioná-los. Tanto a DITG, como a Iperf só

permitem a utilização do seu cliente específico. Entretanto acredito que seria posssível desenvolver este cliente genérico para escutar as mesmas portas utilizadas pelas ferramentas, seja em paralelo ou simplesmente substituindo os clientes específicos de cada uma, sem a necessidade de alterar as ferramentas em si. É preciso investigar questões de compatibilidade, se houverem, especialmente no caso das medições bidirecionais. Como alternativa é possível a utilização de outro tipo de ferramenta para apenas fazer a leitura do tráfego da rede, como por exemplo o Ntop.

Ambas as ferramentas carecem de informações que descrevam em tempo real o andamento dos testes. Isto é especialmente sentido na ferramenta DITG, uma vez que não há esta opção nem para o cliente nem para o servidor. Já a ferramenta Iperf possui no servidor a opção de informar em intervalos definidos pelo usuário a quantidade de dados transmitidos e a que taxa. Esta opção auxilia o acompanhamento dos testes durante a sua execução.

A utilização das ferramentas apresentou vantagens já esperadas em relação aos utilitários *ping*, *traceroute* e *tcpdump* tradicionalmente empregados em testes deste tipo, devido às facilidades de geração de tráfego com características semelhantes ao real e de geração de gráficos e relatórios de texto acerca do experimento. Entretanto a falta de informação em tempo real, principalmente no cliente de ambas as ferramentas, e a familiaridade com os utilitários citados fizeram com que fossem utilizados em conjunto com as ferramentas de geração e medição de tráfego que estavam sendo avaliadas.

Assim foi possível comprovar que estas ferramentas são extremamente úteis, dentro de seus cenários de utilização, apresentando características que facilitaram a obtenção de informações importantes nos testes realizados, entretanto ainda precisam evoluir em alguns aspectos acrescentando funcionalidades e possibilitando uma maior integração com outros recursos. Entretanto estas são ferramentas que não se destinam à utilização em situações que necessitam de alta confiabilidade e desempenho, devido às suas limitações computacionais e à falta de uma entidade que faça a aferição de sua execução. Para estes casos é recomendável a utilização de ferramentas específicas implementadas em *hardware* dedicado.

Capítulo 8
Conclusão

Este trabalho abordou a geração e medição de tráfego como forma de assegurar, em conjunto com a engenharia de tráfego e os mecanismos de QoS, a qualidade de serviço em *backbones* IP, fazendo um levantamento das principais questões técnicas envolvidas. Foram estudadas questões de tecnologia de redes, seus modelos de OAM e de gerência. Também foram abordadas os principais métodos de medição e métricas utilizados para mensurar e avaliar a rede e o seu desempenho. Adicionalmente foi feita uma revisão dos modelos de qualidade de serviço e dos conceitos de engenharia de tráfego, correlacionando-os com a medição, entendida como essencial para a implantação e a operação de uma rede com garantias de qualidade de serviço.

Complementando este estudo teórico foi feito um levantamento das ferramentas desenvolvidas pela comunidade científica internacional, disponíveis publicamente. Estas ferramentas foram avaliadas e demonstraram ser de grande utilidade em diversos cenários de utilização. Entretanto, boa parte delas possui apenas as características básicas de geração e medição de tráfego TCP/IP, não apresentando facilidades como geração de perfis específicos de tráfego e a documentação dos testes em gráficos e relatórios. O levantamento e a avaliação das diversas ferramentas permitiu afirmar que não há uma ferramenta ideal, uma vez que cada uma pode ser a mais indicada para determinado tipo de medição e de ambiente.

Dentre as dezesseis ferramentas estudadas, foram selecionadas as ferramentas DITG e Iperf, formando um conjunto considerado adequado para a realização dos testes necessários ao estudo de caso apresentado no capítulo 7. A ferramenta DITG foi selecionada pela sua flexibilidade, capaz de gerar tráfego segundo diversos perfis. A ferramenta Iperf, por ser muito utilizada pela comunidade acadêmica para a medição ativa das principais métricas de desempenho e, portanto, bem aceita em termos de confiabilidade de resultados.

No capítulo 7 estão apresentados os testes de homologação realizados para avaliação de *switches* do fabricante Dlink para utilização na substituição dos equipamentos do núcleo da sua rede de comunicação de dados da UFF. Estes testes visam ratificar as informações prestadas pelo fabricante a respeito das características e funcionalidades dos *switches*, e verificar o seu desempenho em situações que simulam o ambiente de produção.

Foram testados dois modelos de *switches*: DES6300 e DES 6500, ambos *switches* Gigabit Ethetnet do tipo chassi, que suportam diversos módulos de interface possibilitando diferentes configurações. Os dois equipamentos diferem basicamente pela capacidade de encaminhamento e do *backplane*, quantidade máxima de módulos e pela interface de configuração.

O DES6300 teve um péssimo desempenho, apresentando falhas em vários dos testes executados. Este fato, aliado à falta de uma interface de configuração de fácil utilização, de documentação e de suporte técnico de qualidade, fez com que o equipamento fosse reprovado e substituído pelo modelo DES 6500. O DES6500 apresentou um funcionamento satisfatório, tendo sido sanados os problemas do modelo anterior. Entretanto também possui limitações, em especial no tratamento de QoS, que não implementa nehum dos modelos padronizados pelo IETF. Apesar disto este equipamento foi homologado e recomendado para a sua utilização no *backbone* da UFF. Pessoalmente não concordo com esta recomendação, pois penso que são muito grave as deficiências de documentação e de suporte técnico, principalmente em vista do fato de que a sua operação durante os testes não foi completamente isenta de falhas e do pequeno parque instalado deste equipamento. Entretanto é necessário considerar a relação custo/benefício do equipamento, uma vez que a UFF possui recursos limitados e não é uma prestadora de serviços de rede, podendo portanto prescindir de um equipamento *"carrier-class"*, ou seja, com 99,999% de disponibilidade e confiabilidade.

Durante os testes as ferramentas DITG e Iperf utilizadas para a geração e medição de tráfego demonstraram atender às suas especificações, gerando tráfego de acordo com o previsto (tamanho e intervalo de pacotes e rajadas, distribuição, volume e etc.). Entretanto foi detectada a necessidade de aferir estas ferramentas e outras do mesmo tipo, de forma a corroborar esta percepção. Também verificou-se que o desenvolvimento de algumas facilidades traria contribuições para a realização deste tipo de testes, como por exemplo:

- Recepção do tráfego gerado em um cliente genérico, que pudesse ser utilizado como uma referência para os resultados das ferramentas, consolidando as informações em um mesmo gráfico ou relatório.
- Informações que descrevam em tempo real o andamento dos testes, auxiliando o acompanhamento da sua execução.

Assim foi possível comprovar que estas ferramentas são extremamente úteis, dentro de seus cenários de utilização, apresentando características que facilitaram a obtenção de informações importantes nos testes realizados, entretanto ainda precisam evoluir em alguns aspectos acrescentando funcionalidades e possibilitando uma maior integração com outros recursos. Entretanto estas são ferramentas que não se destinam à utilização em situações que

necessitam de alta confiabilidade e desempenho, devido às suas limitações computacionais e à falta de uma entidade que faça a aferição de sua execução. Para estes eventos é recomendável a utilização de ferramentas específicas implementadas em *hardware* dedicado.

O caso particular das ferramentas de geração e medição de tráfego ilustra bem a evolução dos recursos de OAM da tecnologia IP, dispersa entre várias entidades e realizada por grupos de trabalhos separados. Estes recursos foram desenvolvidos ao sabor dos talentos individuais para atender às diferentes necessidades surgidas nas situações práticas, ou simplesmente inexistentes. Como resultado, apesar dos diversos centros de excelência existentes, as empresas e instituições encontram no seu dia-a-dia uma enorme carências de recursos para fornecer subsídio para a gerência e a operação das redes e *backbones* IP.

8.1. Trabalhos futuros

Este trabalho pretendeu estudar a medição e a engenharia de tráfego como forma para viabilizar a prestação de serviços de rede com qualidade garantida. Para isso devem ser utilizadas ferramentas de medição e geração de tráfego, que no caso da tecnologia IP foram e ainda estão desenvolvidas posteriormente ao protocolo em si e à sua larga utilização. Assim diversas questões ainda presisam ser desenvolvidas, revistas e/ou avaliadas.

Algumas sugestões para trabalhos futuros, continuando e aperfeiçoando o trabalho ora apresentado estão listadas abaixo:

- A realização de um trabalho semelhante a este voltado para redes MPLS, cuja utilização está crescendo cada vez mais a taxas que prometem ser este o caminho para o desenvolvimento das redes IP no futuro próximo.
- Novos testes práticos, envolvendo mais equipamentos em um laboratório específico de QoS para que seja possível fazer a aferição das ferramentas e o estudo mais aprofundado das técnicas da engenharia de tráfego.
- Implantação na rede operacional da UFF de ferramentas voltadas para a medição passiva e ativa dos seus parâmetros de qualidade. Devem ser selecionadas novas ferramentas, uma vez que outras circunstâncias e necessidades devem ser tratadas, em especial de forma a evitar o impacto na rede pelos pacotes de medição.
- Desenvolvimento de módulos adicionais para as ferramentas, complementado-as com as facilidades que foram identificadas neste trabalho como desejáveis e outras a serem definidas.

Capítulo 9

Bibliografia

- ***Bibliografia***

(ABE, 2004) http://www.abe.org

(ADAMS, 2000) Andrew K. ADAMS e Matthew MATHIS, “A System for Flexible Network Performance Measurement”, 2000

(ADAMSON, 1999) R. Brian Adamson; Multi Generator; http://computing.ee.ethz.ch/sepp/mgen-3.0-mo;1999

(ADVANCED, 2004) http://www.advanced.org/

(ALMES, 1999a) Request for Comments: 2679, G. Almes, S. Kalidindi e M. Zekauskas, “A One-way Delay Metric”, September 1999

(ALMES, 1999b) Request for Comments: 2680, G. Almes, S. Kalidindi e M. Zekauskas, “AOne-way Packet Loss Metric for IPPM”, September 1999

(ALMES, 1999c) Request for Comments: 2681, G. Almes, S. Kalidindi e M. Zekauskas, “A Round-trip Delay Metric for IPPM”, September 1999

(AMP, 2004) NLANR; AMP – Active Measurement Program; http://amp.nlanr.net/AMP/

(ANDERSON, 1996) Anderson, J., Lamy, P., Hué, L. e Le Beller, L. “Operations Standards for Global ATM - Networks: Network Element View”. IEEE Communications Magazine. December 1996.

(ASH, 2001) Internet Draft, Ash, J., “Traffic Engineering & QoS Methods for IP-, ATM-, & TDM- Based Multiservice Networks”, October,2001

(ASHWOOD, 2002) Internet Draft . Ashwood-Smith, P. "Generalized Multi-Protocol Label Switching - Signaling Functional Description " August 2002

(ATM, 1996) ATM Forum White Paper. ATM Service Categories: The Benefits to the User

(ATM, 2002) [ATMFa] ATM Forum White Paper: Unleash the Power: Building Multi-Service IP Networks With ATM Cores

(ATM, 2004) http://www.atmforum.org/standards/approved.html

(AVALLONE, 2004) [DIT04] Stefano Avallone, Donato Emma e Antonio Pescapè;DITG – Distributed Internet Traffic Generator; http://www.grid.unina.it/software/ITG/; 2004

(AWDUCHE, 2002) Request For Comments 3272 D. Awduche, A. Chiu, A. Elwalid, I. Widjaja e X. Xiao. “Overview and Principles of Internet Traffic Engineering” IETF 2002.

(BAKER, 1997a) Request For Commentes 2213 Baker, F., Krawczyk, J. e Sastry, A. “Integrated Services Management Information Base using SMIv2” IETF 1997.

(BAKER, 1997b) Request For Comments 2214 Baker, F., Krawczyk, J. e Sastry, A. “Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2” IETF 1997.

(BAKER, 2002) Request For Comments 3289, Baker, F., Chan, K. e Smith, A. “Management Information Base for the Differentiated Services Architecture”. IETF 2002.

(BERNET, 2002) Request For Comments 3290, Bernet, Y., Blake, S., Grossman, D. e Smith, A. “An Informal Management Model for DiffServ Routers. IETF 2002.

(BIANCHINI, 2002) Sheila Monteiro Bianchini, "Laboratório para Avaliação de Modelos com Suporte a QoS em Redes IP", 2002

(BIERMAN, 2002a) Request for Comments: 3287, A. Bierman, “Remote Monitoring MIB Extensions for Differentiated Services” , July 2002

(BIERMAN, 2002b) Request for Comments: 3434, A. Bierman e K. McCloghrie, “Remote Monitoring MIB Extensions for High Capacity Alarms”, December 2002

(BLACK, 1999) Black, U. ATM: Foundation for Broadband Networks, Ed. Prentice Hall, 1999

(BLAKE, 1998) Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. e Weiss, W. RFC 2475 An Architecture for Differentiated Service, IETF 1998.

(BOYD, 1989) Boyd R.T., Brodrick K.J., "Operational Support Systems for the future Local Network”, BT Technology Journal, April 1989

(BRADEN, 1994) Request For Comments 1633 Braden, R., Clark, D. e Shenker, S. “Integrated Services in the Internet Architecture: an Overview”. IETF 1994.

(BRADEN, 1997) Request For Comments: 2205, R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin “Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification” September 1997

(BROWNLEE, 1999) Request For Comments:2722, Brownlee, N., Mills, C. and G. Ruth, “Traffic Flow Measurement: Architecture”, October 1999.

(CAIDA, 2004) CAIDA – Cooperative Association for Internet Data Analysis; http://www.caida.org/; 2004

(CASE, 1990) Request For Comments: 1157, STD 15, Case, J., Fedor, M., Schoffstall, M. and Davin, J., “Simple Network Management Protocol”, May 1990.

(CASE, 1993) Request for Comments: 1441, J. Case, K. McCloghrie, M. Rose e S. Waldbusser, “Introduction to version 2 of the Internet-standard Network Management Framework”, April 1993

(CASE, 1996a) Request For Comments: 1901, Case, J., McCloghrie, K., Rose, M. and Waldbusser, S. , "Introduction to Community-based SNMPv2”, January 1996.

(CASE, 1996b) Request for Comments: 1902, J. Case, K. McCloghrie, M. Rose e S. Waldbusser, “Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)”, January 1996

(CASE, 1996c) Request for Comments: 1905 J. Case, K. McCloghrie, M. Rose e S. Waldbusser, “Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)”, January 1996

(CASE, 1996d) SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M. and S.Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)”, January 1996.

(CASE, 1996e) Request for Comments: 1908, J. Case, K. McCloghrie, M. Rose e S. Waldbusser, “Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework”, January 1996

(CASE, 1999) Request For Comments: 2572, Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)”, April 1999.

(CHOWN, 2002) [TFNGN] Tim Chown, Tiziana Ferrari, “Analysis of less-than-best-effort services” http://www.cnaf.infn.it/%7Eferrari/tfngn/lbe/

(CISCO, 2004) http://www.cisco.com/en/US/products/sw/netmgtsw/index.html

(COMMON, 2004) The Common Solutions Group - http://www.stonesoup.org/

(COTTRELL, 1999) Les Cottrell, Matt Zekauskas, Henk Uijterwaal e Tony McGregor, “Comparison of some Internet Active End-to-end Performance Measurement projects”, July 1999

(COTTRELL, 2001) Les Cottrell, “Passive vs. Active Monitoring”, Mach 2001

(COURTIAT, 2001) Courtiat, Jean-Pierre Qualidade de Serviço no Mundo IP, Minicurso SBRC 2001

(CSELÉNYI, 2001) Cselényi, I., Borg, N., Haraszti, P., Gharib, H. e Schmid, P. “Inter-Operator Interfaces for End-to-End IP QoS”. Tequila WS, Amsterdam, January 2001

(DARPA, 1981) Request For Comments 791.“Internet Protocol – Protocol Specification” DARPA Internet Program. September 1981.

(DARPA, 2004) http://www.darpa.mil/

(DEMICHELIS, 2002) Request for Comments: 3393, C. Demichelis e P. Chimento, “IP Packet Delay Variation Metric”, November,2002

(DENNY, 2003) Barbara Denny; Traffic Generator; http://www.postel.org/tg/tg.htm;2003

(DERI, 2004) Luca Deri; Ntop http://www.ntop.org/; 2004

(DMF, 2004) [DMF04] DMF – Distributed Monitoring Framework; http://dsd.lbl.gov/DMF/; 2004

(DOVROLIS, 2004a) Constantinos Dovrolis; Pathload; http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/pathload.html

(DOVROLIS, 2004b) Constantinos Dovrolis; Pathrate; http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/pathrate.html

(EDER, 2001) Request For Comments 3052 Eder, M. e Nag, S. “Service Management Architectures Issues and Review” IETF 2001.

(EDER, 2002) Request For Comments 3387 Eder, M. Chaskar, H. e Nag, S. “Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network”. IETF 2002.

(EMBRATEL, 2003) [EBT03] http://www.embratel.com.br/Embratel02/cda/portal/0,2997,MG_P_1912,00.html

(EMBRATEL, 2004) [EBT04] http://sla11.rjo.embratel.net.br/cgi-bin/Natl_report_por_mes.pl

(ENABLE, 2000) [ENB00] The Enable Project; http://www-didc.lbl.gov/Enable/

(ESNET, 2004) [ESN04] Energy Sciences Network http://www.es.net/

(FARKOUH, 1993) Farkouh, S. “Managing ATM-based Broadband Networks”. IEEE Communications Magazine.May 1993.

(FAUCHEUR, 2002) Request For Comments 3270. Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P. e Heinanen, J. “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services” IETF 2002.

(FEHER, 1999)] Feher, G., et al., “Boomerang – A Simple Protocol for Resource Reservation in IP Networks”, IEEE Workshop on QoS Support for Real-Time Internet Applications, Vancouver, Canada, June 1999.

(FELDMANN, 2000a) A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, e F. True. “Deriving Traffic Demands for Operational IP Networks: Methodology and Experience”. Proc. ACM SIGCOMM 2000, Estocolmo,Suécia.

(FELDMANN, 2000b) A. Feldmann, A. Greenberg, C. Lund, N. Reingold e J. Rexford. “NetScope: Traffic Engineering for IP Networks”. IEEE Network, March/April 2000.

(FLOYD, 1993) Floyd, S. and Jacobson, V., “Random Early Detection gateways for Congestion Avoidance”, IEEE/ACM Translation on Networking, V.1 N.4, August 1993.

(FLOYD, 1999) Floyd, S. and Ramakrishnan, K. “A Proposal to Add Explicit Congestion Notification (ECN) to IP”, Internet Engineering Task Force, Request for Comments 2481, January 1999.

(FLOYD, 2002) http://www.icir.org/floyd/ccmeasure.html Measurement Studies of End-to-End Congestion Control in the Internet maio/2002

(GILLESPIE, 1997) Gillespie, A. “Broadband Management after Permanent Connections”. IEEE Communications Magazine. October 1997.

(GIORGI, 1996) Ulisses Ponticelli Giorgi, “Tutorial RMON v.2”, Dezembro de 1996

(GRAPE, 2004) GRAPE - GRAvity PipE
http://support.uits.iu.edu/scripts/ose.cgi?anaf.ose.help&osecat=data

(GREENBERG, 2003) Albert Greenberg 2003
http://www.research.att.com/projects/NetworkMeasurementTools/

(HANCOCK, 2003) Robert Hancock, Roke Manor Research e John Loughney. Quality of Service at the Internet Engineering Task Force. Workshop on End-to-End Quality of Service. What is it? How do we get it?

(HARRINGTON, 1999)] Request For Comments: 2571, Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks”, April 1999.

(HARRINGTON, 2002) Request For Comments 3411 Harrington, D., Presuhn, R. e Wijnen, B. “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks” IETF 2002.

(HENP, 2004) Office of High Energy and Nuclear Physics http://er.doe.gov/henp/index.htm

(HPC, 2003) [HPC03] HPC – *High Performance Computing;*
http://www.cise.nsf.gov/funding/pgm_display.cfm?pub_id=5879&div=sci

(HPOV, 2004) HP OpenView; http://www.managementsoftware.hp.com/index.html; 2004

(HURLEY, 1999)] Hurley, P., Le Boudec, J. Y. e Thiran, P. “*The Asymmetric Best-Effort Service***”** Proceedings of IEEE Globecom 1999

(HURLEY, 2000) Internet Draft, Hurley, P., Iannaccone, G., Kara, M., Le Boudec, J. Y., Thiran, P. e Diot, C. “The ABE Service”, Novembro 2000

(HUSTON, 2000) Huston, G., “Next Steps for the IP QoS Architecture”, Internet Engineering Task Force, Request for Comments 2990, November 2000.

(IBM, 2004) http://www.ibm.com/br/products/software/tivoli/

(IEEE, 2003) Istitute of Electrical and Eletronics Engineers; http://www.ieee.org.br/

(IEEE, 2004) Jeffree, Tony A. “IEEE Std 802.1D-2004, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges” Jun 09, 2004

(IERS, 2004)] IEEE Reliability Society - Reliability Engineering http://www.ieee.org/portal/site/relsoc/menuitem.e3d19081e6eb2578fb2275875bac26c8/index.jsp?&pName=relsoc_level1&path=relsoc/Reliability_Engineering&file=index.xml&xsl=generic.xsl
(IETF, 2004) http://www.ietf.org

(INTERNET2, 2004) http://abilene.internet2.edu/

(IPPM, 2004) http://www.ietf.org/html.charters/ippm-charter.html

(IQOM, 2003)] http://www.nuperc.unifacs.br/gtqos/IQoM.html

(IQOM, 2004) http://www.iqom.ufsc/

(ISO, 1987) ISO 8824 “Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)”, December 1987.

(ISO, 1990) ISO 9595. "Information Processing Systems - Open Systems Interconnection - Common Management Information Service Definition” 1990

(ISO, 1991) ISO 9596. "Information Processing Systems - Open Systems Interconnection - Common Management Information Service Definition” 1991

(ISO, 1993) ISO DIS 10165-1. "Information Processing Systems - Open Systems Interconnection - Structure of Management Information - Part 1: Management Information Model”, 1993

(ITTC, 2004) http://www.ittc.ku.edu/index.phtml

(ITUT, 1976) ITUT. Recommendation X.25.“Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit”. October 1976

(ITUT, 1988) ITUT. Recommendation G.702. “Digital hierarchy bit rates” November 1988

(ITUT, 1991) ITUT. Recommendation G.707. “Network node interface for the synchronous digital hierarchy (SDH)” April 1991

(ITUT, 1992) ITU-T. Recommendation M.3010 “Principles for a Telecommunications Management Network” February 1992

(ITUT, 1993a) ITU-T. Recommendation I.350 “General aspects of quality of service and network performance in digital networks, including ISDNs” March 1993

(ITUT, 1993b) ITUT. Recommendation I.120.“Integrated services digital networks (ISDNs)”. March 1993

(ITUT, 1994) Recommendation E.800 “Terms and definitions related to quality of service and network performance including dependability” Agosto1994

(ITUT, 1996a) ITU-T. Recommendation I.356 “B-ISDN ATM Layer Cell Transfer Performance” November 1996

(ITUT, 1996b) ITU-T. Recommendation M.3010 “Principles for a Telecommunications Management Network” February 1996

(ITUT, 1998a) ITUT. Recommendation G.692. “Optical interfaces for multichannel systems with optical amplifiers” October 1998

(ITUT, 1998b) ITU-T. Recommendation M.3010 “Principles for a Telecommunications Management Network” February 1998

(ITUT, 2001) ITU-T Recommendation G.1000 “Communications quality of service: A framework and definitions” Novembro 2001.

(ITUT, 2002a) ITU-T. Recommendation Y.1540 “Internet protocol data communication service - IP packet transfer and availability performance parameters” December 2002

(ITUT, 2002b) Recommendation Y.1710 “Requirements for OAM functionality for MPLS networks” November 2002

(ITUT, 2002c) ITUT. Recommendation G.694.2. “Spectral grids for WDM applications: CWDM frequency grid” July 2002

(ITUT, 2002d) ITUT. Recommendation G.694.1. “Spectral grids for WDM applications: DWDM frequency grid” July 2002

(ITUT, 2004a) http://www.itu.int/ITU-T/

(ITUT, 2004b) ITU-T. Recommendation Y.1711 “Operation & Maintenance mechanism for MPLS networks” February 2004

(JACOBSON, 1989) V. Jacobson, traceroute, ftp://ftp.ee.lbl.gov/traceroute.tar.Z, 1989.

(JACOBSON, 1997) Van Jacobson, abstract for April 97 MSRI talk

(JACOBSON, 1997b) Van Jacobson; Pathchar; http://www.caida.org/tools/utilities/others/pathchar/; 1997

(JAMIN, 1996) Jamin, S., Danzig, P., Shenker, S.e Zhang L., “A Measurement-based Admission Control Algorithm for Integrated Services Packet Networks (Extended Version)”, ACM/IEEE Transactions on Networking, 1996.

(JONES, 2003) Rick Jones; Netperf; http://www.netperf.org/netperf/NetperfPage.html

(JONKMAN, 1997) Roel Jonkman; NetSpec; http://www.ittc.ku.edu/netspec/

(KALINDINDI, 1999) S. Kalindindi, M. Zekauskas, “Surveyor: An Infrastructure for Internet Performance Measurements”, June 1999

(KANSAS, 2004) http://www.ku.edu/

(LAI, 2003a) Internet Draft, W. Lai, R. Tibbs e S. Van den Berghe, “A Framework for Internet Traffic Engineering Measurement”, Febuary 2003

(LAI, 2003b) Internet Draft, W. Lai, R. Tibbs e S. Van den Berghe, “Requirements for Internet Traffic Engineering Measurement”, July 2003
(LAI,K., 2002) Kevin Lai; Nettimer; http://mosquitonet.stanford.edu/~laik/projects/nettimer/

(LAINE, 2002) Juha Laine , Sampo Saaristo e Rui Prior , RUDE & CRUDE; http://rude.sourceforge.net/

(LBNL, 2004) Lawrence Berkeley National Laboratory; http://www.lbl.gov

(LESSA, 1999) Demian Lessa, “O Protocolo de Gerenciamento RMON”, NewsGeneration – RNP – Rede Nacional de Ensino e Pesquisa, volume 3, número 1, Janeiro de 1999

(LIAKOPOULOS, 2003) Liakopoulos, A., Maglaris, B., Bouras, C. e Sevasti, A. “Providing and Verifying Advanced IP Services in Hierarchical DiffServ Networks – The case of GEANT” , January 2003.

(MAH, 2001) Bruce A. Mah; Pchar; http://www.employees.org/~bmah/Software/pchar/

(MAHDAVI, 1998) Request for Comments: 2330, J. Mahdavi, V. Paxson, G. Almes e M. Mathis. “Framework for IP Performance Metrics”, May 1998

(MAHDAVI, 1999) Request for Comments: 2678, J. Mahdavi e V. Paxson, “IPPM Metrics for Measuring Connectivity”, September 1999

(MATHIS, 1996) M. Mathis and J. Mahdavi, "Diagnosing Internet Congestion with a Transport Layer Performance Tool," *Proc. INET '96*, Montreal, June 1996.

(MATSUSHITA, 1991) Masahiko Matsushita. "Telecommunication Management Network", NTT Review, July 1991

(MCCLOGHRIE, 1990) Request for Comments: 1155, McCloghrie, K. “ Structure and Identification of Management Information for TCP/IP-based Internets”, May 1990

(MCCLOGHRIE, 1991) Request for Comments: 1213, K. McCloghrie e M. Rose, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II” March 1991

(MCCLOGHRIE, 1999) Request For Comments: 2578, STD 58 McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)”, April 1999.

(MCI, 2004) http://global.mci.com/about/network/latency/

(MILHAM, 1989) Milham D.J., Willetts K.J., "BT's Communications Management Architecture”, in: Proceedings of the IFIP TC6/WG 6.6 Symposium on Integrated Network Management, page 109-116, 1989

(MOAT, 2004) MOAT – Measurement and Operations Analysis Team; http://moat.nlanr.net; 2004

(MOREIRA, 2004) Moreira, J. “Redes Locais e TCP/IP” NCE/UFRJ. 2004

(MORTIER, 2002) Mortier, R. “Internet traf_c engineering” Uiversity of Cambridge. Computer Laboratory. 2002

(MTRACE, 2004) http://hegel.ittc.ukans.edu/topics/linux/man-pages/man8/mtrace.8.html

(NAI, 1998) MOAT/NAI – Network Analysis Infrastructure; http://moat.nlanr.net/NAI/; 1998

(NETPREDICT, 2004) http://www.netpredict.com/solutions/usecases/BDP-and-Chatter.htm

(NETRAMET, 2002) NeTraMet – Network Traffic Flow Measurement Tool; http://www.caida.org/tools/measurement/netramet/

(NGUYEN, 2000) Nguyen, L. e Fandel, B. “ATM End-to-End QoS Testing Using DominoATM and TPI-750”, May 2000

(NLANR, 2004) NLANR – National Laboratory for Applied Network Research; http://www.nlanr.net/

(NRL, 2004) Navy Research Laboratory http://www.nrl.navy.mil/

(NS2, 2004) www.isi.edu/nsnam/ns/

(NSF, 2004) NSF – *National Science Foundation;* http://www.nsf.gov/

(NTP, 2004) Network Time Protocol project; http://www.ntp.org; 2004

(OBSERVATORY, 2004) The Abilene Observatory; http://abilene.internet2.edu/observatory/; 2004

(OETIKER, 2004) Tobias Oetiker e Dave Rand, “*Multi Router Traffic Grapher*” http://people.ee.ethz.ch/~oetiker/webtools/mrtg/, 2004

(OLIVEIRA, 1998) Oliveira, Antonio Mauro Introdução ao Gerenciamento de Redes ATM, Minicurso SBRC 1998

(OPS, 2004) http://www.ops.ietf.org/

(ORAM, 2002) Oram A. e Grojsgold A. *“Um jeito amigável de obter qualidade de serviço na rede?”*, Dezembro 2002.

(PAXSON, 1996) V. Paxson, "End-to-End Routing Behavior in the Internet," Proc. SIGCOMM '96, Stanford, Aug. 1996

(PAXSON, 1997) V. Paxson, "Measurement and Analysis of End-to-End Internet Dynamics," Ph.D. Thesis, University of California, Berkeley, UCB-CSD-97-945, 1997.

(PAXSON, 1998) V . Paxson, J. Mahdavi, A. Adams, and M. Mathis, "An Architecture for Large-Scale Internet Measurement," IEEE Communications, Vol. 36, No. 8, Aug. 1998

(PINGER, 2002) SLAC – Stanford Linear Accelerator Center; The PingER Project; http://www-iepm.slac.stanford.edu/pinger/

(PMA, 2004) The Passive Measurement and Analysis Project; http://pma.nlanr.net/; 2004

(POSTEL CENTER, 2004) Postel Center – USC University of Southern Califórnia; http://www.postel.org/; 2004

(POSTEL, 1981a) Request for Comments: 792, J. Postel, “Internet Control Message Protocol”, September 1981

(POSTEL, 1981b) Request For Comments: 793, J. Postel, “Transmission Control Protocol”,September 1981

(POSTEL, 1981c) Request for Comments: 959, J. Postel e , J.K. Reynolds, “File Transfer Protocol”, October 1981

(QAME, 2004) https://noc.metropoa.tche.br/qame/

(QBSS, 2004) QBone Scavenger Service; http://qbone.internet2.edu/qbss/; 2004

(RELIABILITY, 2003) Reliability Center, Inc http://www.reliability.com/glossary.htm .

(RIPE, 2004) Réseaux IP Européens; http://www.ripe.net/; 2004

(RNP2, 2004) Rede Nacional de Ensino e Pesquisa – rede RNP2; http://www.rnp.br/rnp2/; 2004

(ROMASCANU, 2001) Request for Comments: 3144, D. Romascanu, “Remote Monitoring MIB Extensions for Interface Parameters Monitoring”, August 2001

(ROSE, 1991) Request For Comments: 1215, Rose, M., "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991.

(ROSEN, 2001) Request For Comments: 3031. E. Rosen, A. Viswanathan, and R. Callon. “Multiprotocol Label Switching Architecture”, January 2001.

(SAMIDI, 2002) Michael Samidi; Netprobe http://www.cs.ucr.edu/%7Emsamidi/projects.htm; 2002

(SANDILANDS, 2001) Robert Sandilands Network Traffic Generator; http://sourceforge.net/projects/traffic; 2001

(SHALUNOV, 2001) Internet2 Technical Report, Proposed Service Definition, S. Shalunov e B. Teitelbaum, “QBone Scavenger Service (QBSS) Definition Internet2 Technical Report, Proposed Service Definition”, March,2001
(SHALUNOV, 2004) http://www.internet2.edu/~shalunov/ippm/draft-ietf-ippm-owdp-08.txt; 2004

(SIDDIQUI, 2005) Internet Draft, Anwar Siddiqui, Dan Romascanu e Eugene Golovinsky, “Real-time Application Quality of Service Monitoring (RAQMON) MIB, March,2005

(SKITTER, 2004) Skitter

http://www.caida.org/analysis/topology/as_core_network/AS_Network.xml

(SLAC, 2004) Stanford Linear Accelerator Center; http://www.slac.stanford.edu/; 2004

(SRI, 2004) SRI International; http://www.sri.com/; 2004

(STALLINGS, 1996) William Stallings. SNMP, SNMPv2 and RMON: Practical Network Management. Addison Wesley, 2a. edição, 1996.

(SURVEYOR, 2004) Surveyor Project;, http://www.advanced.org/surveyor/; 1999

(TANENBAUM, 1996) Andrew S.Tanenbaum. Computer Networks. Prentice-Hall, 3a. edição, 1996

(TEITELBAUM, 2001a) Teitelbaum B. "Future Priorities for Internet2 QoS", October , 2001

(TEITELBAUM, 2001b) Teitelbaum B, Shalunov S. "Why Premium IP has not deployed (and probably never will)", Internet2 Qos Working Group Informational Document, May 2002.

(TEIXEIRA, 1999) Teixeira , S., Moraes, L.e Teixeira, J. "Uma Proposta para Gerenciamento de Conexões em Redes ATM". 1999

(TEKELEC, 1997) TEKELEC Publication 908-0119-01 Rev. C 0497-5000. "ATM Pocket Guide". 1997

(TELEFÓNICA, 2004) http://www.telefonica.com.br/empresas

(TELESCOPE, 2004) http://www.caida.org/analysis/security/telescope/

(TEQUILA, 2002) TEQUILA – Traffic Engineering for Quality of Service in the Internet, at Large Scale; http://www.ist-tequila.org/; 2002

(TEWG, 2004) http://www.ietf.org/html.charters/tewg-charter.html

(TIRUMALA, 2004)] Ajay Tirumala, Feng Qin, Jon Dugan, Jim Ferguson e Kevin Gibbs; Iperf; http://dast.nlanr.net/Projects/Iperf; 2004

(UCSD, 2004) [UNO04] UCSD – University of California, San Diego, Network Operations http://www-no.ucsd.edu/
(VBNS, 2004) Very High Performance Backbone Network Service; http://www.vbns.net/

(VINTON, 1991) Request for Comments: 1262, Vinton G. Cerf, "Guidelines for Internet Measurement Activities", October 1991

(WALDBUSSER, 1995) Request for Comments: 1757, S. Waldbusser. "Remote Network Monitoring Management Information Base", February 1995

(WALDBUSSER, 1997) Request for Comments: 2021, S. Waldbusser, "Remote Network Monitoring Management Information Base Version 2 using SMIv2", January 1997

(WALDBUSSER, 2000) Request for Comments: 2819, S. Waldbusser, “Remote Network Monitoring Management Information Base”, May 2000

(WALDBUSSER, 2002) Request for Comments: 3273, S. Waldbusser, “Remote Network Monitoring Management Information Base for High Capacity Networks”, July 2002

(WALDBUSSER, 2003) Request for Comments: 3577, S. Waldbusser, R. Cole, C. Kalbfleisch e D. Romascanu, “Introduction to the Remote Monitoring (RMON) Family of MIB Modules”, August 2003

(WALDBUSSER, 2004) Request for Comments: 3729, S. Waldbusser, “Application Performance Measurement MIB”, March 2004

(WATERMAN, 1999) Request for Comments: 2613, R. Waterman, B. Lahaye, D. Romascanu e D. Romascanu, “Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0”, June 1999

(XIAO, 1998) Xiao, X. QoS Routing in the Internet. Presentation to Ascend Communications, now Lucent Technologies 1998.

(XIAO, 1999a) Xiao, X. e Ni, L. Internet QoS: a Big Picture. IEEE Network Magazine, March 1999.

(XIAO, 1999b) Xiao, X Router Architeture, QoS and Trafic Engineering. Presentation to Tyco Submarine Systems 1999.

(XIWT, 2003) [XIWT03] XIWT – Cross Industry Working Team; http://www.xiwt.org/

(ZANDER, 2002) Sebastian Zander; UDPGen - UDP kernel traffic generator; http://www.fokus.fraunhofer.de/research/cc/berlios/employees/sebastian.zander/private/udpgen/; 2002