Daniel Bitencourt Cadorin

Ferramenta para monitoramento de Redes IP com Serviços Diferenciados utilizando SNMP

Florianópolis, 2003

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Daniel Bitencourt Cadorin

FERRAMENTA PARA MONITORAMENTO DE REDES IP COM SERVIÇOS DIFERENCIADOS UTILIZANDO SNMP

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para obtenção do grau de Mestre em Ciência da Computação

Prof. Dr. Carlos Becker Westphall
Orientador

Florianópolis, março de 2003

FERRAMENTA PARA MONITORAMENTO DE REDES IP COM SERVIÇOS DIFERENCIADOS UTILIZANDO SNMP

Daniel Bitencourt Cadorin

Esta dissertação foi julgada adequada para obtenção do Título de Mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada na sua forma final pelo programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Dr. Fernando Álvaro Ostuni Gauthier

Coordenador do Curso de Pós-Graduação em Ciência da Computação

Banca examinadora:

_____

Prof. Dr. Carlos Becker Westphall
Presidente

_____

Prof.ª Dr.ª Carla Merkle Westphall

_____

Prof. Dr. Roberto Willrich

Dedicatória

Para minha noiva, Ândrea;

Meu pai, Lauvir;

Minha mãe, Neusa;

Meu irmão, Fábio;

Minha irmã, Laís;

E meus amigos.

Agradecimentos

À Ândrea pelo amor, dedicação, companheirismo e incentivo, que foram muito importantes na realização deste trabalho.

A minha família, que me deu a vida e a oportunidade de estudar, pelo apoio e incentivo constante para que eu nunca desanimasse.

Ao Professor Carlos Becker Westphall pelo incentivo, apoio e orientação.

Aos demais membros da banca:
Prof.ª Carla Merkle Westphall e Prof. Roberto Willrich.

A todos os amigos da ATI – Unisul. Pelo apoio e companheirismo, em especial a Dickson dos Santos Guedes e Rodrigo Santana.

A meu grande amigo Edison Tadeu Lopes Melo, pelo apoio, incentivo e troca de experiências.
A todos os meus amigos e principalmente a Deus.

Resumo

Este trabalho apresenta uma ferramenta para o monitoramento de redes IP com Serviços Diferenciados (DS) utilizando o SNMP. O objetivo dessa ferramenta é capturar valores de configuração e estatísticas do DS em tempo real, através do SNMP.

Para validar a sua funcionalidade, foram executados diversos experimentos, cujos resultados são apresentados através de gráficos criados automaticamente pela ferramenta.

Foram avaliadas duas MIBs da CISCO, que permitem obter informações da estrutura DiffServ configurada em seus roteadores. Para que a ferramenta apresentasse informações relevantes, foram selecionadas, também, através da avaliação das MIBs, as variáveis que serão apresentadas. Definiram-se as formas de como os resultados serão calculados e apresentados. Com essas definições desenvolveu-se a ferramenta de gerenciamento de redes IP com DiffServ utilizando SNMP.

Em todos os experimentos utilizou-se o tráfego EF, que simula uma classe de voz sobre IP. Além deste tráfego, usou-se também o tráfego de background, para saturar o canal em determinados experimentos. Para a classe EF, foram realizadas medições referentes ao atraso, perdas. Através da utilização das MIBs de DiffServ da CISCO, foram obtidas estatísticas relacionadas à utilização das classes de serviço. Realizaram-se, então, medições sobre o percentual de bytes que entram e saem pelas classes e o percentual de bytes que são descartados por elas.

Os resultados obtidos demonstram que, através da ferramenta de gerenciamento de redes IP com Serviços Diferenciados utilizando SNMP, é possível visualizar em tempo real o comportamento dos métodos de DS, o comportamento do tráfego das classes e também descobrir possíveis falhas na configuração do DS.

Abstract

This paper depicts a tool for the monitoring of IP networks with Differentiated Services (DS) by using the SNMP. The object of this tool is that of capturing DS configuration and statistics values in real time, by means of the SNMP.

In order to validate its functioning, a number of experiments were conducted, whose outcomes are shown by charts automatically created by the tool.

Two CISCO MIBs were evaluated, which will allow to gather information from DiffServ structure formed on its steerers. By the evaluation of MIBs, the variables that will be shown, were also screened so that the tool might come up with relevant information. With such definitions, the IP networks management tool with DiffServ using SNMP was developed.

The EF traffic was utilized at all the experiments, which simulates a voice class over the IP. Besides this traffic, the background traffic was also used to saturate the channel at determined experiments. Measurements related to delay, losses, were taken for the EF class. By the use of DiffServ MIBs of CISCO, statistics related to the utilization of service classes were obtained measurements on bytes percentage that come and go by the classes and the percentage of bytes that are discarded by them were, then, taken.

The results gathered show that, by the management tool of IP networks with Differentiated Services utilizing SNMP, it is possible to visualize in real time the behavior of DS methods, the behavior of classes traffic as well as find out possible DS configuration flaws.

Índice

Listas de Figuras

Lista de Tabelas

Lista de abreviaturas

AF	Assured Forwarding
ATM	Asynchronous Transfer Mode
BA	Behavior Aggregate
BE	Best-Effort
CAR	Committed Access Rate
DiffServ	Differentiated Services
DS	Differentiated Services
DSCP	Differentiated Services Code-Point
EF	Expedited Forwarding
FIFO	First In First Out
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
PPP	Point-to-Point Protocol
MF	Multi-field
PHB	Per-Hop Behavior
PQ	Priority Queuing
QOS	Quality of Service
RTT	Round Trip Time
SLA	Service Level Agreement
TOS	Type of Service
UDP	User Datagram Protocol

VOIP	Voice over IP
WAN	Wide Area Network
WFQ	Weighted Fair Queuing

1 INTRODUÇÃO

O mercado está cada vez mais utilizando arquiteturas de Qualidade de Serviço (QOS) nas redes. O principal objetivo da implementação de estruturas deste tipo é o aumento do desempenho e garantia de banda utilizada pelas aplicações importantes nas empresas. Existem duas formas principais para implementar QOS nas redes que são DiffServ (Differentiated Services) e IntServ (Integrated Services). O DiffServ atua basicamente na utilização de mecanismos para classificar, marcar, formatar e priorizar o tráfego [3].

O IntServ atua sob dois princípios básicos: reserva de recursos e controle de admissão, ou seja, antes da transmissão dos pacotes se iniciar, a aplicação faz a solicitação dos serviços, o caminho é configurado e os recursos são previamente alocados [3].

Um fato imprescindível à utilização de QOS é a Voz sobre IP (VOIP). As companhias somente obterão sucesso na implementação de VOIP se estiverem usando algum método de QOS. A utilização de VOIP tem o objetivo, por exemplo, de diminuir custos com ligações entre empresas e suas filiais que estão distribuídas em localizações geográficas distantes. Haja visto que apenas é viável sua implementação se as mesmas linhas que serão utilizadas pela voz também forem utilizadas pelo tráfego das aplicações.

É importante saber o que está sendo utilizado pelo tráfego de voz e pelo tráfego das aplicações. Pois a voz exige prioridade sobre outros tráfegos. De forma que, caso a implementação e a distribuição dos recursos da rede não estiverem bem definidas e analisadas, afetará a qualidade da voz. Por outro lado, é importante analisar as políticas definidas, para validar se realmente os recursos alocados para a utilização da voz estão sendo bem usados ou estão subutilizados. Neste segundo caso, os recursos que não estão sendo utilizados pela voz poderiam ser alocados para o tráfego de outras aplicações.

Gerenciar QOS é tão importante quanto sua implementação. Segundo [1], o suporte a QOS requer medição de desempenho para aferir se os níveis de qualidade especificados foram

alcançados. Quando um provedor de Internet ou uma corporação fornece serviços baseados em QOS para seus usuários, diferentes níveis de medições podem ser realizados:

- Na aplicação para adaptação aos níveis de QOS esperados;
- Pelos usuários para verificar o serviço fornecido pela rede;
- Pelo provedor para monitorar e validar os serviços.

Para [4], há necessidade de se monitorar ao menos três aspectos importantes para testar mecanismos e verificar o desempenho da implementação de QOS: Protocolo, Rede e desempenho de QOS fim a fim.

- **Protocolo:** a monitoração dos protocolos utilizados pela arquitetura de QOS é importante para a validação da sua utilização.
- **Rede:** a monitoração do status geral da rede é importante para conhecer os recursos utilizados e disponíveis para sua utilização e gerência.
- **Desempenho de QOS fim a fim:** monitorar o desempenho do tráfego fim a fim é importante para comparar o pedido inicial do serviço. Este tipo de monitoramento também é necessário para verificar o impacto da combinação de mecanismos heterogêneos de QOS no desempenho fim a fim.

Neste trabalho, será desenvolvida uma ferramenta que permitirá fazer a gerência de redes IP com Serviços Diferenciados utilizando SNMP. Serão selecionadas nas MIBs de QOS variáveis relevantes para o gerenciamento de DiffServ. Será implementado um ambiente de testes para validar a efetividade da ferramenta na gerência de DS. A ferramenta de monitoramento será utilizada para dar apoio na visualização das estatísticas importantes no gerenciamento de DiffServ. As informações de gerenciamento serão obtidas através do SNMP (Simple Network Management Protocol). Serão avaliadas duas MIBs da CISCO existentes para suporte a DiffServ. Com essas informações, o objetivo é obter recursos suficientes para detectar possíveis falhas na implementação de QOS utilizando DiffServ. Também será

possível identificar a superutilização ou subutilização de alguns recursos. Todas estas informações serão visualizadas através de gráficos.

1.2 Trabalhos correlatos

Várias pesquisas já comprovaram que a utilização de QOS é um fator que muito contribui no desempenho das aplicações e satisfação dos usuários nas redes. Em [1] foi feito um estudo sobre efetividade da utilização de QOS usando a arquitetura Serviços Diferenciados (DiffServ) em um ambiente WAN. Os resultados foram positivos. Percebeu-se que houve eficácia quanto ao isolamento e garantia de largura de banda para diferentes classes de tráfego. Pesquisas realizadas pela RNP [2] na implementação de QOS utilizando DiffServ evidenciaram que a utilização de uma estrutura deste nível nas redes traz um grande benefício. A RNP possui um ambiente heterogêneo e com diversos tipos de fluxos. Percebeu-se claramente que para apoiar a utilização de recursos como Vídeoconferência e Telemedicina, a estrutura ideal era implementando DiffServ.

Um estudo experimental de videoconferência pessoal em inter-redes IP com QOS foi realizado pelo Instituto de Computação – IC e Universidade Federal Fluminense – UFF. Foi utilizado o padrão DiffServ para proteger o tráfego de videoconferências do congestionamento causado por um tráfego de melhor esforço. Os resultados deste estudo demonstram que o modelo DiffServ viabiliza a utilização de aplicações de mídia contínua em redes de dados, através do atendimento de seus requisitos, mesmo em condições de congestionamento extremo [5].

1.3 Objetivos do Trabalho

1.3.1 Objetivo geral

Desenvolver uma ferramenta para o monitoramento de redes IP com Serviços Diferenciados utilizando SNMP.

1.3.2 Objetivos específicos

- Implementar um ambiente de QOS utilizando DiffServ;
- Analisar as MIBS existentes para o monitoramento de DiffServ;
- Selecionar variáveis nas MIBs que possibilitem a visualização das estatísticas dos mecanismos de DiffServ em tempo real;
- Visualizar através de gráficos a efetividade da ferramenta no gerenciamento de DiffServ;
- Criar uma forma automatizada de monitoramento de um ambiente de DiffServ.

1.4 Gerência de Redes

Gerenciar uma rede é tão importante quanto seu funcionamento. A gerência de redes pode significar coisas diferentes para pessoas diferentes [6]. A ISO [7] definiu cinco áreas conceituais para o gerenciamento de redes: Gerenciamento de Desempenho, Gerenciamento de Configuração, Gerenciamento de Logs, Gerenciamento de Falhas e Gerenciamento de Segurança. A maioria das redes utiliza a arquitetura básica de gerenciamento. Estações de trabalhos, servidores ou outros dispositivos de rede possuem mecanismos que possibilitam o envio de alarmes quando algo de errado acontece. Também podem possuir um agente que é capaz de armazenar valores de muitas variáveis em uma base de dados. Estas informações podem ser acessadas quando unidades de gerência fazem solicitação aos agentes. Estes buscam a informação desejada na base de dados e informam seus valores ao solicitante.

1.5 QOS e Gerenciamento de QOS

Com o crescimento das redes, novas aplicações começam a ser utilizadas em redes IP. Vários serviços estão sendo agregados neste contexto. Cada usuário da rede envia seus dados e compartilha a largura de banda com todos os fluxos de dados de todos os outros usuários. Neste meio, trafegam informações dos mais diferentes níveis de importância e prioridade para os usuários e empresas. Aplicações com maior prioridade estão disputando com aplicações de baixa prioridade um mesmo meio de comunicação.

Para minimizar este problema, dá-se um tratamento diferenciado nos fluxos de dados através de alguma estrutura de QOS (Quality of Service).

Aplicar algum método de QOS nas redes é necessário quando se busca melhorar o desempenho da mesma e aproveitar de forma mais eficiente todos os seus recursos. Desta forma, é possível priorizar também o tráfego das aplicações de maior importância.

Para garantir que os métodos de QOS utilizados estão sendo eficazes, é necessário que seja feito um gerenciamento intensivo e contínuo. É importante avaliar os resultados de uma implementação de QOS, verificando se as respostas das aplicações analisadas estão alcançando as métricas de QOS desejadas [22]. Uma das formas mais eficientes de monitorar a efetividade destes métodos de QOS é utilizando o SNMP (Simple Network Management Protocol).

1.6 SNMP (Simple Network Management Protocol)

No início das redes de computadores, os problemas que aconteciam com os alguns componentes das redes eram facilmente detectados através de alguns testes. Esta facilidade se dava pela pequena quantidade de equipamentos que faziam parte da rede. Com o passar dos tempos, as redes foram crescendo. Vários equipamentos foram interligados através dela. Com este crescimento, paralelamente foi aumentando a necessidade de se criar uma estrutura que facilitasse o controle de todos estes equipamentos interligados.

Houve algumas tentativas em se definir melhores ferramentas para facilitar este gerenciamento, mas não obtiveram sucesso. Depois foi publicada a RFC 1157. Nela foi definida a primeira versão do SNMP (**SIMPLE NETWORK MANAGEMENT PROTOCOL).** Com esta estrutura de gerenciamento, tornou-se mais fácil e otimizada a tarefa de gerenciamento da rede. Vários fabricantes começaram a implementar o SNMP em seus produtos. Em pouco tempo, o SNMP tornou-se um padrão no gerenciamento de redes.

Como sua utilização tornou-se grande, foram descobertas várias falhas no projeto do SNMPv1. Então foi desenvolvida uma nova versão do SNMP, chamada de SNMPv2, que tinha como objetivo corrigir várias deficiências do SNMPv1, principalmente em relação à segurança do protocolo. O SNMPv2 tornou-se um padrão da Internet. Esta versão foi e está sendo muito utilizada ainda, embora já tenha sido publicada a versão SNMPv3, que busca aumentar ainda mais a segurança inserindo criptografia na comunicação entre o agente e o gerente.

1.7 Organização do Trabalho

No capítulo 1, apresentaremos conceitos básicos relacionados a QOS, gerência de redes, gerência de QOS. Depois veremos no capítulo 2 definições importantes sobre QOS e DiffServ. No capítulo 3, analisaremos as MIBs SNMP que serão utilizadas para o gerenciamento de DiffServ. Através destas MIBs serão selecionadas as variáveis importantes que devem ser capturadas pela ferramenta de gerência de DiffServ. Será descrito no capítulo 4 como foi a implementação do ambiente onde foram configurados os equipamentos com mecanismos de qualidade de serviço ativados. Para fazer a análise deste ambiente, será também apresentada neste capítulo a ferramenta desenvolvida para o gerenciamento de redes IP com DiffServ utilizando o SNMP. Os experimentos foram definidos para que fosse possível simular as várias situações em que uma rede pode se encontrar. Após a execução dos experimentos, no capítulo 5 será feita a validação da ferramenta através da apresentação dos resultados obtidos.

2 QUALIDADE DE SERVIÇO E GERÊNCIA SNMP

2.1 Qualidade de Serviço (QOS)

Em [8], QOS é fornecer um serviço de entrega dos dados consistente e confiável, ou seja, satisfazendo as exigências das aplicações dos clientes. Para [12], QOS combina técnicas inteligentes para a melhor utilização dos recursos de rede disponíveis com as necessidades das aplicações. Já em [14], QOS refere-se à capacidade da rede em prover melhores serviços para tráfegos selecionados sobre várias tecnologias, incluindo Frame Relay e ATM. Isso é feito concedendo melhores serviços para determinados fluxos e minimizando recursos para fluxos com menor prioridade.

De uma forma geral, QOS é a habilidade para definir níveis de performance na comunicação de dados [13]. A idéia de QOS é prover largura de banda suficiente com qualidade adequada, de forma que o uso da largura de banda seja tão eficiente quanto for possível [15]. Atualmente na Internet, a forma mais utilizada para o encaminhamento de pacotes é chamada de "Melhor Esforço". Esta filosofia de trabalho funciona muito bem, dependendo das condições das redes e das necessidades das aplicações. Quando uma rede está congestionada, os pacotes são descartados indiscriminadamente, ou seja, fluxos de várias aplicações podem ser descartados.

Existem aplicações que são sensíveis a qualquer tipo de perda ou atraso. Dessa forma, elas exigem um nível de confiabilidade mais elevado por parte das redes. Neste momento é possível visualizar a importância de se utilizar algum método de QOS nas redes. QOS é uma solução que está sendo tratada com muita seriedade por parte dos grupos de pesquisas como ATM Fórum [9] e IETF [10], empresas e fabricantes de dispositivos de redes.

Existem algumas técnicas para o provimento de QOS nas redes. As principais são DiffServ e IntServ. Aplicar QOS nas redes não é mais um acontecimento distante. É um fato real. As redes estão crescendo, os usuários estão aumentando, proporcionalmente o tráfego está subindo. A largura de banda é um item extremamente importante para uma rede que está crescendo muito. Mas largura de banda não elimina a necessidade de QOS, da mesma forma que QOS não cria largura de banda. QOS deve ser usado para alocar e garantir recursos da largura de banda existentes para determinadas situações [11].

Diversas aplicações não suportam o uso concorrente dos mesmos recursos de rede. Para elas, é importante que exista um tratamento diferenciado para seus fluxos. Através de um mecanismo de QOS, é possível dar um tratamento especial para fluxos predefinidos. Dessa forma, é possível garantir que determinadas aplicações sempre terão recursos de rede disponíveis.

2.2 Serviços Diferenciados (DiffServ)

No item 2.1, percebe-se a importância de se obter QOS nas redes. Com isto, surgiu o pensamento de se criar alguma forma simples e eficiente para dar um tratamento especial para diferentes classes de serviços para o tráfego da Internet. Também se pensou em uma estrutura que suportasse vários tipos de aplicações, principalmente que suportasse as exigências de negócios de cada empresa. Baseado neste pensamento, foi criado o grupo de trabalho do IETF [10], chamado de Differentiated Services (DiffSserv) [16]. Este grupo tem por objetivo padronizar a arquitetura DiffServ, muito utilizada para prover QOS nas redes IP. A arquitetura de Serviço Diferenciado tornou-se o método preferido para obter qualidade de serviço (QOS) em redes IP, principalmente pela sua simplicidade e facilidade de configuração [23].

A definição desta arquitetura é baseada no campo DS, que substitui a definição do byte TOS existente no cabeçalho do pacote IPv4 e o byte Class no cabeçalho do pacote IPv6.

Seis bits do campo DS são usados como codepoint (DSCP) para selecionar o PHB em cada nó. Os bits (CU) são dois bits restantes do campo DS. Atualmente, não são usados e são reservados para utilização futura. Os valores dos bits CU são ignorados pelos nós que possuem DiffServ quando determinam a seleção do PHB para aplicar em um pacote recebido [17].

A figura 2.2.1 mostra a estrutura do campo DS.

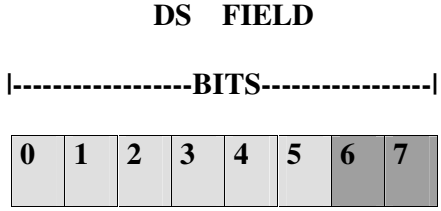


Figura 2.2.1 – Estrutura do campo DS

DSCP – Differentiated services codepoint

CU - Currently Unused

Serviço Diferenciado é obtido através da concatenação de várias redes, também conhecida como Domínio DS utilizando a arquitetura DiffServ. Para fornecer um serviço diferenciado fim-a-fim, é necessário que cada nó integrante do Domínio DS contenha políticas comuns de tratamento diferenciado para o tráfego que atravessa o domínio. Este tratamento é dado através de definições Per Hop Behavior (PHB) [23].

Um domínio DS tem nós de borda e nós de interior [1]. Cada nó de borda é responsável por fazer a classificação e a moldagem do tráfego que entra no domínio DS. Estas funções são executadas por vários componentes existentes em cada nó do domínio DS.

Para poder dar um tratamento diferenciado em determinados fluxos de dados, primeiramente é necessário que este tráfego seja classificado. Esta classificação pode ocorrer através de duas formas. Na primeira, o nó, utilizando seu classificador, classifica o tráfego baseado em vários campos do protocolo IP. Campos como endereço IP, portas TCP ou UDP, ou classifica baseado na combinação de alguns desses campos. Este classificador tem uma função mais complexa, examinando vários campos do pacote IP. Por este motivo, é utilizado em equipamentos de borda do domínio DS. Este classificador chama-se MF – Multfield Classifier. Após classificar o pacote, o próximo passo será verificar através de uma medição se o pacote está de acordo com algum perfil de tráfego preestabelecido. Se estiver de acordo, o pacote será marcado com o DSCP. Em seguida, passará para os procedimentos de envio ou será descartado.

A outra forma de classificação é baseada na marcação do campo DS, através do DSCP. Esta forma é mais simples pelo fato de que o nó não precisará fazer a classificação baseando-se em vários campos do cabeçalho do pacote IP. Ele simplesmente analisa qual é a marcação existente no campo DS. Este classificador chama-se BA – Behaviour Agregate. Ele é utilizado em nós internos do domínio DS. Existem alguns fatores importantes que evidenciam a utilização de classificadores do tipo BA somente em nós do interior do domínio DS. Um dos fatores relevantes que não aconselha utilizar classificador BA em nós de extremidade da rede é que poderão chegar pacotes com marcações não confiáveis ou até mesmo sem marcação. Neste caso, o classificador BA não poderá saber qual é a credibilidade desta marcação. Outro fator importante na utilização do classificador BA em nós internos do domínio DS é que estes nós não terão a necessidade de muito hardware, fazendo com que o custo também seja menor. Após ter sido classificado o perfil do pacote, é possível aplicar políticas definidas pelo administrador da rede para determinados perfis de tráfego para que seja efetuado o reenvio.

No encaminhamento dos pacotes, [1] os campos DSCP (DiffServ Code Point) são mapeados para os PHBs (Per Hop Beahaviours) [17] definidos na arquitetura DiffServ. Per Hop Behaviours (PHBs) definem o comportamento de encaminhamento de um pacote em um nó DiffServ. Existem dois tipos de PHBs que foram padronizados pelo IETF [10].

O PHB EF [18] e o PHB AF [19]. O PHB EF [1] é também definido como serviço premium ou de canal dedicado. Pode ser usado para tráfego com requisitos de baixa perda, baixo atraso, baixa variação de atraso e garantia de largura de banda. No PHB AF, é possível dividir o tráfego em até quatro classes diferentes. É possível fazer ainda com que cada classe seja subdividida em três níveis para preferência de descartes. Os níveis são Baixo, Médio e Alto e também podem ser caracterizados pelas cores vermelha, amarela e verde, respectivamente [23]. No caso de congestionamento, o PHB AF descarta pacotes com mais baixa procedência. Podem ser utilizados vários níveis de procedência de descartes para se fazer a distribuição da largura de banda de forma que evite o congestionamento. Dependendo das exigências de QOS e o nível de emergência, podem ser configurados fluxos de tráfego para usuários com prioridade para uma das quatro classes. Dentro de cada classe podem ser criadas procedências de descartes apropriadas para cada situação [23].

2.3 Gerenciamento de Tráfego

A grande utilização pelo tráfego de voz, vídeo e dados em um link pode exceder sua capacidade de transmissão. Neste caso, um roteador não poderá fazer nada a não ser descartar o tráfego excedente. Isto pode comprometer a performance de algumas aplicações. A presença de congestionamento significa que a carga é maior do que os recursos de uma parte do sistema podem suportar [20]. Para que isso não ocorra, é necessário que haja algum

mecanismo que gerencie a entrada e saída do tráfego nas interfaces do um roteador. Estes mecanismos são chamados de gerenciadores de filas.

Após o tráfego ser identificado, configurado sua prioridade e mapeado para seu PHB, o próximo passo é servir as filas das interfaces. As filas podem trabalhar sob dois conceitos. No primeiro, os pacotes somente deixam as filas quando forem servidos pelo roteador. No segundo, os pacotes podem ser descartados enquanto esperam na fila [23].

As filas não têm tamanhos infinitos. Em determinados momentos elas podem encher. Neste caso, quando chegam pacotes, imediatamente são descartados. Mas como o roteador faz para saber se o pacote tem alta prioridade antes de entrar na fila? Para esta situação existem algumas ferramentas que são conhecidas como gerenciadores de filas, que precisam fazer duas coisas:

- Tentar fazer com que a fila não encha e que sobre lugar para os pacotes de alta prioridade;
- Usar algum critério que permita descartar pacotes de mais baixa prioridade antes dos pacotes com mais alta prioridade.

Um mecanismo que possui estas duas características é chamado de Weighted early random detect (WRED) [22].

2.3.1 Ferramentas de Gerenciamento de Tráfego

Evitar congestionamento é uma forma de gerenciar filas. As filas são ferramentas que buscam monitorar a carga do tráfego da rede com o objetivo de antecipar e evitar o congestionamento e gargalos comuns nas redes. Uma forma para minimizar o descarte de pacotes em um link que está sobrecarregado é usar algum algoritmo de gerenciamento que

crie e ordene os pacotes em filas. Depois, determina o método de priorização que será utilizado. Existem vários métodos de enfileiramento:

- **First-in, first-out (FIFO) queuing**
- **Priority queuing (PQ)**
- **Custom queuing (CQ)**
- **Flow-based weighted fair queuing (WFQ)**
- **Class-based weighted fair queuing (CBWFQ)**

Cada algoritmo foi desenvolvido para resolver problemas diferentes. Por padrão, se um link não estiver congestionado, não há necessidade de enfileirar os pacotes. Sem ausência de congestionamento, os pacotes são encaminhados diretamente para a interface de saída [22].

- **First-in, first-out (FIFO) queuing**

Enfileiramento FIFO envolve armazenamento do pacote quando a rede está congestionada e encaminhamento do mesmo quando a rede está disponível. Os pacotes são enviados para a interface de saída na mesma ordem como chegam na interface de entrada.

Esta é a técnica padrão de filas. Utiliza poucos recursos de processamento. Porém, não pode dar nenhum tratamento de prioridade para tráfego de emergência [23].

- **Priority queuing (PQ)**

Nesta forma de enfileiramento é garantida a manipulação mais rápida para o tráfego mais importante. Nela a priorização pode ser feita de uma forma muito flexível através do protocolo de rede, destino do pacote de entrada ou saída, interface de entrada ou saída, tamanho do pacote, etc. Em PQ, os pacotes são colocados em quatro filas com diferentes prioridades: alta, média, normal e baixa. Na transmissão, o algoritmo dá prioridade absoluta

para as filas de alta prioridade sobre as filas de baixa prioridade. Neste caso, as filas de baixa prioridade são servidas quando as filas de alta prioridade estão vazias. Este esquema provê QOS para tráfego de emergência. Em contra partida, deixa as filas de baixa prioridade com poucos recursos [23].

Em [1] este mecanismo de enfileiramento por prioridade pode ter um efeito adverso no desempenho de encaminhamento dos pacotes por causa da reordenação destes na fila de saída e, também, porque o roteador tem que analisar em detalhes cada pacote para saber como ele deve ser enfileirado, sobrecarregando desta forma o processador.

- **Custom queuing (CQ)**

CQ foi criada para que várias aplicações com baixas necessidades de largura de banda e exigências quanto à latência compartilhem os recursos da rede. Neste ambiente, a largura de banda deve ser compartilhada proporcionalmente com as aplicações e usuários. Pode-se utilizar largura de banda garantida para um fluxo que seja um ponto em potencial para iniciar um congestionamento. Neste caso, o restante da largura de banda poderá ser utilizado para outros fluxos.

- **Weighted fair queuing (WFQ)**

Este método é mais recomendado que o FIFO. WFQ envolve uma série de filas competindo com prioridades configuradas pelos valores do IP Procedence e tamanho dos pacotes. Este algoritmo tenta manter servidas as filas de baixa prioridade dando, ao mesmo tempo, tratamento diferenciado para o tráfego de alta prioridade. O número de filas não é fixo e pode ser ajustado.

Esta estratégia de enfileiramento está entre a Priority queuing (PQ), a qual deixa faltar recursos para filas de baixa prioridade, indiscriminadamente, e Custom queuing (CQ), o qual mantém fixas as classes de tráfego [23].

- **Class-based weighted fair queuing (CBWFQ)**

Quando o administrador deseja prover uma quantidade mínima de largura de banda, deve utilizar CBWFQ. Esta técnica de enfileiramento permite que o administrador crie o mínimo de classes com largura de banda garantida. Ao invés de definir filas para fluxos individuais, são definidas filas para classes que podem possuir um ou mais fluxos. Um exemplo no qual este algoritmo pode ser usado é prevenindo que múltiplos fluxos de baixa prioridade saiam como um simples fluxo de alta prioridade.

2.3.2 Ferramentas para evitar o congestionamento

- **Random Early Detection (RED)**

O algoritmo random early detection (RED) é utilizado para evitar congestionamento nas redes antes que isso se torne um problema. Este algoritmo é utilizando em grandes redes IP. A técnica descobre que vai acontecer congestionamento através de cálculos feitos sobre a média do tamanho das filas [23]. Este enfoque é diferente das técnicas de enfileiramento descritas acima.

O RED trabalha monitorando a carga de tráfego em determinados pontos da rede. descarta pacotes se percebe que o congestionamento começa aumentar. Quando efetua o descarte de um simples pacote, o roteador envia um sinal ao host de origem, informando que houve congestionamento. Este sinal é enviado através do protocolo da camada de transporte [23]. O

resultado é que a fonte percebe que o pacote foi descartado, então diminui sua taxa de transmissão [22]. Dessa forma, evita o transbordamento da fila. Este algoritmo foi desenvolvido para trabalhar principalmente com os protocolos IP e TCP. Ele é o mais recomendado para se implementar mecanismos AF. A principal vantagem do RED é o fato de evitar a sincronização global de muitas conexões ao mesmo tempo [23].

- **Weighted Random Early Detection (WRED)**

O WRED combina a capacidade do algoritmo RED com o IP Procedence. Esta combinação possibilita fazer uma manipulação preferencial para pacotes com alta prioridade. Através dele, é possível selecionar e descartar pacotes com baixa prioridade quando se inicia um congestionamento na rede. Em uma fila pode ser colocado um número fixo de pacotes. Com uma fila cheia, inicia-se o processo de descarte de pacotes. No entanto, isto não é aconselhável, pois o roteador não terá como ver o IP Procedence.

2.4 Níveis de QOS

Nível de serviço refere-se à capacidade de uma rede obter QOS fim-a-fim. Os níveis de serviço se diferem pela largura de banda, atraso, variação de atraso ou características de perda.

Segundo [22], três níveis básicos de QOS fim-a-fim podem existir em uma rede heterogênea:

- **Serviço de melhor esforço:** também conhecido como serviço sem QOS. Neste caso, não existe garantia nenhuma a qualquer tipo de tráfego. Não existe diferenciação para os fluxos;

- **Serviço diferenciado:** Uma parte do tráfego é tratada diferentemente do resto. Este tráfego é manipulado mais rapidamente, tem maior largura de banda disponível e menor taxa de perda.
- **Serviço garantido:** Faz uma reserva absoluta dos recursos da rede para determinado tráfego.

2.5 Classificação dos fluxos

Para poder dar prioridade para determinado fluxo, primeiro é necessário classificá-lo e marcá-lo. Esta tarefa chama-se classificação. Basicamente a identificação dos fluxos é feita através de access control lists (ACLs). Estas ACLs identificam o tráfego para o gerenciamento do congestionamento. No momento em que os pacotes chegam no roteador, é possível identificá-los através de métodos da CAR (Committed Access Rate). Estes métodos são utilizados nos roteadores CISCO e possibilitam a identificação dos fluxos através de redes IP fonte/destino, porta TCP/UDP. Além destes métodos, a CAR permite identificar se determinados fluxos que estão entrando na interface excedem a quantidade de largura de banda que foi alocada para este fluxo. Após fazer a análise do fluxo, é feita a comparação com o que está configurado no roteador.

2.6 Modelo e características do SNMP

Em [20], o modelo de uma rede gerenciada consiste em quatro componentes, que são os seguintes:

- **Nós gerenciados**
- **Estações de gerenciamento**
- **Informações de gerenciamento**
- **Protocolo de gerenciamento**

De uma forma geral, o gerenciamento dos dispositivos de redes se dá através de três componentes básicos: Agente, MIB (Management Information Base) e Gerente. Uma aplicação de gerência baseia-se na troca de informações entre um Agente e um Gerente.

O Agente é o componente que faz a coleta das informações dos dispositivos gerenciados. Estas informações referem-se ao estado de funcionamento do equipamento e também ao estado de muitas outras variáveis. Todas estas informações são armazenadas na MIB. Também é ele quem realiza operações de gerenciamento sobre os objetos contidos na MIB, atendendo as solicitações feitas pelo gerente.

A MIB é o componente essencial para as aplicações de gerenciamento. Nela estão contidas todas as informações referentes aos dispositivos de rede. Através das informações contidas na MIB, é possível que seja feita uma detecção e correção de possíveis falhas nas redes. Como SNMP é um padrão em gerenciamento de redes, vários fabricantes de componentes de redes utilizam agentes SNMP em seus produtos. A MIB foi desenvolvida com o intuito de fazer com que fosse possível a comunicação entre componentes de diferentes fabricantes. Por esta razão, para escrever a MIB foi utilizada uma linguagem de definição de objetos chamada de ASN.1 (Abstract Syntax Notation 1). Esta linguagem tinha um caráter neutro em relação ao fornecedor, possibilitando assim a criação de uma estrutura padronizada

para diferentes fabricantes. O próximo passo foi criar uma estrutura para construir os objetos na MIB de uma forma padronizada. Surge, então, a SMI (Structure of Management Information). Esta realmente foi usada para definir estruturas de dados do SNMP [20].

O Gerente é o componente que monitora o estado dos dispositivos da rede. Este monitoramento é realizado através de solicitações feitas aos agentes que estão embutidos nos equipamentos das redes. Quando o gerente envia estas solicitações aos agentes, estes fazem um acesso à MIB e devolvem ao gerente o estado da variável que ele solicitou. Com o valor desta variável ou de outras variáveis em mãos, o gerente pode executar uma série de tarefas configuradas pelo administrador da rede. Tarefas como enviar um e-mail ao administrador da rede, fazer uma ligação para o celular dele e avisar sobre o problema, alterar a cor do dispositivo na console da estação de gerência, entre outras funções.

Observando estas vantagens, visualiza-se claramente a importância e o benefício que o gerenciamento de redes através do SNMP pode oferecer.

2.6.1 Comunicação entre os componentes da arquitetura SNMP

Para que uma plataforma de gerência de rede utilizando a estrutura do SNMP funcione de forma adequada, é importante conhecer como funciona a comunicação, a troca de informações entre os componentes da estrutura do SNMP. A figura 2.6.1.1 apresenta o estado inicial de uma rede que possui a plataforma de gerência baseada no SNMP.

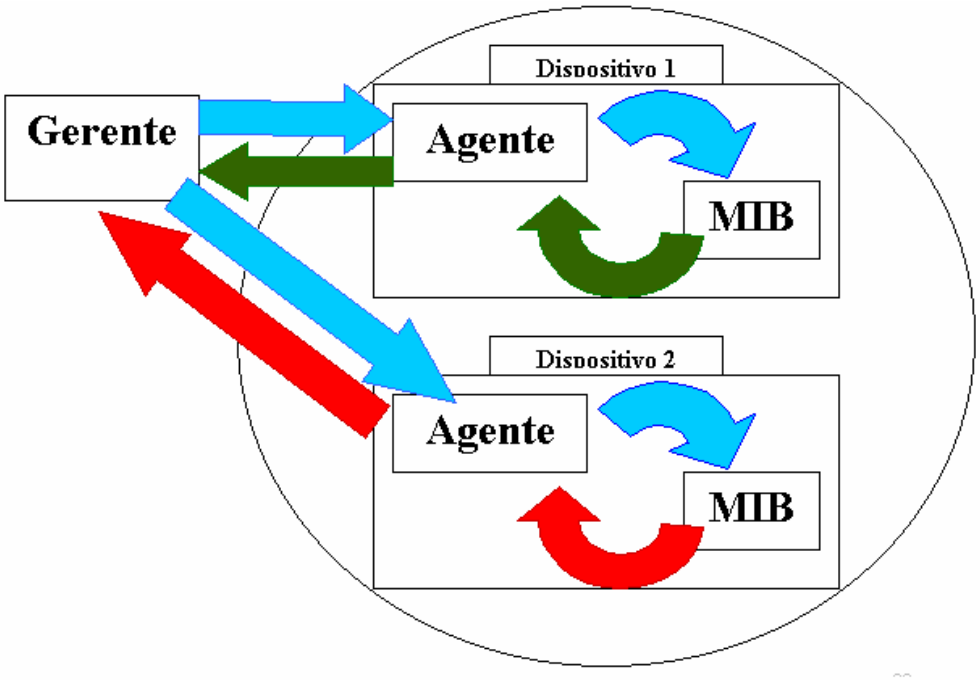


Figura 2.6.1.1 - Rede com um gerente e dois dispositivos gerenciados

Como foi abordado no item 2.3, para que o gerenciamento dos dispositivos da rede funcione de forma adequada, é importante que a comunicação entre o agente e o gerente esteja funcionando de forma correta.

Na estação gerente deve existir um software que possibilite criar os gráficos da estrutura da rede. Este software também deve ser capaz de descobrir a topologia da rede e automaticamente gerar um gráfico contendo todos os componentes da rede juntamente, com suas características. Através deste gráfico, é possível manter um acompanhamento mais efetivo sobre o estado dos dispositivos da rede e conseqüentemente da rede como um todo. Este software também é capaz de alertar sobre problemas utilizando uma forma gráfica, ou seja, alterando a cor de algum dispositivo que esteja com problema. Desta forma, facilmente o administrador da rede terá condições de tomar conhecimento do problema visualizando na tela do computador onde está o software de gerência.

Quando um gerente necessita de informação sobre uma variável de algum dispositivo, ele envia uma solicitação para o agente deste dispositivo, informando o que ele deseja. A solicitação é feita através da mensagem **Get-request**, juntamente com o parâmetro informando a variável desejada. Quando o agente recebe esta mensagem, ele faz uma busca na MIB. Após encontrar, extrai o valor e retorna o resultado ao gerente. Existe ainda uma outra forma de solicitar os valores de muitas variáveis da MIB ao mesmo tempo. Para isto, utiliza-se a mensagem de **Get-next-request,** que também envia acoplada nesta mensagem a variável a qual se deseja que seja iniciada uma extração seqüencial dos valores das outras variáveis. Esta extração segue até chegar na última folha que deriva desta ramificação na árvore da MIB. Outra mensagem importante utilizada pelo SNMP é a mensagem de **Set-request**. Esta é utilizada quando o gerente quer alterar o valor de alguma variável. Para fazer isso, o gerente precisa informar à mensagem de **Set-request**, mais a variável a ser alterada e qual o valor que ele deseja para esta variável. A figura 2.6.1.2 apresenta uma solicitação simples do gerente para o agente, utilizando a mensagem de **Get-request**.

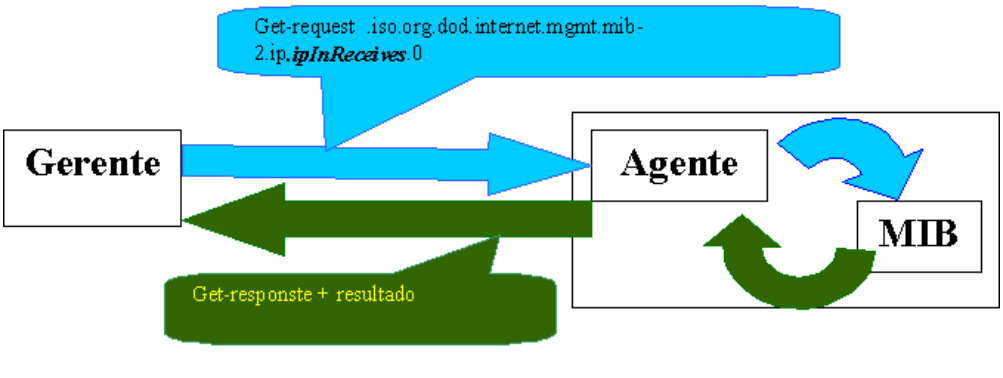


Figura 2-6.1.2 – Gerente solicita o valor de uma variável e obtêm a resposta

Talvez uma das mensagens mais importantes do SNMP é a mensagem de **Trap.** Esta é enviada pelo agente ao gerente sempre que ocorre algum evento anormal no dispositivo de rede, isto é, se for um evento que o Agente SNMP possa detectar.

A comunicação entre o Gerente e o Agente pode ser realizada através de duas formas. Na primeira, a comunicação inicia a partir do Gerente. De tempos em tempos, o software de gerência deve consultar os nós gerenciados para ver qual é seu status de operação. Esta forma de monitoramento é eficiente, mas também possui uma deficiência muito relevante. Como as consultas são feitas em ciclos de tempos, pode acontecer um problema em um nó da rede onde o gerente acabou de fazer a consulta. Neste caso, se não existe nenhuma outra forma para que o gerente detecte o problema, o mesmo somente será visualizado no momento em que o gerente fizer uma nova consulta nos dispositivos da rede. Ou seja, se o tempo configurado para o gerente fazer esta consulta rotineira (também conhecida como **polling**) for muito elevado, o tempo para solução do problema pode demorar ainda mais. Por outro lado, se o tempo de **polling** for configurado muito baixo, pode gerar um tráfego desnecessário e prejudicial para a rede.

A outra forma de comunicação inicia do Agente ao Gerente. Esta busca otimizar a utilização da rede em relação ao software de gerência de rede. Em cada nó gerenciado é informado um endereço **IP** que está associado às mensagens de **Trap**. Assim que o Agente SNMP toma conhecimento do problema, imediatamente envia uma mensagem avisando que existe um problema à estação de gerência, possibilitando que o gerente faça todos os testes necessários para ver o que aconteceu e possa solucionar o problema.

2.7 Conclusão do capítulo

Neste capítulo, foi apresentado com mais detalhes o funcionamento de QOS e DiffServ em redes IP. Foram apresentados os mecanismos e ferramentas para o gerenciamento de tráfego. Também descreveu-se em detalhes o modelo de gerenciamento SNMP. No próximo capítulo, será apresentado o propósito geral do trabalho e serão analisadas e selecionadas as variáveis das MIBs que a ferramenta irá utilizar para o gerenciamento de DiffServ.

3 PROPÓSITO GERAL DO TRABALHO

3.1 Descrição

O propósito geral deste trabalho é desenvolver uma ferramenta para o monitoramento de redes IP com Serviços Diferenciados utilizando SNMP. Através dessa ferramenta será possível obter informações importantes que permitirão analisar a atuação de mecanismos de DS bem como descobrir possíveis problemas de configuração. Para isso, é necessário encontrar e selecionar os valores que possibilitam a visualização em tempo real de informações úteis.

3.2 Estrutura SNMP utilizada para captura das informações DiffServ

Uma das melhores formas de se obter informações em tempo real sobre estatísticas da implementação/utilização de DS é através do SNMP. Pois a característica deste protocolo possibilita manter nos equipamentos onde estão sendo aplicadas as políticas de DS informações importantes sobre tudo o que está acontecendo.

Estas informações são capturadas pelos agentes SNMP que estão nos equipamentos. Eles pegam as informações e as armazenam nas MIBs, que estão implementadas em cada nó do domínio DS.

Existem algumas MIBs que armazenam informações somente sobre DS. Apesar de alguns fabricantes possuírem suas MIBs proprietárias, o grupo de pesquisa do IETF chamado DIFFERENTIATED SERVICES**,** definiu a MIB padrão para o gerenciamento de QOS que utiliza a estrutura DIFFSERV [21].

Como o ambiente utilizado para a análise de DS foi baseado em equipamentos da CISCO, as MIBs utilizadas para captura das informações foram definidas pela própria CISCO. As MIBs utilizadas formam: CISCO-CAR-MIB e CISCO-CLASS-BASED-QOS-MIB.

3.3 CISCO-CAR-MIB

A CISCO-CAR-MIB é uma MIB proprietária, através da qual é possível obter informações sobre configurações e estatísticas da classificação e moldagem do tráfego que chega no domínio DS. Por esta razão, esta MIB deve ser analisada nos equipamentos das extremidades do domínio DS. A forma de configurar a classificação e moldagem do tráfego nestes dispositivos é através de métodos da CAR (Commited Access Rate). Através dela, é possível utilizar critérios muito flexíveis que permitem limitar as taxas de tráfego de entrada e saída das interfaces e subinterfaces. Também possibilita que seja moldado o perfil deste tráfego. Outra qualidade é a possibilidade de classificar os pacotes através de diferentes características utilizando o tipo de Classificador MF apresentado na seção 2.2.

3.3.1 Descrição das variáveis de configuração da CISCO-CAR-MIB

Para analisar as estatísticas da implementação de métodos da CAR, é importante que sejam visualizadas as características de configuração em determinado equipamento. Para isto, foi definido como necessária a captura das seguintes variáveis:

- **ccarConfigDirection:** esta variável tem um valor inteiro e indica em que direção está aplicada a configuração. Ela pode possuir dois valores, 1 ou 2, que indicam entrada e saída, respectivamente.
- **ccarConfigAccIdx:** esta variável tem um valor inteiro e indica a que ACL esta regra da classe está associada.
- **CcarConfigRate:** esta variável apresenta a taxa de acesso garantida pela classe. Ela apresenta a unidade em **bits/segundo**.
- **ccarConfigLimit:** esta variável apresenta a quantidade de tráfego em bytes que excedem a taxa de acesso garantido no qual será instantaneamente permitida pela classe.
- **ccarConfigExtLimit:** esta variável apresenta a quantidade de tráfego máxima em bytes que excedem a configuração do limite, na qual condicionalmente será permitido pela classe. A probabilidade do tráfego não ser permitido aumenta à medida em que aumenta o tráfego que ultrapassa o limite permitido. O cálculo é feito através de **P(não permitido) = (BurstRate - ConfLimit) / (ConfLimitExt - ConfLimit).**
- **CcarConfigConformAction:** esta variável apresenta a ação que será efetuada para o tráfego que estiver de acordo com a configuração da classe.
- **ccarConfigExceedAction**: esta variável apresenta a ação que será efetuada para o tráfego que não estiver de acordo com a configuração da classe.

3.3.2 Descrição das variáveis de estatísticas da CISCO-CAR-MIB

Verificar as estatísticas da CAR é necessário principalmente para saber se os acordos de nível de serviço (SLA) estão sendo cumpridos. É necessário saber também qual é a taxa de bytes que está entrando em cada classe e a taxa de bytes que está sendo descartada em cada classe. Dessa forma, é possível saber se está sendo garantido por parte do provedor de serviços o que foi acordado, como também saber se a taxa de dados que o cliente está enviando está sendo cumprida ou ultrapassando os limites.

As variáveis utilizadas para a captura destas informações são:

- **ccarStatSwitchedBytes**: esta variável é um contador que apresenta em bytes a quantidade de tráfego que se encaixou nas classes.
- **CcarStatFilteredBytes:** esta variável é um contador que apresenta em bytes a quantidade de tráfego que ultrapassou a classe e foi descartada.

3.4 CISCO-CLASS-BASED-QOS-MIB

A outra MIB utilizada é a CISCO-CLASS-BASED-QOS-MIB [25]. Através desta MIB, é possível obter informações sobre as classes de tráfego que estão criadas nos roteadores internos do domínio DS. Embora possa ser utilizada nos roteadores de extremidades do domínio DS. É possível conhecer também as políticas definidas para o tráfego bem como a característica destas políticas.

3.4.1 Descrição das variáveis de configuração da CISCO-CLASS-BASED-QOS-MIB

Para uma visualização adequada das configurações de QOS, é necessário conhecer as políticas configuradas. Nestas políticas é importante saber a qual interface ela está aplicada. Dentro de cada política, é necessário obter informações das classes configuradas. Em cada classe, deve ser apresentado o padrão de comparação (match) no qual o tráfego será comparado para saber se está dentro do perfil da classe.

Na política das classes estão configurados os algoritmos de enfileiramento que serão aplicados ao tráfego de cada classe. Os algoritmos de enfileiramento que serão tratados e apresentados no ambiente são o Priority Queue e o Fair-Queue.

É necessário ainda obter a informação sobre a quantidade de largura de banda garantida pela classe.

Com as informações de configuração das classes e políticas, é possível apresentar as configurações de DS através da CISCO-CLASS-BASED-QOS-MIB. Nesta MIB existem diversas variáveis que apresentam informações de configuração de DS. Mas serão apresentadas as informações das variáveis que através de vários testes foram julgadas como relevantes.

3.4.2 Definição das variáveis selecionadas na CISCO-CLASS-BASED-QOS-MIB

3.4.2.1 Informações relacionadas às políticas

- É importante saber qual é o nome e a descrição da política;
- É importante saber a qual interface esta política está associada;
- É importante saber a qual direção esta política está associada.

3.4.2.2 Informações relacionadas à classe

- É necessário saber a qual política esta classe está associada;
- É importante saber a quantidade de tráfego que entra em determinada classe;
- Também é importante saber a quantidade de tráfego que sai por uma determinada classe;
- Outra informação relevante é saber a quantidade de tráfego que foi descartado pela classe.

3.4.2.3 Informações relacionadas aos padrões de comparação

- Em cada padrão de comparação (match) deve ser apresentada a quantidade de tráfego que está dentro dos seus padrões.

3.4.2.4 Informações relacionadas aos algoritmos de enfileiramento

- Cada classe é associada a algum algoritmo de enfileiramento. Os algoritmos que serão apresentados são Priority Queue e o Fair-Queue.
- É necessário obter a variável que informe a quantidade de largura de banda alocada para determinada classe.

Todas estas informações são obtidas através das variáveis descritas a seguir:

✓ **Informações relacionadas às políticas**

- **cbQosIfType**: esta variável apresenta informação referente a que interface determinada política de QOS está associada.
- **CbQosPolicyDirection:** esta variável apresenta informação referente a que direção a política de QOS está configurada.
- **CbQosPolicyMapName:** esta variável apresenta informação sobre o nome da política criada.
- **CbQosPolicyMapDesc:** esta variável apresenta informação sobre a descrição da política criada.

✓ **Informações relacionadas às classes**

- **CbQosCMName:** esta variável apresenta informação sobre o nome da classe criada.
- **CbQosCMDesc:** esta variável apresenta informação sobre a descrição da classe criada.

- **CbQosQueueingCfgBandwidth:** esta variável apresenta o valor da banda alocada para determinada classe.
- **CbQosQueueingCfgBandwidthUnits:** esta variável apresenta a unidade do parâmetro de configuração de largura de banda alocada para a classe.
- **CbQosQueueingCfgFlowEnabled:** esta variável apresenta um valor booleano, o qual indica se o algoritmo de enfileiramento fair-queue está habilitado para a classe.
- **CbQosQueueingCfgPriorityEnabled:** esta variável apresenta um valor booleano, o qual indica se o algoritmo de enfileiramento priority está habilitado para a classe.

✓ **Informações relacionadas ao padrão de comparação (match)**

- **CbQosMatchStmtName:** esta variável apresenta o tipo de padrão que está configurado para a classe.

3.5 Estatísticas através de gráficos

Além da apresentação dos valores descritos acima, é importante gerar gráficos que permitam o acompanhamento em tempo dos valores das estatísticas do DS. Para que as informações sejam apresentadas de forma mais útil pelos gráficos, é feito um cálculo que apresenta resultados em percentuais. Foram selecionadas algumas variáveis importantes para o cálculo dos valores que serão apresentados pelos gráficos. Através destes gráficos será possível analisar os valores obtidos com a CISCO-CLASS-BASED-QOS-MIB e CISCO-CAR-MIB.

3.5.1 Gráficos da CISCO-CLASS-BASED-QOS-MIB

Para as classes foram definidos três gráficos, os quais apresentam o percentual de bytes que entram e saem pela classe, percentual de bytes descartados pela classe e percentual de bytes que estão de acordo com determinados padrões de comparação da classe.

3.5.1.1 Gráfico de bytes que entram e saem pela classe

No gráfico de bytes que entram e saem pela classe, o cálculo é feito utilizando duas variáveis que apresentam o total de bytes que entram pela classe e o total de bytes que saem pela classe que são **CbQosCMPrePolicyByte** e **CbQosCMPostPolicyByte**, respectivamente. O cálculo é feito da seguinte forma:

- **Resultado1 = percentual de bytes que entram na classe, ou seja, 100 %, pois é todo o tráfego que entra na classe.**
- **Resultado2 = (CbQosCMPostPolicyByte * 100)/ CbQosCMPrePolicyByte**

A variável **Resultado1** possuirá o percentual de bytes que entram na classe. A variável **Resultado2** possuirá o percentual de bytes que saem pela classe. Então, as informações do gráfico das classes terão duas variáveis que são **Resultado1** e **Resultado2,** as quais irão apresentar o percentual de bytes que entram e saem da classe, respectivamente. Estes gráficos possuirão um histórico no qual será possível realizar um acompanhamento diário, semanal, mensal e anual.

3.5.1.2 Gráfico de bytes descartados pela classe

No gráfico de bytes descartados pela classe, também devem ser encontrados dois valores. O cálculo é feito utilizando duas variáveis que apresentam o total de bytes que entram pela classe e o total de bytes descartados pela classe que são **CbQosCMPrePolicyByte** e **CbQosCMDropByte,** respectivamente. O cálculo é feito da seguinte forma:

- **Resultado1 = percentual de bytes que entram na classe, ou seja, 100 %, pois é todo o tráfego que entra na classe.**
- **Resultado2 = (CbQosCMDropByte *100)/ CbQosCMPrePolicyByte**

Da mesma forma que o gráfico de bytes que entram e saem pela classe, o gráfico que apresenta o percentual de bytes descartados pela classe utiliza as variáveis **Resultado1** e **Resultado2**.

3.5.1.3 Gráfico de bytes que entram em cada padrão de comparação da classe

Cada classe pode possuir várias formas para comparar o tráfego. Pode existir a necessidade de se colocar dentro de uma mesma classe fluxos de tráfego diferentes. Todo fluxo que entra em uma classe é comparado com os padrões que estão configurados nas classes. Na CISCO-CLASS-BASED-QOS-MIB, existem algumas variáveis que estão relacionadas a estes padrões. É importante saber o total de bytes que entra na classe e se encaixam em determinado padrão. Esta informação é obtida através da variável **CbQosMatchPrePolicyByte**.

Para a apresentação no gráfico, foi feito o cálculo de duas variáveis que são: percentual de bytes que entram na classe e percentual de bytes que se encaixam em determinado padrão. O cálculo foi feito utilizando as variáveis **CbQosCMPrePolicyByte** e **CbQosMatchPrePolicyByte** e foi feito da forma que está descrita abaixo:

- **Resultado1 = percentual de bytes que entram na classe, ou seja, 100 %, pois é todo o tráfego que entra na classe.**
- **Resultado2=** (**CbQosMatchPrePolicyByte *100) / CbQosCMPrePolicyByte**

Com estas variáveis, é possível visualizar a informação que apresenta o percentual de bytes que se encaixam em cada padrão em relação ao percentual de bytes que entram na classe.

3.5.2 Gráficos da CISCO-CAR-MIB

Para as estatísticas de classificação e moldagem do tráfego, foi definido um gráfico que apresenta o percentual de bytes que entram e o percentual de bytes que são descartados pela classe. O tráfego será classificado utilizando a classificação MF. Para este gráfico, foram utilizadas duas variáveis: **ccarStatSwitchedBytes** e **CcarStatFilteredBytes**. Através destas variáveis, é possível apresentar o percentual de bytes que entram na classe e o percentual de bytes que é descartado pela classe.

3.5.2.1 Gráfico de bytes que entram ou são descartados pela classe

No gráfico de bytes que entram ou são descartados pela classe, o cálculo é feito da seguinte forma:

- **Resultado1 =** (**ccarStatSwitchedBytes*100)/(CcarStatFilteredBytes +ccarStatSwitchedBytes)**
- **Resultado2 =** (**CcarStatFilteredBytes *100)/(CcarStatFilteredBytes +ccarStatSwitchedBytes)**

A variável **Resultado1** possuirá o percentual de bytes que entram na classe. A variável **Resultado2** possuirá o percentual de bytes que foram descartados pela classe. A informação do gráfico com as estatísticas de classificação e moldagem do tráfego terá duas variáveis que são **Resultado1** e **Resultado2,** nas quais será apresentado o percentual de bytes que entram ou são descartados pela classe.

3.6 Fatores que contribuem na análise de QOS

Na ferramenta de análise de DS é importante visualizar todas as variáveis possíveis que podem contribuir para o desempenho de QOS. Para isso, foram utilizadas outras MIBS que permitem capturar valores para auxiliar na gerência de DS.

3.6.1 CISCO-PING-MIB

Além das informações obtidas através das MIBs de DS, foi necessário utilizar a CISCO-PING-MIB. Através desta MIB, é possível obter informações sobre atraso e perdas das aplicações. Esta medição é feita através do uso de pacotes ICMP Echo Request e Echo Reply. Um detalhe importante é fazer com que estes pacotes ICMP tenham um tratamento diferenciado em relação ao tráfego comum. Para isso, foi considerado que o tráfego ICMP de uma determinada origem para determinado destino estivesse dentro da mesma classe à qual se deseja obter informação de atraso e perdas.

Para obter resultados confiáveis, é necessário fazer com que este tráfego ICMP não ultrapassasse os valores padrões de determinada classe. Para isso, foi definido que o tamanho dos pacotes ICMP injetados na rede fosse de 40 bytes, haja visto que estes pacotes trafegarão em dois sentidos para obter o resultado. Isso simula a utilização do canal de voz, possibilitando, dessa forma, calcular os valores de atraso e perdas em cima de situações reais, pois, no caso de aplicações de voz, os pacotes geralmente possuem um tamanho de 80 bytes.

As variáveis da CISCO-PING-MIB que foram utilizadas estão descritas a seguir:

- **CiscoPingAddress:** esta variável indica qual o endereço IP do equipamento a que será feito o teste de ping.

- **CiscoPingPacketCount:** esta variável indica o número de pacotes que foram enviados para o endereço de destino através do PING.
- **CiscoPingPacketSize:** esta variável indica o tamanho dos pacotes que foram enviados para o endereço de destino através do PING.
- **CiscoPingReceivedPackets:** esta variável indica o número de pacotes que foram recebidos do endereço de destino através do PING.
- **CiscoPingAvgRtt:** esta variável apresenta a média do RTT de todos os pacotes que foram enviados e recebidos.

3.6.2 RFC1213-MIB

Outro item importante na análise de QOS é visualizar a utilização dos links aos quais estão sendo aplicadas as políticas de QOS. Pois é necessário comparar a situação dos itens de QOS nos momentos em que o link estiver saturado, como também quando estiver pouco utilizado.

O gráfico gerado para apresentar informações de utilização do link foi baseado em duas variáveis que são **ifInOctets** e **ifOutOctets,** as quais são encontradas na MIB RFC1213, MIB padrão da Internet. Estas variáveis apresentarão a quantidade de Bits por segundo que entram e saem por um determinado link.

3.7 Resumo

Neste capítulo, foram analisadas e selecionadas as variáveis das MIBs que apresentarão os resultados dos experimentos. Foram definidos os gráficos que serão criados e

apresentados pela ferramenta. Para a construção dos gráficos, apresentou-se a forma como serão calculados os valores das variáveis. Através destas definições, será possível obter informações detalhadas sobre as classes que estarão configuradas no ambiente de Serviços Diferenciados. Em cada classe será possível obter informações como tempo de resposta para o tráfego, percentual de bytes que entram e saem e percentual de bytes que são descartados pela classe.

Para que as informações sejam capturadas puramente através do SNMP, concluiu-se que é necessário criar uma classe que conceda garantias para o tráfego de gerência. Pois, caso não existir esta configuração nos momentos em que a rede estiver saturada, o gerente SNMP poderá ter dificuldades nas capturas dos valores necessários. No próximo capítulo, será apresentado o software de gerenciamento de redes IP com Serviços Diferenciados utilizando SNMP.

4 FERRAMENTA PARA O GERENCIAMENTO DE DIFFSERV UTILIZANDO SNMP

4.1 Apresentação da ferramenta

Esta ferramenta foi desenvolvida com o objetivo de permitir e facilitar a monitoração de um ambiente de Serviços Diferenciados. Desta forma evitando que o gerente tenha que navegar nas MIBs para obter algum resultado. Para desenvolver esta ferramenta, foram utilizadas todas as definições descritas no capítulo três.

Também para desenvolver esta ferramenta foi necessário utilizar alguns softwares. Como é importante que a aplicação seja acessada de qualquer lugar, o software foi desenvolvido para que permitisse o acesso através do browser.

Neste caso foi utilizado o PHP como ferramenta para o desenvolvimento desta aplicação web. No PHP, existem as funções básicas do SNMP e através delas é possível capturar valores das variáveis das MIBs.

As informações das configurações e estatísticas de QOS são capturadas e apresentadas em tempo real. Nos casos onde foi necessário armazenar valores, foi utilizado o banco de dados MYSQL. Neste banco de dados serão armazenadas variáveis como endereço IP do roteador e as comunidades de leitura e escrita.

Para apresentar os gráficos com as estatísticas de QOS, o software de gerenciamento de QOS utiliza o MRTG [26]. Esta ferramenta permite que sejam informados os parâmetros desejados e através deles os gráficos são gerados. As informações são divididas em gráficos que apresentam as estatísticas diárias, semanais, mensais e anuais, possibilitando um acompanhamento efetivo.

O sistema operacional utilizado no servidor onde estão instalados e configurados o PHP e o MYSQL foi o Conectiva Linux 7.0. Todas as ferramentas utilizadas não possuem custos e estão disponíveis através do sistema de licenciamento GPL.

4.2 Modo de operação da ferramenta

Para utilizar o software, o administrador da rede precisa utilizar um browser. Depois deverá visualizar a página que permite fazer o gerenciamento do ambiente de QOS. Na página inicial, serão apresentadas informações sobre o ambiente de gerenciamento de QOS utilizando a estrutura DIFFSERV.

Para iniciar o processo de gerência do ambiente de QOS, o usuário precisa informar o endereço IP do roteador no qual deseja fazer gerenciamento. Para isso deve inserir um roteador na lista de roteadores gerenciados. Para inserir o roteador, o usuário deve informar o endereço IP bem como o nome das comunidades SNMP de leitura e escrita. Através dessas informações, é possível acessar o roteador e capturar os valores necessários.

Após inserir o roteador, o usuário poderá visualizar o mesmo na lista de roteadores cadastrados. Ao clicar sobre a IP do roteador, serão apresentadas suas informações básicas. Todas as informações são capturadas em tempo real através do SNMP.

Na tela inicial do sistema são apresentadas informações como endereço IP do roteador, e-mail do responsável, localização física e tempo em que o roteador está ativo. Logo após esta tela são apresentadas informações sobre as interfaces de rede. Em cada interface serão apresentados seu nome, descrição, velocidade, status operacional, endereço IP e máscara. O status da interface também poderá ser detectado visualmente. No caso da interface estar com status operacional como DOWN, as informações serão apresentadas com a cor de fundo vermelha. Para o caso da interface estar com o status operacional como UP, a cor de fundo a

que aparecerá será verde. A figura 4.2.1 apresenta a tela inicial do sistema com dois roteadores cadastrados.

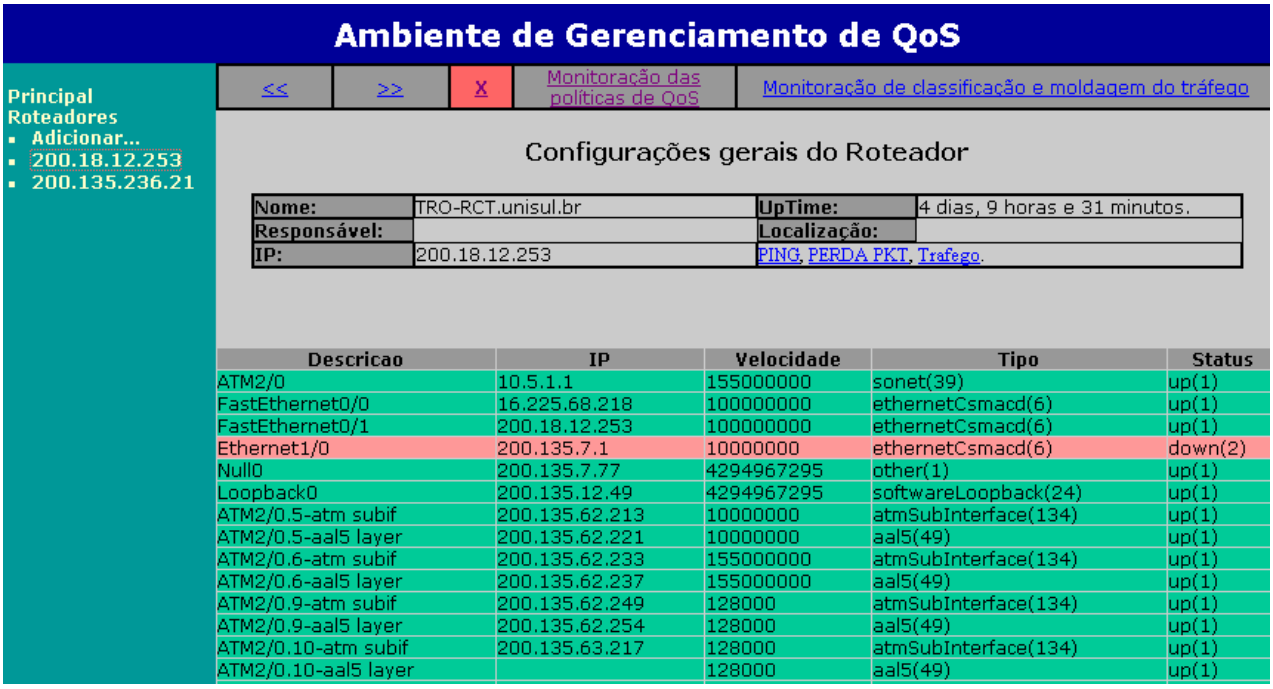


Figura 4.2.1 – Tela inicial do sistema

Após aparecer estas informações, serão apresentados dois links que darão acesso às informações relacionadas às políticas e classes configuradas e também às informações de classificação e moldagem do tráfego.

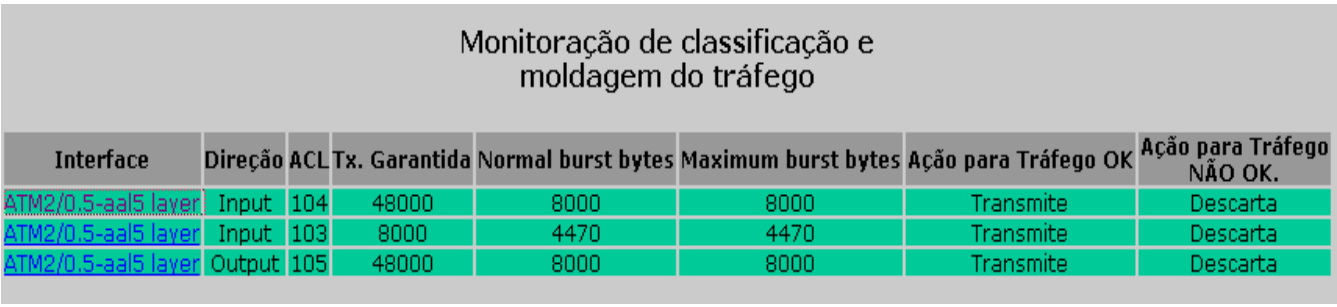
Através do link de “políticas e classes de QOS”, é possível visualizar todas as políticas de QOS configuradas. A figura 4.2.2 apresenta esta característica.

Figura 4.2.2 – Política de classes de QOS

Nas informações de políticas são apresentados o nome, descrição e direção da política. Dentro de cada política ainda são apresentadas as classes com seus valores como nome, descrição, largura de banda alocada e algoritmo de enfileiramento utilizado. Nas informações estatísticas das classes é apresentado o total de bytes que entraram e total de bytes que foram transmitidos através da classe. Outra informação apresentada é o total de bytes que foram descartados pela classe.

Em cada classe são apresentados os padrões de comparação que identificam os fluxos através das suas características. Em cada padrão de comparação é apresentado o total de bytes que se encontram dentro das características configuradas.

No link “Configuração e moldagem de tráfego”, aparecerão informações relacionadas às configurações de classificação e moldagem do tráfego. Serão apresentadas a identificação de cada interface a que está configurada a característica de classificação e moldagem do tráfego, bem como outras informações importantes, como taxa de bits por segundo que é assegurada pela configuração, entre outras informações. A figura 4.2.3 apresenta essa característica.



Monitoração de classificação e moldagem do tráfego

Interface	Direção	ACL	Tx. Garantida	Normal burst bytes	Maximum burst bytes	Ação para Tráfego OK	Ação para Tráfego NÃO OK.
ATM2/0.5-aal5 layer	Input	104	48000	8000	8000	Transmite	Descarta
ATM2/0.5-aal5 layer	Input	103	8000	4470	4470	Transmite	Descarta
ATM2/0.5-aal5 layer	Output	105	48000	8000	8000	Transmite	Descarta

Figura 4.2.3 – Classificação e moldagem do tráfego

Na primeira vez em que o usuário acessa as informações de QOS, na parte superior será apresentado um link “Ativar estatísticas”. Quando o usuário acessar esta opção, será iniciada a criação dos gráficos que apresentarão as estatísticas das classes. Para gerar estatísticas de tempo de resposta e perdas da classe, será solicitado que o usuário informe o IP de origem, IP de destino e o número da ACL que pertence à classe à qual se deseja fazer a medição. O IP de origem deve ser o endereço IP da interface na qual está aplicada a política de QOS que possui a classe a ser medida. O endereço IP de destino é o endereço IP do equipamento de destino no qual se deseja fazer a medição do tempo de resposta e perdas da classe.

Para visualizar os gráficos com as estatísticas, o usuário deve acessar os links que estarão relacionados com os valores capturados em tempo real. Ao clicar sobre as variáveis capturadas através do SNMP, será apresentado na tela o gráfico relacionado à variável selecionada. Todos os gráficos que serão gerados através desta ferramenta estão definidos no capítulo três. A figura 4.2.4 apresenta o gráfico que será visualizado através destes links.

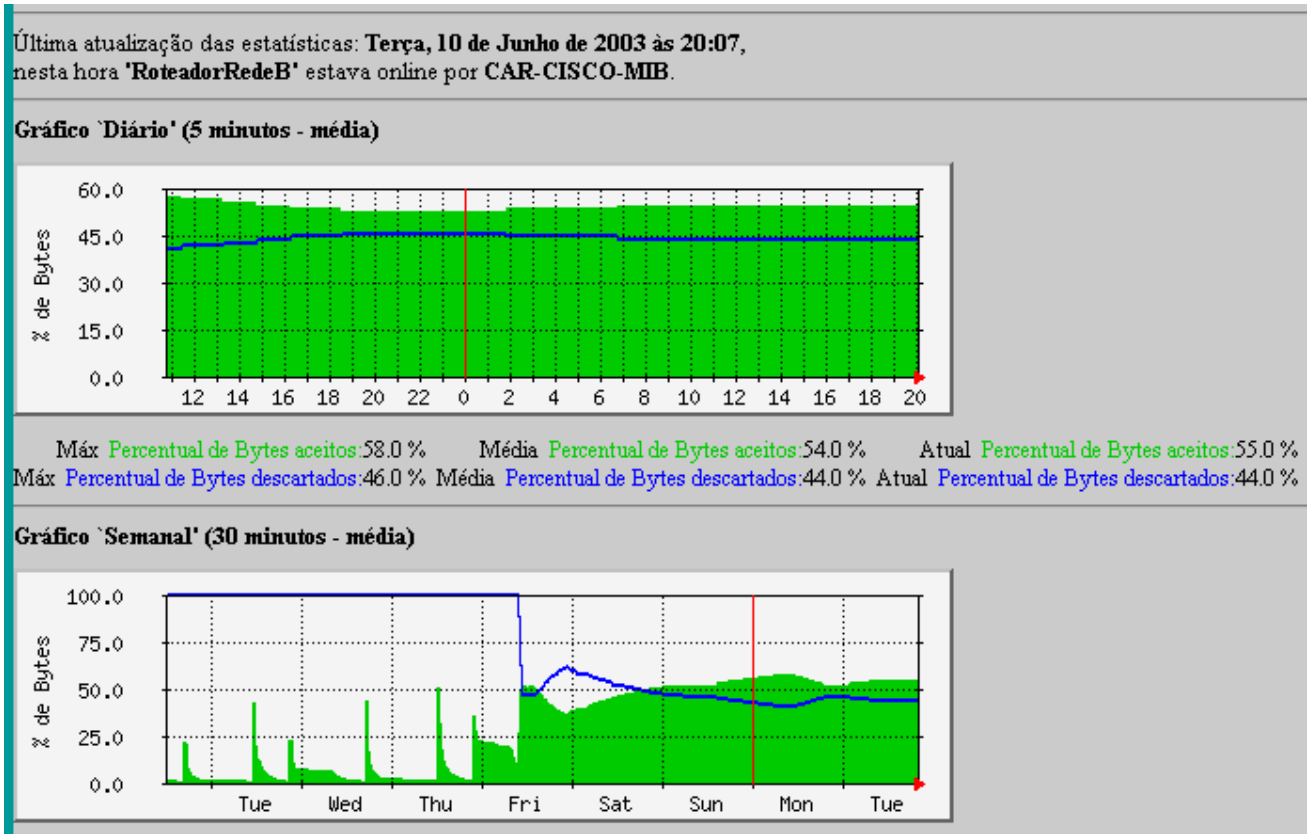


Figura 4.2.4 – Gráfico de percentual de bytes aceitos e descartados pela classe

Sempre que o usuário desejar visualizar qualquer informação do roteador, primeiramente deve selecionar o mesmo na lista de roteadores cadastrados.

4.3 Ambiente para validação da ferramenta

Para validar a ferramenta, é necessário criar um ambiente que possibilite obter valores das MIBs de DiffServ. O objetivo principal deste ambiente será avaliar a funcionalidade da ferramenta desenvolvida para o gerenciamento de QOS. Também será analisado se através da ferramenta é possível verificar o comportamento do tráfego EF em relação ao tráfego de melhor esforço.

Foi configurando um ambiente (Figura 4.3.1) com duas redes locais (LAN1 e LAN2), as quais possuem o endereço IP 192.168.201.0/24 e 192.168.200.0/24, respectivamente. Elas estão interligadas através de uma rede WAN que possui três roteadores Cisco 2500 Series interligados utilizando um canal PPP de 64 Kbps. Na rede LAN1 existe uma estação (EST_LAN1) que gera o tráfego EF que será priorizado. Além do tráfego EF, esta estação gera tráfego do tipo BE para saturar o canal. Todo esse tráfego é gerado com direção a (EST_LAN2). A EST_LAN2 é a estação que está conectada na LAN2. Da mesma forma que a EST_LAN1 gera o tráfego do tipo EF e BE, esta estação estará gerando tráfego em direção a EST_LAN1. Estas estações estarão gerando tráfego entre si para simular uma situação real de um canal com tráfego nos dois sentidos. Esse tráfego é gerado utilizando o protocolo UDP.

Na rede WAN existem três roteadores. Neles estarão configuradas as características funcionais do Diffserv. Nos roteadores ROUTER_LAN1 e ROUTER_LAN2 estarão sendo aplicadas características de classificação do tipo MF, marcação e moldagem para o tráfego que chega no domínio DS. No ROUTER_CORE estarão sendo aplicadas as políticas definidas para as classes que serão identificadas através da marcação (DSCP) que será definida pelos roteadores que estão nas extremidades do domínio DS.

Nos experimentos estará sendo avaliado se através da ferramenta é possível verificar o comportamento das aplicações críticas que trafegam na internet como voz. Serão criadas classes de serviços EF (Expedited Forwarding).

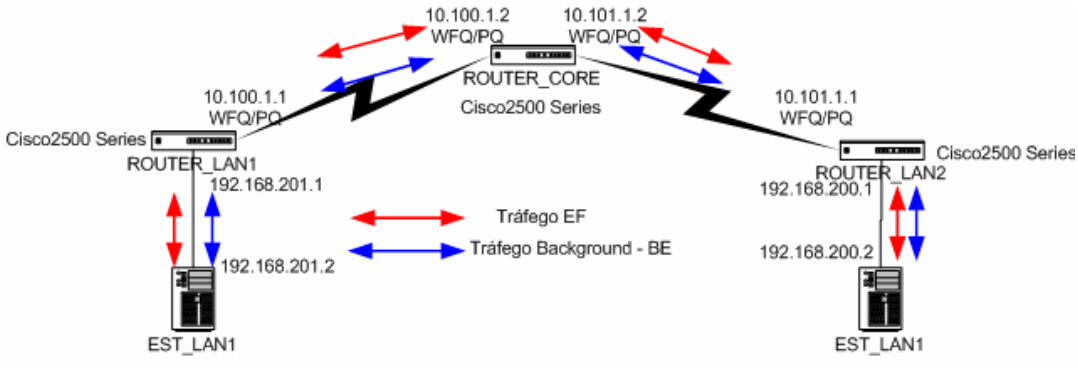


Figura 4.3.1 – Ambiente DS com roteadores CISCO e conexões PPP

4.4 Descrição dos Experimentos

O objetivo dos experimentos foi avaliar o comportamento da ferramenta com a rede em diversas situações. É necessário analisar se através da ferramenta é possível obter informações relacionadas às configurações e estatísticas das classes e políticas de QOS aplicadas ao tráfego EF e também analisar informações relacionadas a tempo de resposta, perdas do tráfego EF e utilização da rede.

Para obter informações de RTT e perdas, foram injetados na rede pacotes ICMP Echo Request e Echo Reply através da aplicação PING. Estes pacotes buscam simular pacotes de voz. Por esse motivo, foram definidos os tamanhos de 40 bytes, haja visto que os pacotes partem para o destino e voltam para a origem com o mesmo tamanho. Para obter as

informações de RTT e perdas foram inseridos em cada experimento 20 pacotes com o tamanho de 40 bytes a cada cinco minutos.

Os experimentos foram definidos sob dois pontos básicos. Na primeira fase foram executados experimentos usando como ponto de gerência o roteador interno do domínio DS. Na segunda fase foram executados os experimentos usando como ponto de gerência roteadores que estão nas extremidades do domínio DS.

4.4.1 Experimentos com roteador interno do Domínio DS

Através desses experimentos é possível fazer a análise da utilização da rede, tempo de resposta, perdas e análise das variáveis das MIBS de QOS da CISCO definidas nas seções 3.3.2 e 3.4.2. Serão realizados seis experimentos, com objetivos de simular todas as situações possíveis em que a rede com e sem QOS habilitado pode se encontrar.

Para gerar o tráfego foi utilizado o mgen [24]. Esta ferramenta permite gerar tráfego utilizando o protocolo UDP. O mgen permite que seja definido o endereço IP de destino, porta UDP de destino, tempo que o tráfego será gerado. As informações de endereço IP e portas UDP que foram utilizadas estão apresentadas na descrição dos experimentos.

4.4.1.1 Rede sem DS habilitado

Foram realizados dois experimentos sem QOS habilitado. O objetivo destes experimentos foi visualizar os resultados dos gráficos de utilização da rede, tempo de resposta e perdas do tráfego do tipo BE. Através desses gráficos é possível analisar o comportamento

destas variáveis em uma rede sem QOS. As variáveis utilizadas nos dois experimentos são as mesmas, o que diferencia é a forma como é gerado o tráfego.

4.4.1.1.1 Rede com tráfego normal

Para analisar a rede sem QOS e com tráfego normal, foi gerado o tráfego criando três fluxos de pacotes com tamanho de (1024 + cabeçalho UDP). Estes fluxos geram um tráfego de 24.8Kbps. A tabela 4.4.1.1.1 apresenta as características da geração desse fluxo. Os fluxos são gerados a partir da EST_LAN1 com destino à EST_LAN2. Esta medição será executada para comparar quando o DS estiver habilitado.

IP Origem	IP Destino	Porta Origem	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote
192.168.201.2/32	192.168.200.2/32	5600	5000	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5601	5001	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5602	5002	UDP	28 Bytes	1024 Bytes

Tabela 4.4.1.1.1 – Geração de tráfego normal para a rede sem QOS.

4.4.1.1.2 Rede com tráfego saturando o canal

Para analisar a rede sem QOS e com tráfego saturando o canal, foi gerado o tráfego criando dez fluxos de pacotes com tamanho de (1024 + cabeçalho UDP). Estes fluxos geram um tráfego de 84Kbps. A tabela 4.4.1.1.2 apresenta as características da geração desse fluxo.

IP Origem	IP Destino	Porta Origem	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote
192.168.201.2/32	192.168.200.2/32	5600	5000	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5601	5001	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5602	5002	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5603	5003	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5604	5004	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5605	5005	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5606	5006	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5607	5007	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5608	5008	UDP	28 Bytes	1024 Bytes
192.168.201.2/32	192.168.200.2/32	5609	5009	UDP	28 Bytes	1024 Bytes

Tabela 4.4.1.1.2 – Geração de tráfego saturando o canal para rede sem QOS

4.4.1.2 Rede com DS habilitado

Foram executados quatro experimentos com QOS habilitado na rede. Todos utilizam as mesmas variáveis de medição. O que os diferencia é a quantidade de fluxo gerado e as configurações de garantia de largura de banda para a classe. Através destes experimentos serão analisados o comportamento das variáveis de tempo de resposta, perdas e utilização da rede. Serão também analisadas as variáveis da MIB de QOS da cisco (CISCO-CLASS-BASE-QOS-MIB) definidas na seção 3.3.2 e 3.4.2. As variáveis desta MIB que serão analisadas nestes experimentos são: percentual de bytes que entram e saem pela classe, percentual de bytes descartados pela classe.

4.4.1.2.1 Rede com tráfego normal

O objetivo desse experimento é analisar a rede e as estatísticas de QOS com o tráfego da rede em situação ideal, ou seja, tráfego da classe dentro do acordo e a rede sem tráfego saturando o canal. Para executar este experimento, foram criadas duas classes. A classe chamada VOIP do tipo (EF), que possui 48Kbps de largura de banda reservada para utilizar o canal de 64Kbps, e a classe DEFAULT, que possui o restante da largura de banda, mas sem prioridade.

Na geração de tráfego para esse experimento foram definidos cinco grupos com quatro fluxos que pertencem à classe VOIP e um grupo com um fluxo que pertence à classe DEFAULT. Cada grupo da classe VOIP envia quatro fluxos com um pacote de (52 bytes + cabeçalho) por segundo cada um, simulando um canal de voz. Também é gerado um fluxo para a classe DEFAULT que envia um pacote de (1472 bytes + cabeçalho) por segundo.

A tabela 4.4.1.2.1 apresenta a característica do fluxo do tráfego gerado para executar este experimento.

IP Origem	IP Destino	N.º Fluxos	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote	Classe
192.168.201.2/32	192.168.200.2/32	1	5000	UDP	28 Bytes	1472 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	4	5012	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5013	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5014	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5015	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5016	UDP	28 Bytes	52 Bytes	VOIP

Tabela 4.4.1.2.1 – Geração de tráfego normal para a rede com QOS habilitado

4.4.1.2.2 Rede com tráfego em background saturando o canal

O objetivo desse experimento é verificar se a utilização de QOS está sendo efetiva para as classes configuradas, sendo que o tráfego da classe está dentro do acordo e o tráfego restante que está sendo gerado está saturando o canal. Para executar este experimento, também foram criadas duas classes. A classe VOIP, que possui 48Kbps de largura de banda reservada para utilizar o canal, e a classe DEFAULT, que possui o restante da largura de banda, mas sem prioridade.

Na geração de tráfego para esse experimento foram definidos cinco grupos com quatro fluxos que pertencem à classe VOIP e um grupo com cinco fluxos que pertencem à classe DEFAULT. Cada grupo da classe VOIP envia quatro fluxos com um pacote de (52 bytes + cabeçalho) por segundo cada um, simulando um canal de voz. Cada fluxo gerado para a classe DEFAULT envia um pacote de (1472 bytes + cabeçalho) por segundo.

A tabela 4.4.1.2.2 apresenta a característica do fluxo do tráfego gerado para executar este experimento.

IP Origem	IP Destino	Nº Fluxos	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote	Classe
192.168.201.2/32	192.168.200.2/32	5	5000	UDP	28 Bytes	1472 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	4	5012	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5013	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5014	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5015	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	4	5016	UDP	28 Bytes	52 Bytes	VOIP

Tabela 4.4.1.2.2 – Geração de tráfego saturando o canal para a rede com QOS habilitado

4.4.1.2.3 Rede com tráfego normal e com o tráfego da classe acima do acordo

O objetivo desse experimento é fazer uma simulação em que o tráfego geral da rede esteja dentro da capacidade total do canal, mas que o tráfego da classe esteja acima do que está no acordo. Para executar este experimento, foram criadas duas classes. A classe VOIP, que possui 20Kbps de largura de banda reservada para utilizar o canal, e a classe DEFAULT, que possui o restante da largura de banda, mas sem prioridade.

Na geração de tráfego para esse experimento foram definidos cinco grupos com oito fluxos que pertencem à classe VOIP e um grupo com quatro fluxos que pertencem à classe DEFAULT. Cada grupo da classe VOIP envia oito fluxos com um pacote de (52 bytes + cabeçalho) por segundo cada um, simulando dois canais de voz. Também são gerados quatro fluxos para a classe DEFAULT que envia um pacote de (52 bytes + cabeçalho) por segundo cada um.

A tabela 4.4.1.2.3 apresenta a característica do fluxo do tráfego gerado para executar este experimento.

IP Origem	IP Destino	Nº Fluxos	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote	Classe
192.168.201.2/32	192.168.200.2/32	5	5000	UDP	28 Bytes	52 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	8	5012	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5013	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5014	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5015	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5016	UDP	28 Bytes	52 Bytes	VOIP

Tabela 4.4.1.2.3 – Geração de tráfego acima do acordo da classe e o tráfego geral da rede é normal

4.4.1.2.4 Rede com tráfego saturando o canal e com o tráfego da classe acima do acordo

O objetivo desse experimento é analisar o comportamento do tráfego da classe quando a rede está saturada e a quantidade de fluxo entrante na classe está acima do previsto no acordo. Para executar este experimento também foram criadas duas classes. A classe VOIP, que possui 20Kbps de largura de banda reservada para utilizar o canal, e a classe DEFAULT, que possui o restante da largura de banda, mas sem prioridade.

Na geração de tráfego para esse experimento foram definidos cinco grupos com oito fluxos que pertencem à classe VOIP e um grupo com quatro fluxos que pertencem à classe DEFAULT. Cada grupo da classe VOIP envia oito fluxos com um pacote de (52 bytes + cabeçalho) por segundo cada um. Cada fluxo gerado para a classe DEFAULT envia um pacote com (1472 bytes + cabeçalho) por segundo.

A tabela 4.4.1.2.4 apresenta o fluxo do tráfego gerado para executar este experimento.

IP Origem	IP Destino	Nº Fluxos	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote	Classe
192.168.201.2/32	192.168.200.2/32	4	5000	UDP	28 Bytes	1472 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	8	5012	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5013	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5014	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5015	UDP	28 Bytes	52 Bytes	VOIP
192.168.201.2/32	192.168.200.2/32	8	5016	UDP	28 Bytes	52 Bytes	VOIP

Tabela 4.4.1.2.4 - Geração de tráfego acima do acordo da classe e o tráfego BE saturando o canal

4.4.2 Experimento com roteadores da extremidade do Domínio DS

Em um roteador que está na extremidade de um domínio DS é necessário visualizar se a configuração de classificação e moldagem do tráfego está correta. Para isso, é necessário visualizar as estatísticas de classificação e moldagem. Foram realizados dois experimentos com o objetivo de apresentar através de gráficos o percentual de bytes que chegam no domínio DS e são transmitidos para dentro do domínio DS e o percentual de bytes que chegam no domínio DS e são descartados. O que muda é a quantidade de tráfego que é gerado para entrar no domínio DS.

4.4.2.1 Rede com tráfego normal e com tráfego da classe dentro dos limites

O objetivo desse experimento é fazer uma simulação em que um roteador de extremidade de um domínio DS esteja entrando em um tráfego que não esteja saturando o

canal e também que esteja dentro do acordo das classes. Com essa simulação, é possível analisar o comportamento dos métodos de classificação e moldagem do tráfego. Neste experimento foram configuradas três classes. A classe REDE1, REDE2 e DEFAULT. Para a classe REDE1 foram gerados cinco fluxos com pacotes UDP de (512 bytes + cabeçalho) por segundo cada um. A taxa garantida para esta classe é de 24Kbps. Para a classe REDE2 foram gerados cinco fluxos com pacotes UDP de (256 bytes + cabeçalho). A taxa garantida para esta classe é 20Kbps. Para a classe DEFAULT foram gerados cinco fluxos com pacotes UDP de (52 bytes + cabeçalho). A tabela 4.4.2.1 apresenta a característica dos fluxos.

IP Origem	**IP Destino**	**Nº Fluxos**	**Porta Destino**	**Protocolo**	**Tamanho Cabeçalho**	**Tamanho Pacote**	**Classe**
192.168.201.2/32	192.168.200.2/32	5	5000	UDP	28 Bytes	52 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	5	5012	UDP	28 Bytes	512 Bytes	REDE1
192.168.201.2/32	192.168.200.2/32	5	5013	UDP	28 Bytes	256 Bytes	REDE2

Tabela 4.4.2.1 – Geração de tráfego dentro do acordo da classe e o tráfego geral da rede é normal

4.4.2.2 Rede normal e com tráfego fora dos limites da classe

O objetivo desse experimento é analisar o comportamento dos métodos de classificação e moldagem de tráfego para uma rede que esteja com a utilização do canal normal, mas a quantidade de fluxo que chega nas classes está acima do acordo. Neste experimento também foram configuradas três classes. A classe REDE1, REDE2 e DEFAULT. Para a classe REDE1 foram gerados cinco fluxos com pacotes UDP de (512 bytes + cabeçalho) por segundo. A taxa garantida para esta classe é de 8Kbps. Para a classe REDE2 foram gerados cinco fluxos com pacotes UDP de (256 bytes + cabeçalho). A taxa garantida

para esta classe é 8Kbps. Para a classe DEFAULT foram gerados cinco fluxos com pacotes UDP de (52 bytes + cabeçalho). A tabela 4.4.2.2 apresenta a característica dos fluxos.

IP Origem	IP Destino	Nº Fluxos	Porta Destino	Protocolo	Tamanho Cabeçalho	Tamanho Pacote	Classe
192.168.201.2/32	192.168.200.2/32	5	5000	UDP	28 Bytes	52 Bytes	DEFAULT
192.168.201.2/32	192.168.200.2/32	5	5012	UDP	28 Bytes	512 Bytes	REDE1
192.168.201.2/32	192.168.200.2/32	5	5013	UDP	28 Bytes	256 Bytes	REDE2

Tabela 4.4.2.2 – Geração de tráfego fora do acordo da classe e o tráfego geral da rede é normal

4.5 Conclusão do capítulo

Neste capítulo, descreveu-se a forma como foi desenvolvida a ferramenta para o monitoramento de redes IP com Serviços Diferenciados utilizando SNMP. Foram apresentados seu modo de operação e suas características. Também apresentou-se o ambiente que foi montado e os experimentos executados para fazer a validação da ferramenta. No próximo capítulo, serão apresentados os resultados obtidos através dos experimentos.

5 RESULTADOS OBTIDOS

5.1 Análise da funcionalidade da ferramenta em roteadores internos do domínio DS

Para analisar a ferramenta, os experimentos foram aplicados no roteador interno do domínio DS. A meta principal foi analisar os resultados apresentados pela ferramenta com a rede sob diferentes aspectos, com e sem QOS habilitados. Todos os resultados foram obtidos através do SNMP. Por esta razão, foram criados e apresentados em tempo real. Os gráficos foram gerados utilizando o MRTG. Para a rede sem QOS foram obtidos valores sobre vazão, atraso e perdas. Para a rede com QOS habilitado, além dos valores descritos acima, foram obtidos valores sobre percentual de bytes que entram e saem de cada classe, percentual de bytes descartados pelas classes.

5.1.1 Rede sem DS e tráfego normal

O gráfico apresentado na figura 5.1.1.1 mostra a utilização de um canal de 64Kbps com DS desabilitado e sem tráfego excedendo a capacidade do canal. Os gráficos apresentados nas figuras 5.1.1.2 e 5.1.1.3 mostram o RTT e as perdas apresentadas em uma rede nesta situação.

Nota-se através desses gráficos que mesmo a rede com DS desabilitado, se a utilização do canal estiver normal, o tempo de resposta se apresenta baixo e estável e não existem perdas.

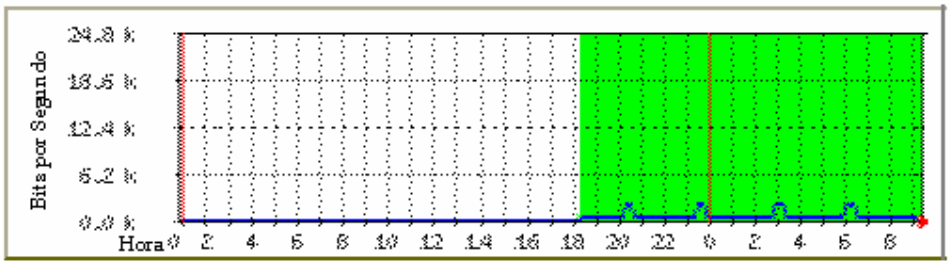


Figura 5.1.1.1 – Vazão do canal de 64Kbps

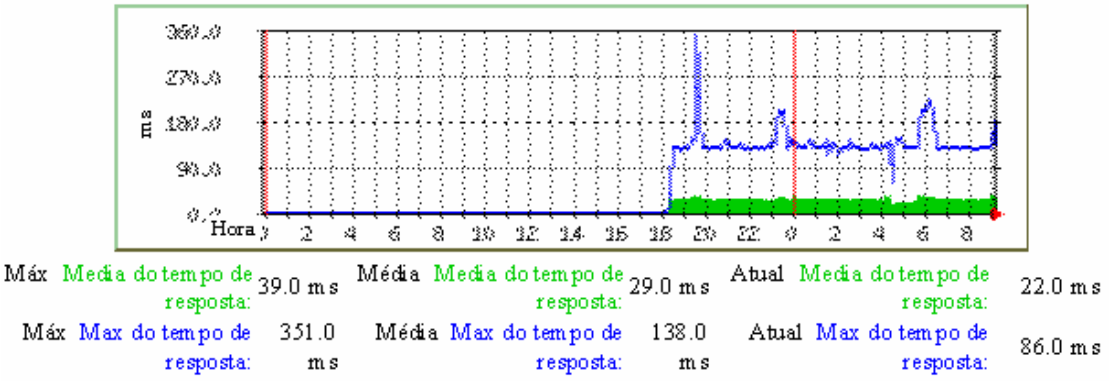


Figura 5.1.1.2 – Análise do RTT partindo do ROUTER_LAN1 para EST_LAN2

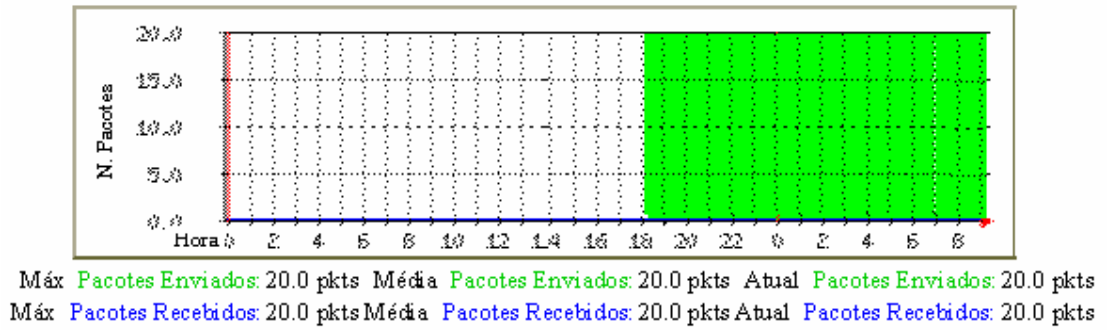


Figura 5.1.1.3 – Análise de perdas partindo do ROUTER_LAN1 para EST_LAN2

5.1.2 Rede sem DS e tráfego saturando o canal

O gráfico apresentado na figura 5.1.2.1 mostra a utilização de um canal de 64Kbps com DS desabilitado e com tráfego saturando a capacidade do canal. Os gráficos apresentados nas figuras 5.1.2.2 e 5.1.2.3 mostram o RTT e as perdas apresentadas em uma rede nesta situação.

Através destes gráficos, percebe-se claramente que quando a rede não possui DS habilitado e está congestionada é praticamente impossível obter resultados sobre tempo de resposta e perdas através do SNMP.

Nota-se que no gráfico de pacotes enviados e recebidos são enviados os vinte pacotes, e a média de pacotes recebidos é um. No gráfico de análise do RTT, não foi capturado nenhum valor para a rede nestas condições.

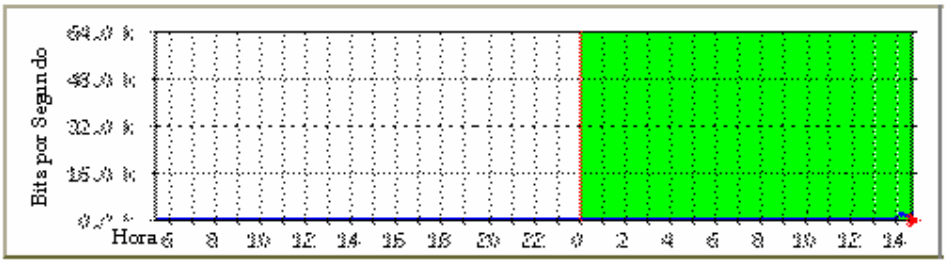


Figura 5.1.2.1 – Vazão do canal de 64Kbps

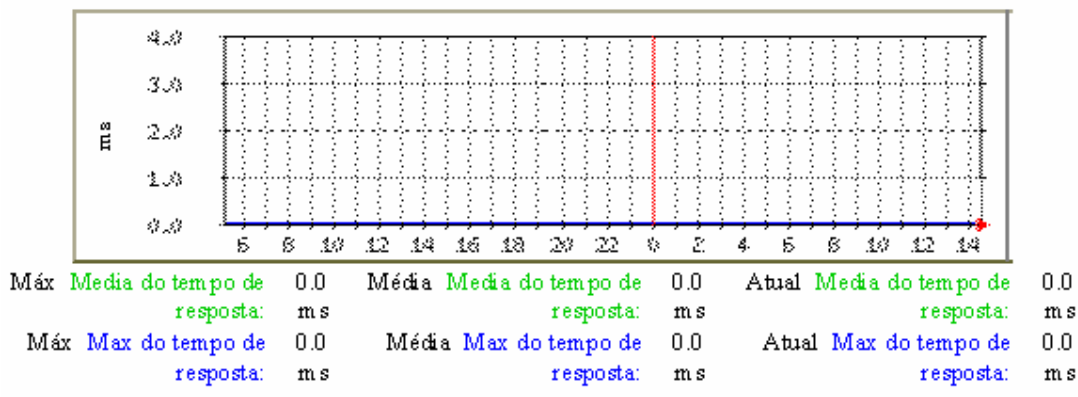


Figura 5.1.2.2 – Análise do RTT partindo do ROUTER_LAN1 para EST_LAN2

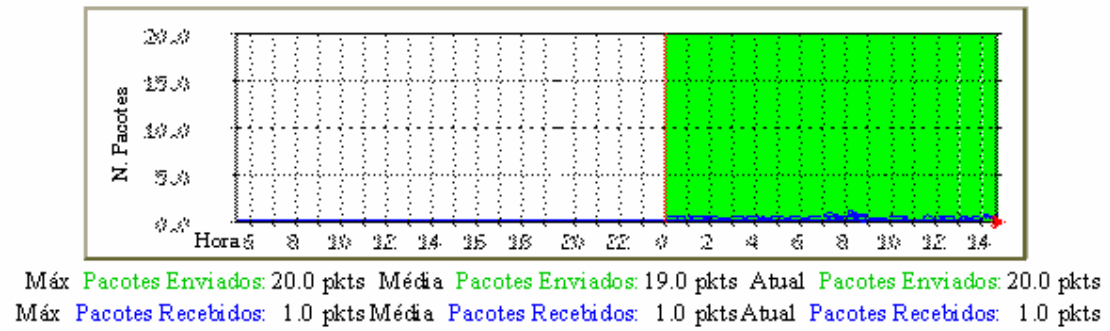


Figura 5.1.2.3 – Análise de perdas partindo do ROUTER_LAN1 para EST_LAN2

5.1.3 Rede com DS habilitado e tráfego normal

Os gráficos apresentados nas figura 5.1.3.1, figura 5.1.3.2 e figura 5.1.3.3 mostram a utilização de um canal de 64Kbps e o RTT e perdas da classe VOIP. Neste caso o DS estava habilitado e com tráfego geral da rede normal. Os gráficos apresentados nas figuras 5.1.3.4 e 5.1.3.5 mostram informações sobre percentual de bytes que entram e saem pelas classes VOIP e DEFAULT. Os gráficos 5.1.3.6 e 5.1.3.7 apresentam informações de percentual de bytes descartados pelas classes VOIP e DEFAULT.

Pode-se notar nos gráficos de tempo de resposta e perdas da classe VOIP que, quando a rede não está saturada, o tempo de resposta para a classe está baixo e constante e não existem perdas para a classe nesta situação.

Nos gráficos que são gerados utilizando as variáveis da CISCO-CLASS-BASED-QOS-MIB, pode-se notar que todo tráfego que chegou nas classes VOIP e DEFAULT foi transmitido. Não ocorreram descartes, que também podem ser visualizados através dos gráficos 5.1.3.6 e 5.1.3.7.

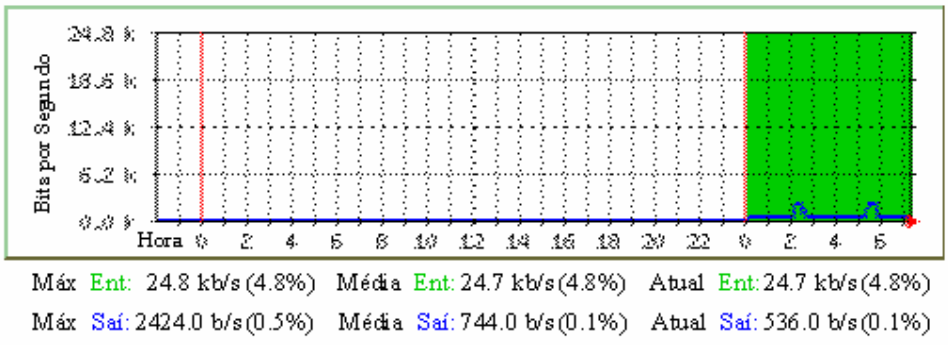


Figura 5.1.3.1 – Vazão do canal de 64Kbps

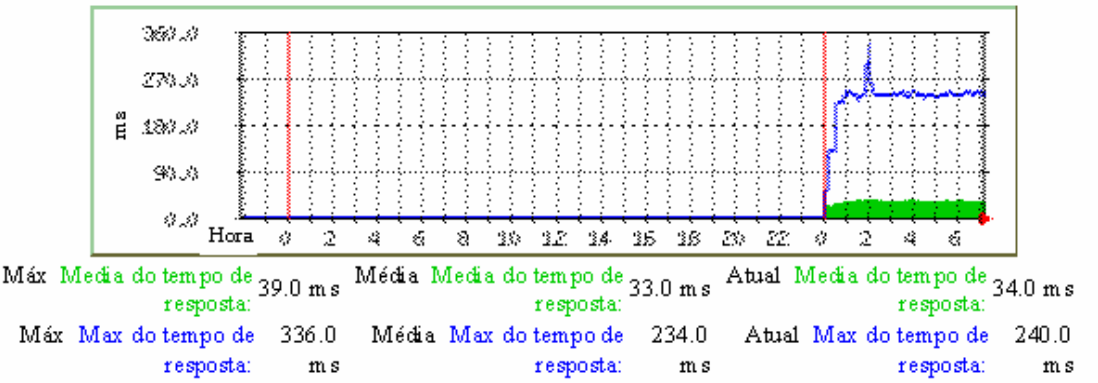


Figura 5.1.3.2 – Análise do RTT para a classe VOIP partindo do ROUTER_CORE para EST_LAN2

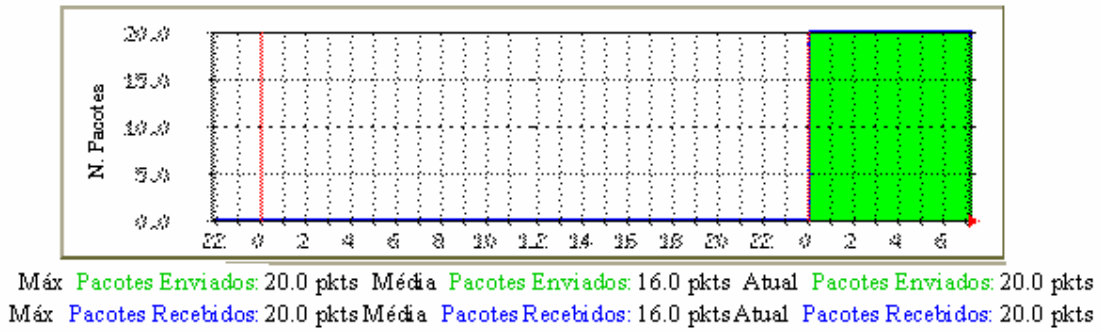


Figura 5.1.3.3 – Análise de perdas para a classe VOIP partindo do ROUTER_CORE para EST_LAN2

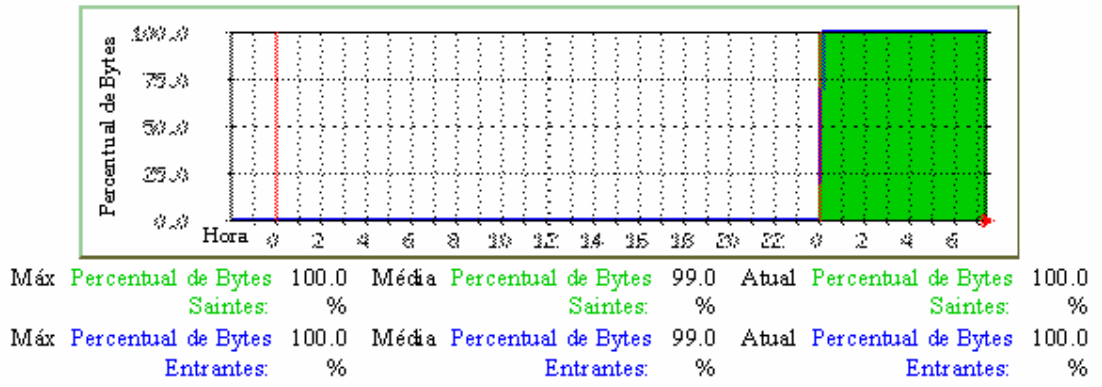


Figura 5.1.3.4 – Análise do Percentual de Bytes que entram e saem pela classe VOIP

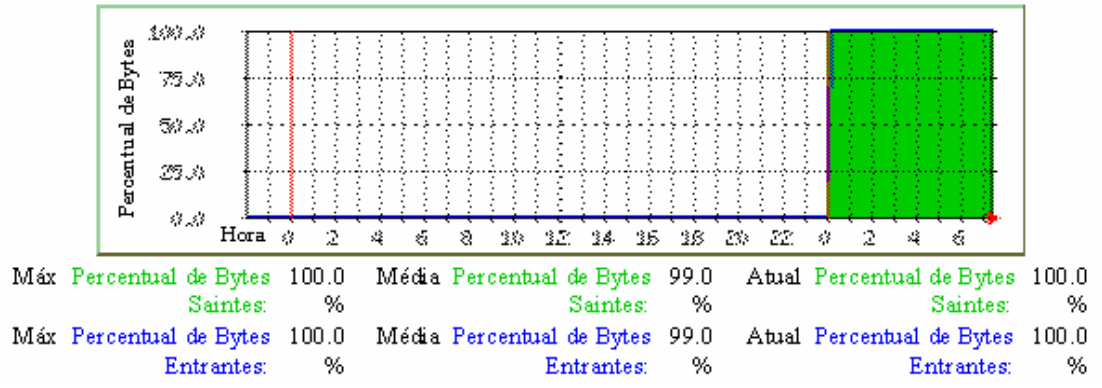


Figura 5.1.3.5 – Análise do Percentual de Bytes que entram e saem pela classe DEFAULT

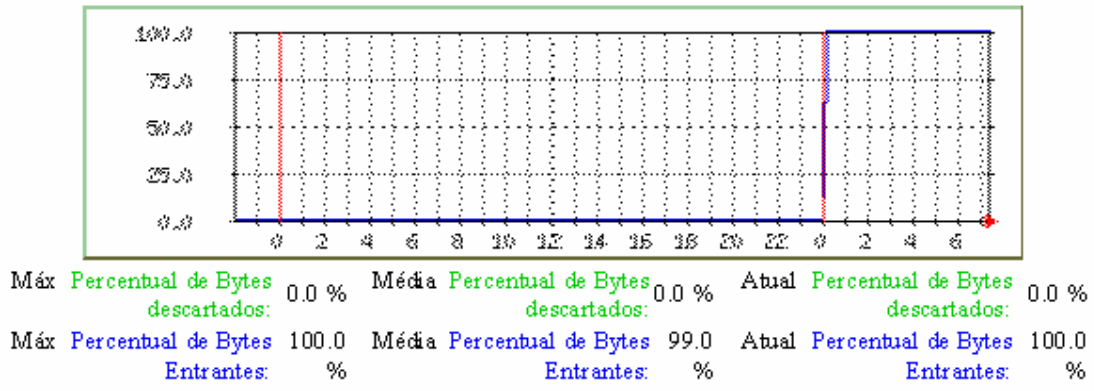


Figura 5.1.3.6 – Análise do Percentual de Bytes descartados pela classe VOIP

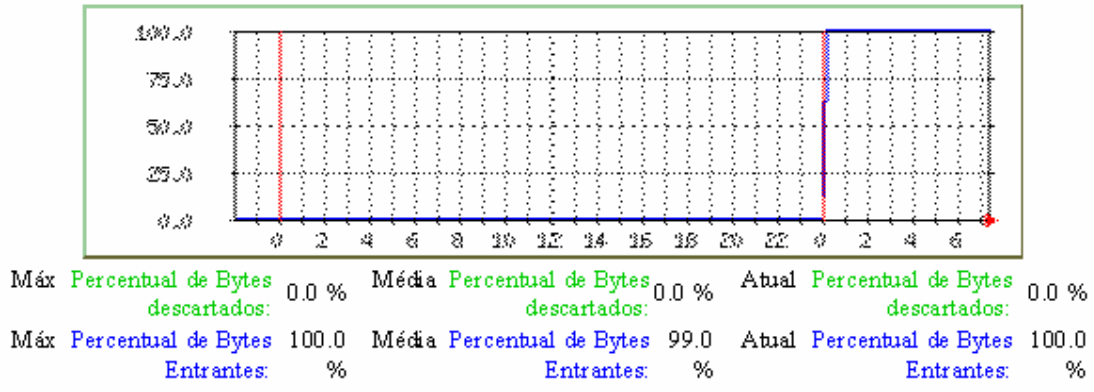


Figura 5.1.3.7 – Análise do Percentual de Bytes descartados pela classe DEFAULT

5.1.4 Rede com DS habilitado e tráfego em background saturando o canal

Os gráficos apresentados nas figura 5.1.4.1, figura 5.1.4.2 e figura 5.1.4.3 mostram a utilização de um canal de 64Kbps e o RTT e perdas da classe VOIP. Neste caso, o DS estava habilitado e com tráfego em background saturando o canal de 64Kbps. Os gráficos apresentados nas figuras 5.1.4.4 e 5.1.4.5 mostram informações sobre percentual de bytes que entram e saem pelas classes VOIP e DEFAULT. Os gráficos 5.1.4.6 e 5.1.4.7 apresentam informações de percentual de bytes descartados pelas classes VOIP e DEFAULT.

Analisando os gráficos de RTT e perdas da classe VOIP, percebe-se que mesmo com a rede saturada, o tráfego da classe é garantido, pois não existe perda de pacotes para esta classe. O tempo de resposta em relação à rede com DS habilitado e com tráfego normal aumenta, mas permanece constante e estável. No gráfico 5.1.4.4 percebe-se que todo tráfego que chega na classe VOIP é transmitido. Quanto ao tráfego que pertence à classe DEFAULT, percebe-se que não existe garantia, pois do total de bytes que chegam nesta classe, apenas 60% é transmitido. Nota-se através dos gráficos 5.1.4.6 e 5.1.4.7 que na classe VOIP não houve descartes, já na classe DEFAULT, percebe-se que 40% do tráfego que chegou na classe foi descartado pela classe. Portanto, através destas informações, percebe-se claramente se a política definida está sendo efetiva.

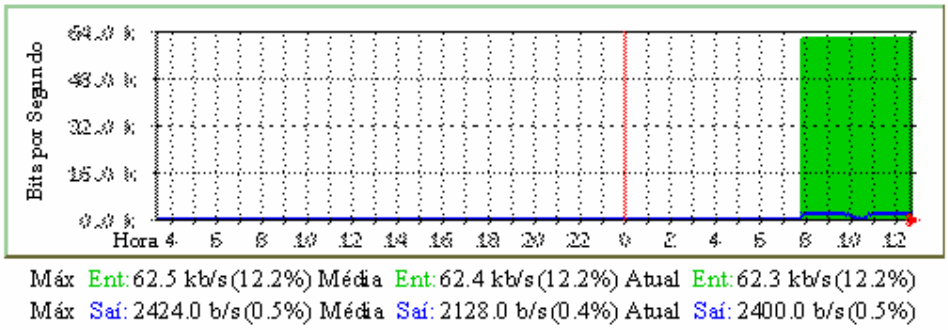


Figura 5.1.4.1 – Vazão do canal de 64Kbps

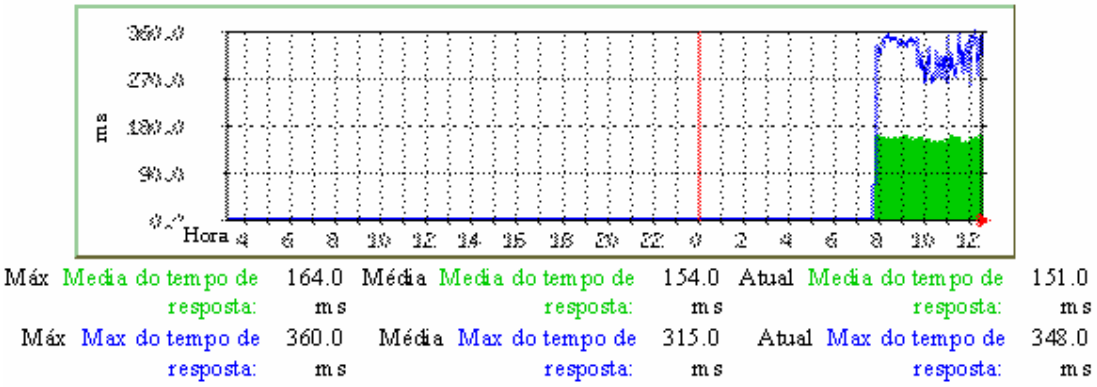
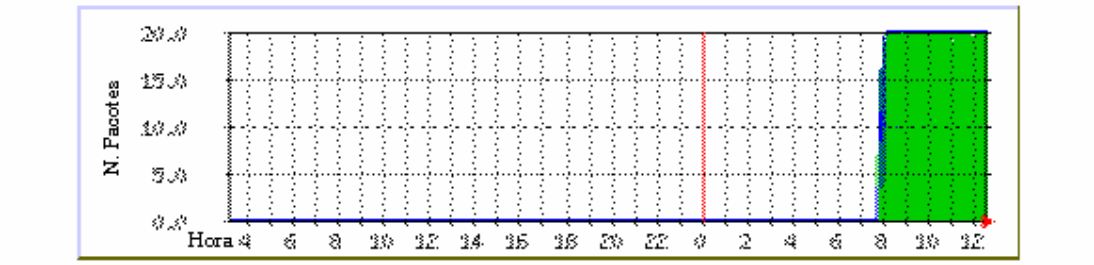
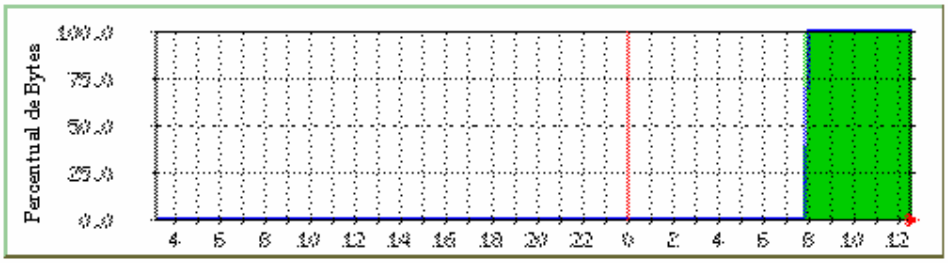


Figura 5.1.4.2 – Análise do RTT para a classe VOIP partindo do ROUTER_CORE para EST_LAN2



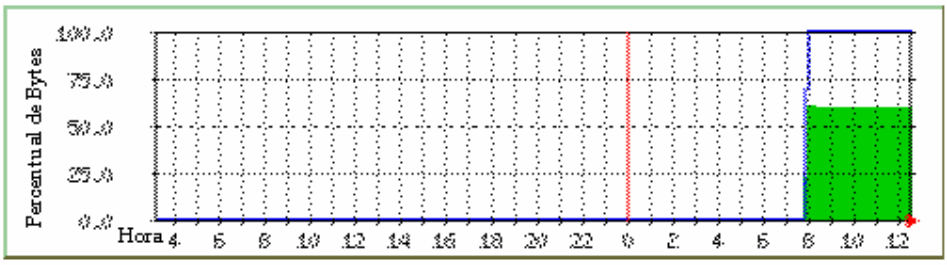
Máx Pacotes Enviados: 20.0 pkts Média Pacotes Enviados: 20.0 pkts Atual Pacotes Enviados: 20.0 pkts
Máx Pacotes Recebidos: 20.0 pkts Média Pacotes Recebidos: 20.0 pkts Atual Pacotes Recebidos: 20.0 pkts

Figura 5.1.4.3 – Análise de perdas para a classe VOIP partindo do ROUTER_CORE para EST_LAN2



Máx Percentual de Bytes Saintes: 100.0 %
Média Percentual de Bytes Saintes: 98.0 %
Atual Percentual de Bytes Saintes: 100.0 %
Máx Percentual de Bytes Entrantes: 100.0 %
Média Percentual de Bytes Entrantes: 98.0 %
Atual Percentual de Bytes Entrantes: 100.0 %

Figura 5.1.4.4 – Análise do Percentual de Bytes que entram e saem pela classe VOIP



Máx Percentual de Bytes Saintes: 61.0 %
Média Percentual de Bytes Saintes: 59.0 %
Atual Percentual de Bytes Saintes: 60.0 %
Máx Percentual de Bytes Entrantes: 100.0 %
Média Percentual de Bytes Entrantes: 98.0 %
Atual Percentual de Bytes Entrantes: 100.0 %

Figura 5.1.4.5 – Análise do Percentual de Bytes que entram e saem pela classe DEFAULT

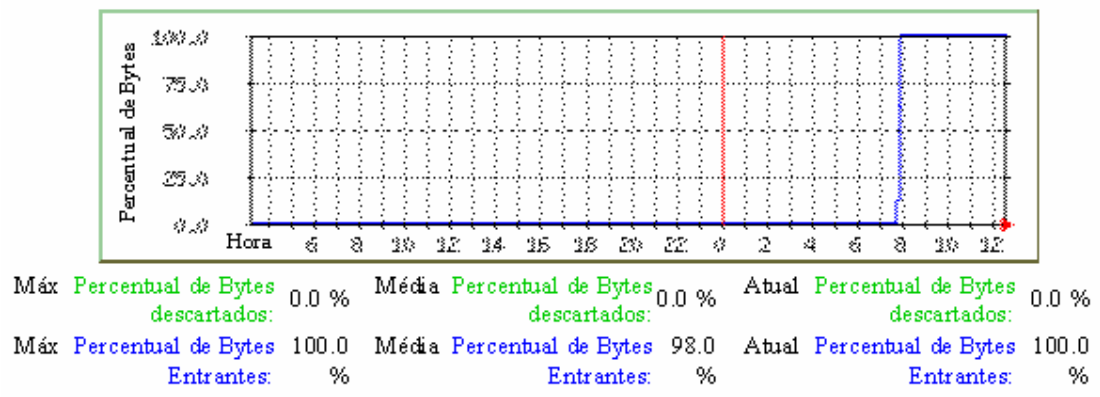


Figura 5.1.4.6 – Análise do Percentual de Bytes descartados pela classe VOIP

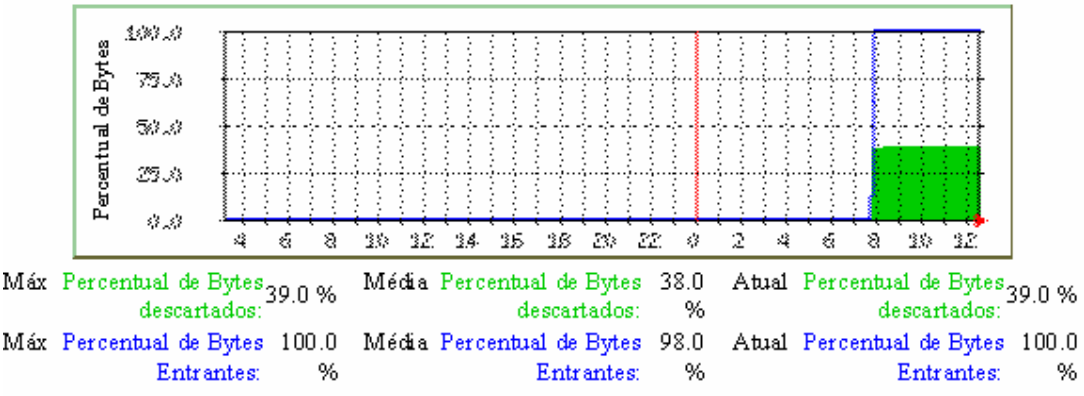


Figura 5.1.4.7 – Análise do Percentual de Bytes descartados pela classe DEFAULT

5.1.5 Rede com DS habilitado, tráfego da classe fora do acordo e a rede em situação normal

Os gráficos apresentados nas figuras 5.1.5.1 e 5.1.5.2 mostram a utilização de um canal de 64Kbps e o RTT e perdas da classe VOIP. Neste caso, o DS estava habilitado e a situação da rede estava normal. Os fluxos que estão entrando na classe VOIP estão acima do acordo. Os gráficos apresentados nas figuras 5.1.5.4 e 5.1.5.5 mostram informações sobre percentual de bytes que entram e saem pelas classes VOIP e DEFAULT. Os gráficos 5.1.5.6 e 5.1.5.7 apresentam informações de percentual de bytes descartados pelas classes VOIP e DEFAULT.

Através das informações dos gráficos, nota-se claramente que a classe VOIP está gerando mais tráfego do que é permitido. Neste caso, como as informações estão sendo capturadas em um roteador interno no domínio DS, pode-se descobrir se as configurações de classificação e moldagem do tráfego que estão sendo executadas nos nós de extremidade do domínio DS estão corretas. Também é possível descobrir se o tráfego que foi acordado através de um possível SLA está fora dos limites definidos.

Nota-se nos gráficos de RTT, mesmo com a classe gerando tráfego fora dos limites, que ela possui o tempo de resposta baixo e estável. No gráfico de perdas da classe, é possível perceber que existem perdas, pois o tráfego que excede o limite é descartado. Para os gráficos com informações relacionadas às classes, percebe-se que do percentual de bytes que chegam na classe VOIP apenas 90% é transmitido. E no gráfico de percentual de bytes descartados pela classe, é possível perceber que 10% dos pacotes que chegam na classe são transmitidos. Para a classe DEFAULT, todo tráfego que chega é transmitido. Não houve descartes para esta classe.

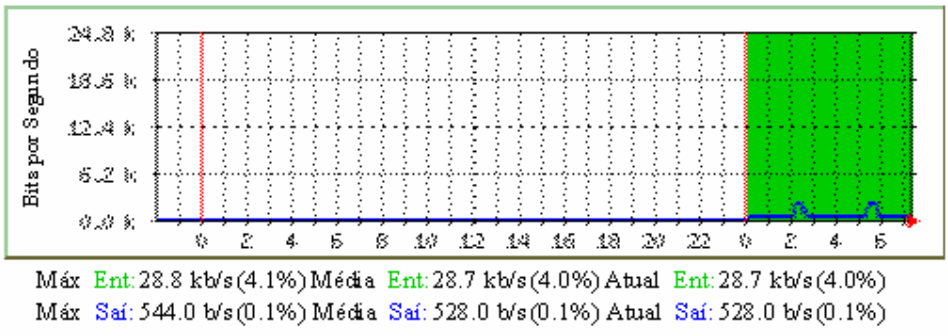


Figura 5.1.5.1 – Vazão do canal de 64Kbps

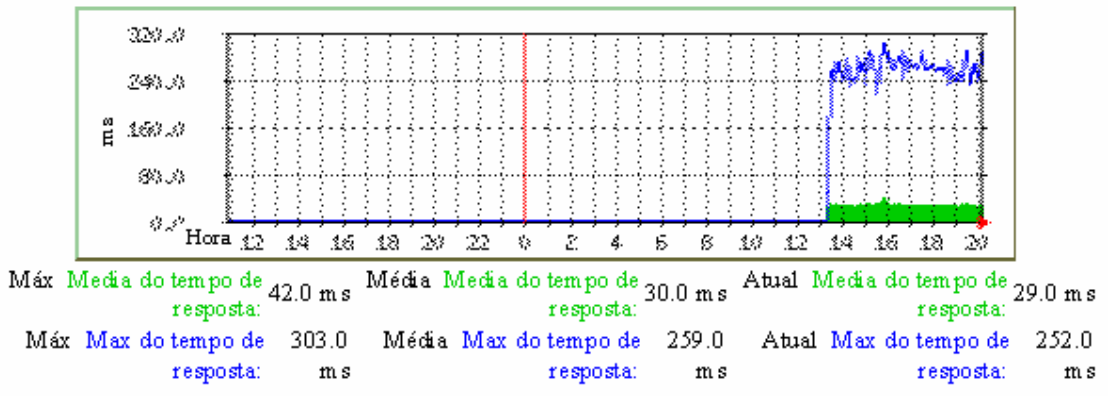


Figura 5.1.5.2 – Análise do RTT para a classe VOIP partindo do ROUTER_CORE para EST_LAN2

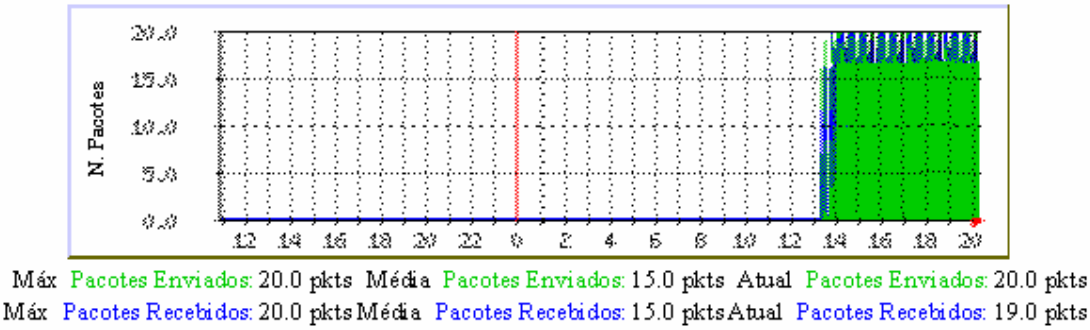


Figura 5.1.5.3 – Análise de perdas para a classe VOIP partindo do ROUTER_CORE para EST_LAN2

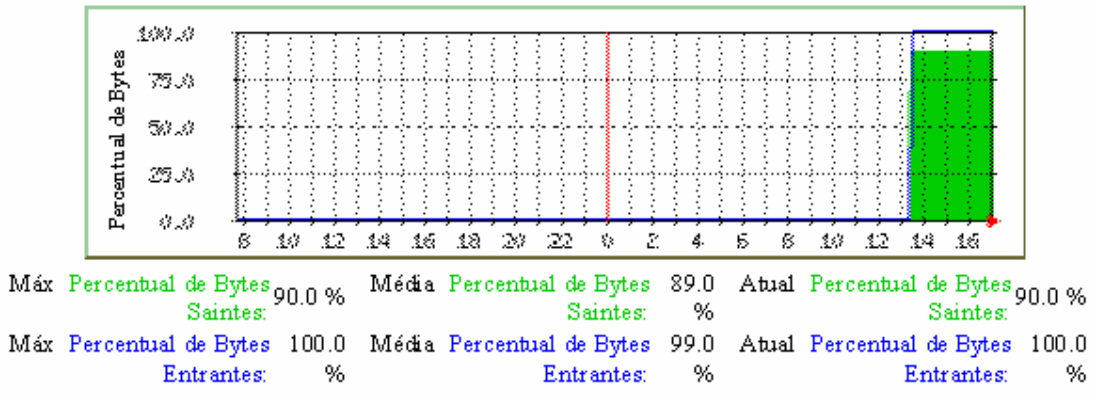


Figura 5.1.5.4 – Análise do Percentual de Bytes que entram e saem pela classe VOIP

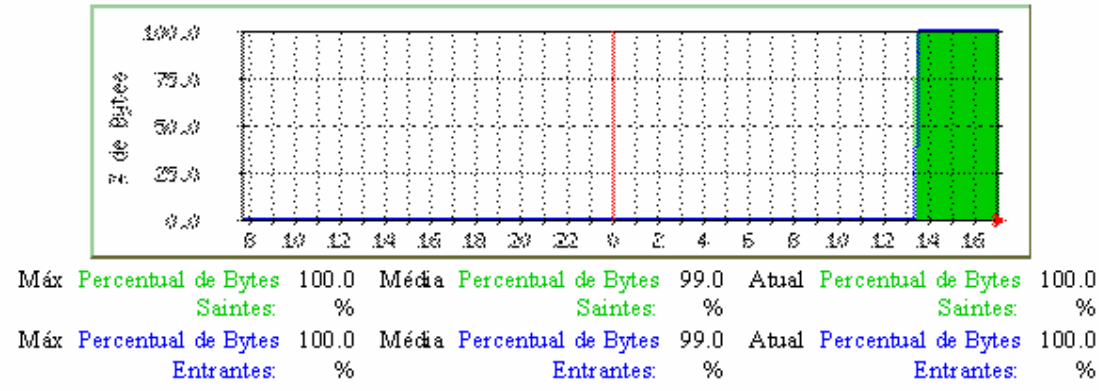


Figura 5.1.5.5 – Análise do Percentual de Bytes que entram e saem pela classe DEFAULT

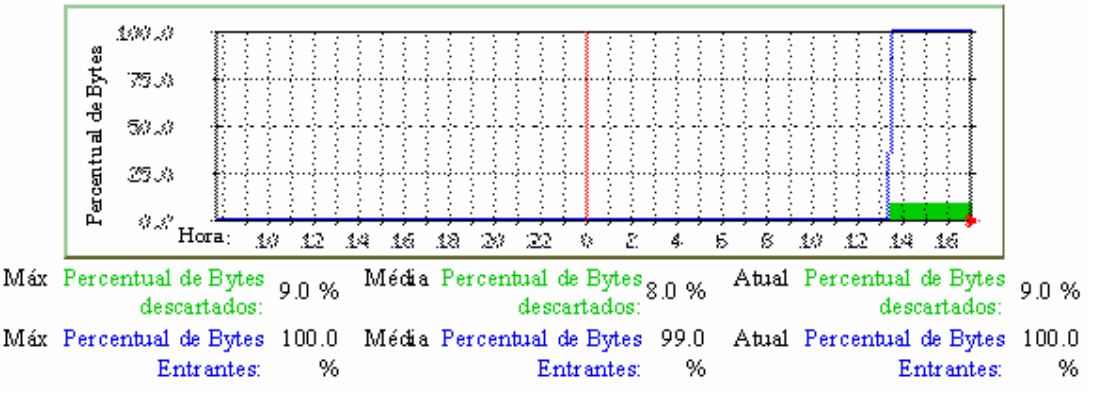


Figura 5.1.5.6 – Análise do Percentual de Bytes descartados pela classe VOIP

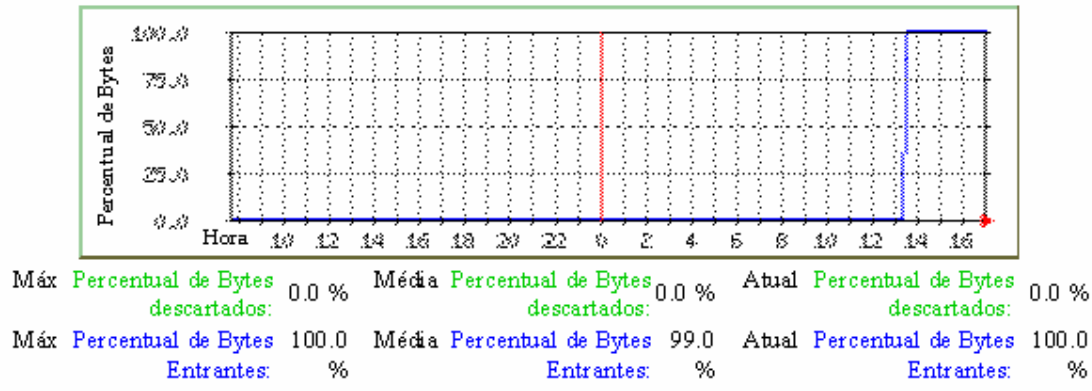


Figura 5.1.5.7 – Análise do Percentual de Bytes descartados pela classe DEFAULT

5.2 Análise da funcionalidade da ferramenta em roteadores das extremidades do domínio DS

Nesta etapa os experimentos foram aplicados nos roteadores das extremidades do domínio DS. A ferramenta foi analisada com a rede sob dois aspectos. No primeiro, a situação da rede está normal. O tráfego que chega nas classes também está dentro do acordo. Através deste experimento, é possível visualizar se está sendo garantida a entrada no domínio DS de todos os fluxos que estão sendo gerados pelas REDES1 e REDES2. Na segunda situação, está sendo analisado o comportamento dos métodos de classificação e moldagem do tráfego para as classes que estão enviando mais tráfego do que foi definido no acordo, embora a rede não esteja saturada.

5.2.1 Rede com tráfego normal e com tráfego da classe dentro dos limites

Os gráficos apresentados na figura 5.2.1.1, figura 5.2.1.2 e figura 5.2.1.3 mostram o percentual de bytes que chegam no domínio DS e são classificados dentro das classes REDE1, REDE2 e DEFAULT. Para cada classe, é apresentado um gráfico que indica o percentual de bytes que chegou na classe e foi transmitido para o domínio DS e percentual de bytes que chegou na classe e foi descartado.

Nota-se nos gráficos que com a situação da rede normal e o tráfego dentro do acordo, não existe descarte para as classes. Através destes gráficos, é possível perceber se está sendo garantida a taxa correta para a classe, como também perceber se a classe envia tráfego superior ao que está no acordo.

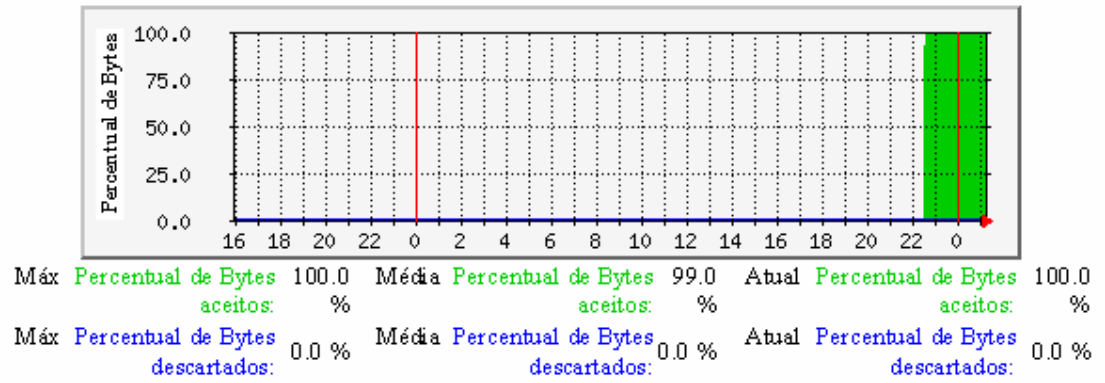


Figura 5.2.1.1 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe REDE1

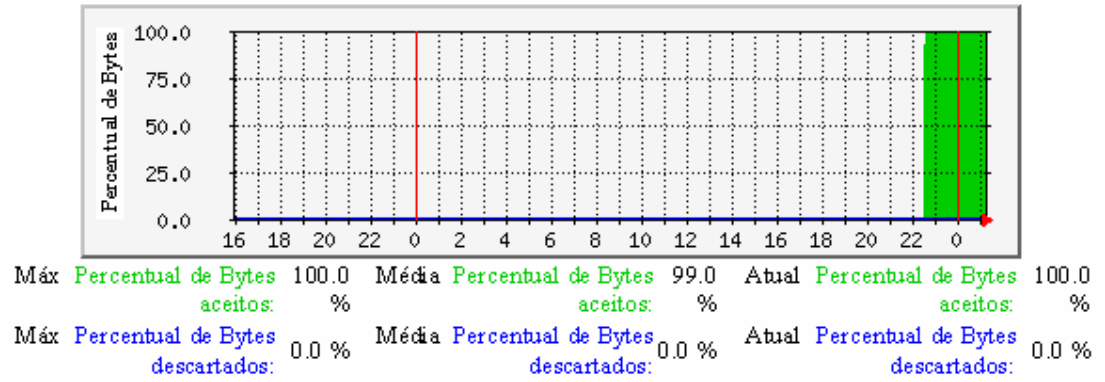


Figura 5.2.1.2 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe REDE2

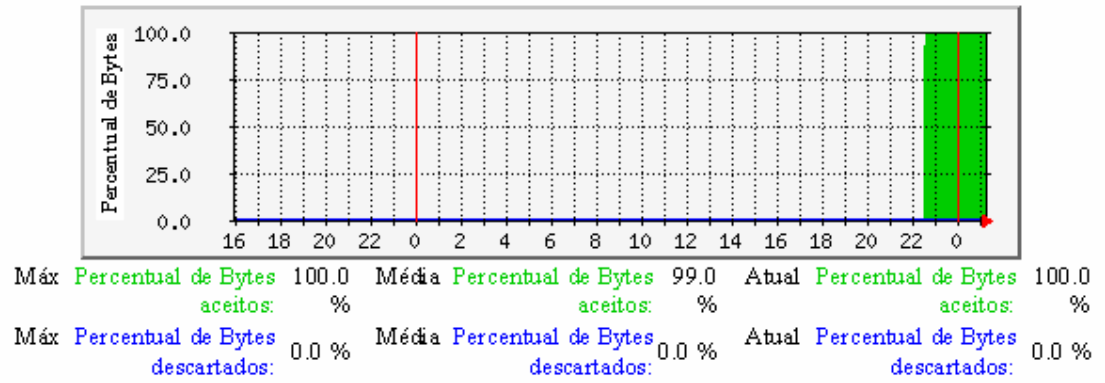


Figura 5.2.1.3 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe DEFAULT

5.2.2 Rede com tráfego normal e com tráfego da classe fora dos limites

Os gráficos apresentados na figura 5.2.2.1, figura 5.2.2.2 e figura 5.2.2.3 mostram o percentual de bytes que chegam no domínio DS e são classificados dentro das classes REDE1, REDE2 e DEFAULT. Para cada classe, é apresentado um gráfico que indica o percentual de bytes que chegou na classe e foi transmitido para o domínio DS e percentual de bytes que chegou na classe e foi descartado.

Nota-se nos gráficos que, com a rede em situação normal e o tráfego das classes fora do acordo, existe descarte para estas classes. Para a classe DEFAULT não houve descartes, pois não existia tráfego saturando o canal. Através destes gráficos, é possível perceber se a classe envia tráfego superior ao que está no acordo ou se a rede não está garantindo o que está no acordo.

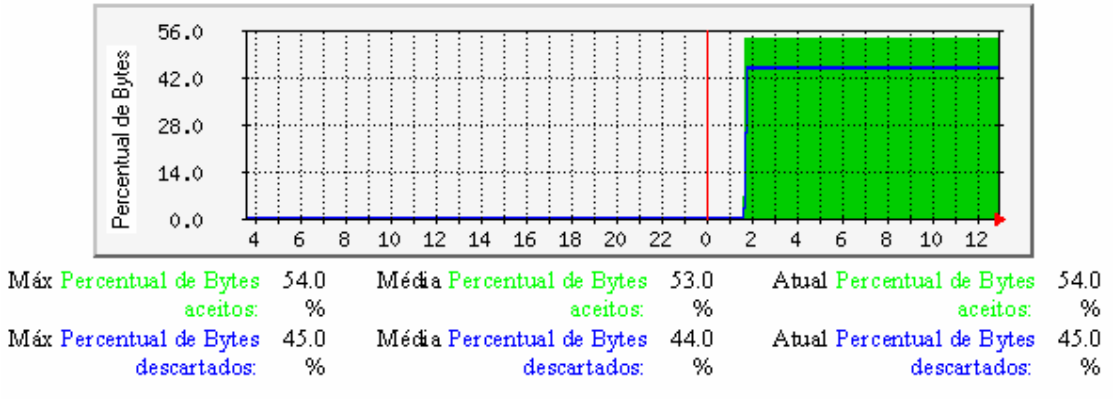


Figura 5.2.2.1 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe REDE1

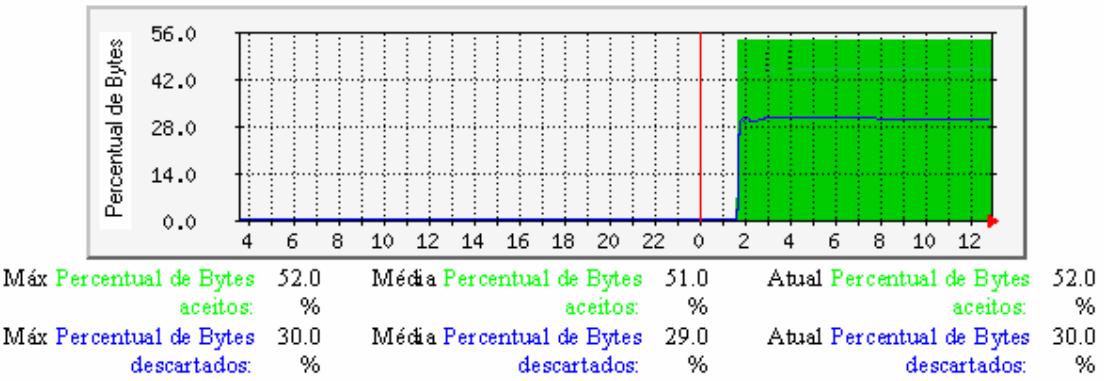


Figura 5.2.2.2 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe REDE2

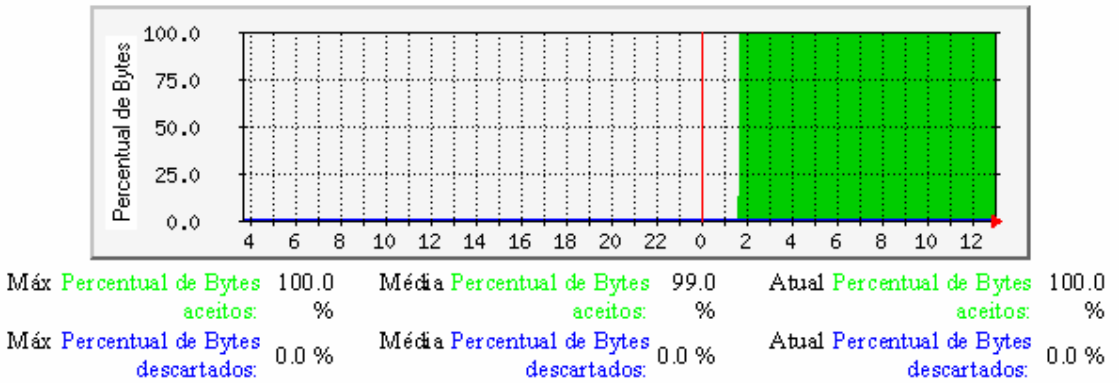


Figura 5.2.2.3 – Percentual de Bytes que chegam no domínio DS e são aceitos ou descartados pela classe DEFAULT

5.3 Conclusão do capítulo

Neste capítulo, apresentaram-se os resultados obtidos através da ferramenta. Foram executados vários experimentos para analisar como a ferramenta reage com a rede em diversas situações. Foram apresentados os gráficos e feita uma análise e descrição dos resultados obtidos para cada experimento.

6 CONCLUSÕES

Neste trabalho, foram apresentados conceitos importantes sobre Qualidade de Serviço em redes IP. Elaborou-se um estudo sobre as MIBS da CISCO que possuem suporte a QOS. Através do estudo, foram selecionadas as variáveis importantes a serem analisadas em um ambiente de gerência de QOS. Com esta definição, foi possível criar formas de se apresentar as informações.

Foi desenvolvida uma ferramenta para o monitoramento de rede IP com QOS (DiffServ) utilizando SNMP. Para constatar se a ferramenta realmente apresenta informações úteis na gerência de QOS, montou-se um ambiente onde foram executados alguns experimentos, criados para simular situações reais nas redes. A análise dos experimentos foi executada sob dois pontos básicos. Na primeira fase, avaliou-se o comportamento do tráfego EF em relação ao BE no roteador interno do domínio DS. Na segunda fase, foi analisado o comportamento do tráfego EF em relação ao BE no roteador da extremidade do domínio DS.

Com a execução dos experimentos, pode-se concluir que a ferramenta de gerenciamento de redes IP com Serviços Diferenciados utilizando SNMP foi eficaz, pois é possível acompanhar em tempo real o que está acontecendo nos roteadores em relação às configurações e estatísticas de DS. Através da análise dos resultados, foi possível identificar quando a classe estava enviando fluxo acima do que estava no acordo, como também foi possível perceber se não houve garantia, mesmo quando o tráfego da classe estava abaixo do acordo.

Foi possível concluir também que para gerenciar QOS através do SNMP é necessário configurar uma classe específica para o tráfego de gerência, pois, caso não exista essa configuração nos momentos em que a rede estiver saturada, será praticamente impossível obter informações de gerência.

7 TRABALHOS FUTUROS

No decorrer desse trabalho, percebeu-se a necessidade de aprofundar os estudos no desenvolvimento de um agente e uma MIB para monitoramento de atraso, variação de atraso e perdas para as classes de serviços. Com este agente, será possível visualizar com maior propriedade a eficácia dos mecanismos de QOS.

Também se percebe a necessidade de desenvolver uma agente e uma MIB para calcular estatísticas de bits por segundo de cada classe. Pois com estas informações é possível visualizar em tempo real a taxa de transferência em bits por segundo que cada classe está transmitindo ou recebendo.

Outro item que se percebeu através deste trabalho é a necessidade de se desenvolver uma ferramenta para monitorar algoritmos de congestionamento, pois é importante analisar o comportamento das filas das classes.

8 REFERÊNCIAS

[1] **MELO, Edison Tadeu Lopes:** Qualidade de Serviço em Redes IP com DiffServ: Avaliação através de Medições. Dissertação de mestrado: UFSC, 2001

[2] **SANTOS, Ana Paula Silva (1999):** Qualidade de Serviço na Internet - *http://www.rnp.br/newsgen/9911/qos.shtml*

[3] **OYAMA, Cybelle Suemi Oda:** Considerações acerca do estabelecimento de QoS no RNP2 - *http://www.rnp.br/newsgen/0205/qos_rnp.shtml#p6*

[4] **Cisco System Inc. (1999):** Quality of Service Solutions. White Paper - *http://www.cisco.com/*

[5] **Cisco System Inc. (1999):** Internetworking Technology Overview – *http://www.cisco.com*

[6]**Cisco System Inc. (2001):** *http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm*

[7] **ISO:** International Organization for Standardization; http://www.iso.org;

[8] **Stardust Technoloies, Inc. (1999):** QOS protocols & architectures – White Paper, *http://www.qosforum.com/*

[9] **Stardust Technologies, Inc. (1999):** Internet Bandwith Management – White Paper, *ATM http://www.qosforum.org*;

[10] **IETF:** Internet Engineering Task; http://www.ietf.org

[11] **Teitlebaum, B. & Hans, T. (1998):** QOS Requirements or Internet2 – Internet2 Technical Paper *http://qos.internet2.edu/may98Workshop/html/requirements.html*

[12] **Ferguson, P. & Huston, G. (1999): Quality of Service:** Delivering QOS on the Internet and in Corporate Networks – Wiley Computer Publishing.

[13] **Cisco System Inc. (2000):** Cisco Management Information Base (MIB) User Quick Reference - *http://cisco.com/univercd/cc/td/doc/product/software/ios11/mbook/index.htm*

[14] **Cisco System Inc. (2001):** *http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm*

[15] **ATM fórum;** *http://www.atmforum.org*;

[16] **Differentiated Service**, *http://www.ietf.org/html.charters/diffserv-charter.html*;

[17] **Nichols (1998):** Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers *http://www.ietf.org/rfc/rfc2474.txt*

[18] **Heinanen, J.; Baker, F.; Weiss, W. & Wroclawski, J. (1999):** Assured Forwarding PHB Goup Request for Comments 2597 - *http://www.ietf.org/rfc/rfc2597.txt*

[19] **Jacobson, V.; K. &. Poduri, K. (1999):** Na Expedited Forwarding PHB Request for Comments: 2598 - *http://www.ietf.org/rfc/rfc2598.txt*

[20] **TANENBAUM, Andrew S**. Redes de computadores**.** 5.ed. Rio de Janeiro: Campus, 1997.

[21] **Baker, Chan, Smith (2001):** Management Information Base for the Differentiated Services Architecture – Internet Draft

http://www.ietf.org/internet-drafts/draft-ietf-diffserv-mib-16.txt

[22] **Cisco System Inc. (2001):**

h*ttp://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm#xtocid9*

[23] Microsoft Corp (1999): Quality of Service Technical White Paper – *http://msdn.microsoft.com/library/psdk/gqos/qosstart_2cdh.htm*

[24]**Naval Researh Laborator (NRL):** The Multi-Generator (MGEN) Toolset *http://manimac.itd.nrl.navy.mil/MGEN*

[25] **Cisco System Inc. (2001):** CISCO-CLASS-BASED-QOS-MIB; *http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml*

[26] **MRTG;** http://www.mrtg.org