Dissertação de Mestrado

Egídio Ieno Júnior

Uma Proposta de Metodologia para Análise de Desempenho de Redes IEEE 802.11 Combinando a Gerência *SNMP* e Ferramentas de Simulação

Agosto/2003

Inatel
Instituto Nacional de Telecomunicações

UMA PROPOSTA DE METODOLOGIA PARA ANÁLISE DE DESEMPENHO DE REDES IEEE 802.11 COMBINANDO A GERÊNCIA *SNMP* E FERRAMENTAS DE SIMULAÇÃO

EGÍDIO IENO JÚNIOR

Dissertação apresentada ao Instituto Nacional de Telecomunicações, como parte dos requisitos para obtenção do Título de Mestre em Engenharia Elétrica.

ORIENTADOR: Prof. Dr. Anilton Salles Garcia

Santa Rita do Sapucaí
2003

FOLHA DE APROVAÇÃO

Dissertação defendida e aprovada em 19/09/2003,
pela comissão julgadora:

Dr. Anilton Salles Garcia / Instituto Nacional de Telecomunicações

Dr. Jorge Moreira de Souza / FITec Inovações Tecnológicas

Dr. José Marcos Câmara Brito / Instituto Nacional de Telecomunicações

Coordenador do Curso de Mestrado

DEDICATÓRIA

“Aos meus pais Egídio e Ilza,
minhas irmãs Irina e Inara,
e a Giselli
pelo apoio incondicional
em todos os momentos”

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado saúde e inteligência para concluir este trabalho.

Ao professor Dr. Anilton Salles Garcia pelo seu trabalho de orientação, sem o qual esta pesquisa não seria possível.

Ao professor Dr. José Marcos Câmara Brito e ao Dr. Jorge Moreira de Souza por fazerem parte da banca examinadora.

Aos amigos Oscavo Gonzaga Prata Júnior, Cristian da Rocha Duarte, Rodrigo Bahia Paiva, Luciano Leonel Mendes, Auder Bonora Nardi, Florence de Castro Campos, Iwanir Araújo da Silva Júnior, Ângelo Pinelli Martins Samia, Giovani Prado Siqueira, William Hiroshi Hisatugu, Ricardo Augusto Rabelo Oliveira, Ádrian Bonfá Drago por suas amizades e apoio.

Aos professores Edson Josias Cruz Gimenez e Mauro Tapajós por estarem sempre dispostos a ajudar.

A busca incessante de vários professores em trazer os melhores softwares de simulação para o INATEL.

A todos os demais funcionários do Instituto Nacional de Telecomunicações que tornam o ambiente de trabalho o melhor possível.

"Já ancorado na Antártida, ouvi ruídos que pareciam de fritura. Pensei: será que até aqui existem chineses fritando pastéis?

Eram cristais de água doce congelada que faziam aquele som quando entravam em contato com a água salgada. O efeito visual era belíssimo. Pensei em fotografar, mas falei para mim mesmo: - Calma, você terá muito tempo para isso...

Nos 367 dias que se seguiram, o fenômeno não se repetiu. Algumas oportunidades são únicas." *Almir Klink*

Como diz o *Dalai Lama*:

"Só existem dois dias no ano que nada pode ser feito. Um se chama ONTEM e o outro AMANHÃ. Portanto HOJE é o dia certo para AMAR, ACREDITAR, FAZER e principalmente VIVER."

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACK - Acknowledgment

AP – Access Point

ASN.1 - Abstract Syntax Notation One

BER - Basic Encoding Rules

BSS – Basic Service Set

CA - Collision Avoidance

CCA – Clear Channel Assessment

CF - Coordination Function

CFP – Contention Free Period

CP – Contention Period

CMIP - Commom Management Information Protocol

CMOT – CMIP over TCP/IP

CRC – Cyclic Redundancy Checking

CSMA - Carrier Sense Multiple Access

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD – Carrier Sense Multiple Access with Collision Detection

CTS – Clear To Send

DA – Destination Address

DCF - Distributed Coordination Function

DES - Data Encryption Standard

DIFS - DCF Interframe Space

DS – Distribuition System

DS1 – Digital Signal Level No 1

DSSS – Direct Sequence Spread Spectrum

ESS – Extended Service Set

FDDI – Fiber Distributed Data Interface

FHSS – Frequency Hopping Spread Spectrum

FTP - File Transfer Protocol

HTTP – Hypertext Transfer Protocol

IANA - Internet Assigned Numbers Authority

IBSS – Independent Basic Service Set

ICMP – Internet Control Message Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IP - Internet Protocol

IrDA – Infrared Data Association

ISM – Industrial, Science and Medical

ISO - International Organization for Standardization

ITU - International Telecommunication Union

LAN – Local Area Network

MAC - Media Access Control

MD – Message Digest

MIB - Management Information Base

MLME - MAC Layer Management Entity

MRTG - Multi Router Traffic Grapher

NAV - Network Allocation Vector

OID – Object Identifier

PCF – Point Coordination Function

PDU – Protocol Data Unit

PHY – Physical Layer

PIFS - PCF interframe space

PLCP - Physical Layer Convergence Protocol

PLME - Physical Layer Management Entity

PMD - Physical Layer Dependent

PPP – Point-to-Point Protocol

PS – Power-Save

QoS – Quality of Service

RA - Receiver Address

RFC – Request for Comment

RMON – Remote Network Monitoring

RTS – Request To Send

SA – Source Address

SHA – Secure Hash Algorithm

SIFS - Short Interframe Space

SMI – Structure Management Information

SNMP – Simple Network Management Protocol

STA – Station

TA - Transmitter Address

TCP – Transmition Control Protocol

UDP – User Datagram Protocol

WAN – Wide Area Network

WAP - Wireless Application Protocol

WEP – Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WPANs - Wireless Personal Area Networks

RESUMO

JÚNIOR, E.I. Uma Proposta de Metodologia para Análise de Desempenho de Redes IEEE 802.11 Combinando a Gerência *SNMP* e Ferramentas de Simulação. Santa Rita do Sapucaí, 2003. Instituto Nacional de Telecomunicações.

A importância da gerência de redes de computadores se torna cada vez mais incontestável. Com o aumento destas redes em complexidade e tamanho torna-se imprescindível um bom conhecimento sobre as possíveis ferramentas de gerência disponíveis para a coleta de dados. Estes dados serão responsáveis por indicar ao administrador da rede a sua situação atual. O *SNMP* é um protocolo capaz de coletar as informações em uma base de informação de gerenciamento (*MIB*) e disponibilizá-las em uma estação gerente para serem tratadas e analisadas. Uma das possíveis análises que podem ser feitas com os dados coletados é relativa ao desempenho da rede, através dos objetos responsáveis por estes indicadores. Desta forma, é proposta nesta dissertação uma metodologia para Análise de Desempenho de redes, combinando a Gerência *SNMP* em um padrão de rede crescente, que é o IEEE 802.11, e o processo de simulação. Ainda nesta metodologia é apresentado um estudo de caso ilustrando a possibilidade do Planejamento de Capacidade em uma rede que tem o seu cabeamento principal (*backbone*) ampliado com redes sem fio.

Palavras-chave: IEEE 802.11, Gerência de Redes, Gerência de Desempenho, Planejamento de Capacidade, Simulação e Ferramentas de Gerência *SNMP*.

ABSTRACT

There is no doubt about the importance of networks management. Computer networks are growing in complexity and size. The complexity of such systems dictates the use of automated network tools to help the tasks of network management. The SNMP is a protocol capable to collect the information in a database (MIB) and to availability them in a controlling station to be treated and analyzed. One of the possible analyses that can be made with the collected data are relative to the performance of the network, through responsible objects for these indicators. Of this form, a methodology for the performance analysis is proposal in this dissertation, using protocol SNMP in a standard of increasing network, that is IEEE 802.11. In addition, in this methodology possibility of the planning of capacity using simulation also was considered. For this, a case study illustrating backbone extended with wireless networks is presented.

Keywords: IEEE 802.11, Network Management, Performance Management, Capacity Planning, Simulation and SNMP Management Tools.

Capítulo I

1 – Introdução

A expansão das redes de computadores vem se tornando cada vez mais abrangente, alcançando um número maior de usuários. Embora esse crescimento venha sendo bem assimilado pelos elementos de redes comerciais existentes, é preciso dar garantias sobre os serviços prestados à rede expandida. Como conseqüência, surge a necessidade de tecnologias para a transmissão dos dados e também para a manutenção da qualidade do serviço prestado ao usuário final.

Uma tecnologia de comunicação sem fio (*wireless*) que consiga ampliar o cabeamento principal (*backbone*) da rede, sem causar transtornos físicos em sua instalação, como perfurar paredes, cortar o piso ou mesmo, possibilitar o acesso à Internet em um local fisicamente inacessível, parece algo inovador e distante. O fato é que esta tecnologia já existe e assim como a própria Internet, teve o início de seu desenvolvimento voltado para fins militares há anos atrás.

A impulsão da tecnologia de redes sem fio ocorre juntamente com o avanço da tecnologia de transmissão digital, a aprovação de padrões para comunicação sem fio e o barateamento dos equipamentos. Além disso, ao longo do tempo, novas aplicações vêm sendo elaboradas para as transmissões sem fio, o que as tornam uma alternativa cada vez mais popular.

Entre os padrões de redes sem fio, existem padrões para redes pessoais sem fio (*Wireless Personal Area Networks - WPANs*) como: *BluetoothÔ*, IEEE 802.15, *HomeRFÔ* e *IrDA* (*Infrared Data Association*), padrões para sistemas móveis, como o protocolo *WAP* (*Wireless Application Protocol*) e padrão para redes locais sem fio, como o padrão IEEE 802.11 [1] [2] [3] [4] [5]. Como se pode observar, o padrão utilizado para redes locais sem fio é o IEEE 802.11, que além das características físicas da comunicação sem fio, apresenta a possibilidade de mobilidade de suas estações, incluindo o movimento entre células (*roaming*).

Segundo a *ISO* (*International Organization for Standardization*), a Gerência de Redes é dividida em cinco áreas: Segurança, Configuração, Desempenho, Contabilidade e Falhas. Destas áreas, a que se voltou à qualidade de serviço prestada ao usuário final é a Gerência de Desempenho. Esta área exige um monitoramento constante dos elementos de rede, ou seja, uma coleta dos indicadores de qualidade, como forma de prevenir a queda da qualidade e planejar melhorias para o futuro.

Todos os indicadores de qualidade ou desempenho de uma rede são altamente dependentes do conjunto de serviços prestados por ela. Para Redes de Telecomunicações, que prestam uma classe de serviços bem conhecida, tais indicadores estão documentados nos padrões *ITU-T E800* e *I350*. Dentre eles, os principais são: atraso (*delay*) na transmissão, *jitter*, eco, taxa de erro e tempo de espera na conexão. Já para as Redes de Computadores e Sistemas Abertos Interconectados existe um consenso apontando para os parâmetros: tempo de resposta, utilização, vazão (*throughput*) e taxa de erros como os mais importantes [6]. Embora os indicadores variem, dependendo do serviço prestado pelo sistema, a análise imposta sobre eles é essencialmente a mesma. O que se deseja é manter os indicadores de desempenho dentro dos limites considerados satisfatórios e ao mesmo tempo atender toda a demanda pelo serviço prestado. Quando os indicadores apontam a degradação do desempenho e a necessidade da correção de rumos, o administrador do sistema deve lançar mão de sistemáticas e técnicas capazes de restabelecer o desempenho desejado. Os principais focos a serem analisados pelo administrador da rede são: Análise de Desempenho, Identificação de Gargalos, Ajuste de Parâmetros do Sistema, Caracterização da Carga de Trabalho e o Planejamento de Capacidade. O que de fato tenta se alcançar com toda essa análise é a melhor relação desempenho/custo para um dado cenário. Embora este seja o objetivo real, em muitos casos o problema do desempenho só é percebido com as reclamações dos usuários e a prática mais comum para se resolver o problema é aumentar a capacidade do sistema, mesmo que a solução não apresente uma boa relação custo/benefício.

Pensando na ampliação da rede tradicional (cabeada) utilizando redes sem fio, surge a seguinte questão: Será que haverá atendimento aos requisitos de qualidade

dos serviços prestados? Qual será o desempenho da rede IEEE 802.11 e como ele poderá afetar a rede como um todo?

Para responder a estas perguntas é primordial a análise do desempenho das redes sem fio, a verificação do tráfego gerado por todas as estações sem fio e que passa pelo Ponto de Acesso (*Access Point - AP*), além da previsão do impacto de novas aplicações e usuários na rede como um todo. Com todos os indicadores de desempenho, consegue-se analisar o desempenho de qualquer rede, inclusive das redes IEEE 802.11. Desta forma, é proposta uma metodologia visando a coleta, o tratamento e a apresentação dos dados de forma mais amigável ao Administrador de Rede. Contudo, ainda buscando uma integração da metodologia com ferramentas de simulação, foi criada uma fase responsável pelo Planejamento de Capacidade da rede.

Foi pensado então em como obter os indicadores de desempenho desejados e que ferramentas poderiam ser utilizadas para a coleta de dados. O interesse se voltou imediatamente à gerência baseada no protocolo *SNMP* (*Simple Network Management Protocol*) que, além de ser a mais utilizada e implementada nos dispositivos de redes tradicionais, possui a segunda versão da base de informação de gerenciamento (*Management Information Base - MIB-II*), com quase todos os objetos responsáveis pelos indicadores de desempenho, e vem sendo bastante empregada em redes IEEE 802.11. Esta arquitetura de gerência inclui o protocolo *SNMP*, diversas *MIBs* e os procedimentos que são utilizados para monitorar e gerenciar os dispositivos conectados à rede.

Com a finalidade de verificar como o tráfego gerado em redes sem fio pode afetar a rede como um todo, foi utilizada a ferramenta de simulação *OPNET® Modeler*, que ainda possibilitou a compreensão dos parâmetros característicos destas redes. As ferramentas de simulação são muito importantes na Análise de Desempenho, já que se pode criar um cenário com o perfil do usuário e o tráfego gerado bem próximos do real, realizar as alterações pertinentes no cenário e obter a melhor solução sem gerar gastos ou paradas no funcionamento da rede real.

1.1 – Motivações para o Estudo sobre Redes IEEE 802.11 e o Protocolo *SNMP*

As redes locais de computadores tradicionais, ou seja, cabeadas (*wired*), usam um meio físico para interconectar os seus terminais, como por exemplo, o par trançado. Vários pontos são fornecidos no meio físico, permitindo assim, a conexão dos terminais ao meio. Essas redes podem ser conectadas entre si utilizando pontes (*bridges*) ou *switches* e o protocolo mais comum é o Ethernet (IEEE 802.3), com todas as suas variações ao longo de sua evolução.

Já as redes locais sem fio aumentam o acesso das redes cabeadas através do *AP*, que liga o *backbone* da rede tradicional ao usuário móvel utilizando o espectro de rádio.

Além da possibilidade de ampliar a cobertura de uma rede cabeada, as redes sem fio apresentam várias outras vantagens, tais como:

- **Facilidade de instalação**

A velocidade e simplicidade de instalação em redes sem fio eliminam a necessidade de "puxar" cabos através de paredes e tetos. Não necessita de homologação para atuar em sua faixa de freqüência, podendo ser criada e desfeita por pessoas leigas, bastando para isto uma estação com a interface adequada e um software instalado que lhe dá os passos para a sua configuração.

- **Flexibilidade**

A retirada e a colocação de estações ocorre de forma dinâmica, ficando a cargo do protocolo de controle de acesso ao meio (*Media Access Control – MAC*) as respectivas comunicações.

- **Mobilidade**

É a possibilidade de sair de um local, por exemplo, seu escritório e ir para outra sala, continuando conectado à rede, permitindo maior produtividade e oportunidades de serviço que não são possíveis em uma rede cabeada.

- **Escalabilidade**

Trata-se da capacidade da rede em ampliar a sua área de cobertura, formando uma rede ainda maior através do uso de pontos de acesso, podendo ser configurado para qualquer topologia. As configurações são facilmente mudadas e englobam desde redes fim-a-fim, ideais para um pequeno número de usuários, até uma infra-estrutura

de rede completa com centenas de usuários e movimentação dentro da área de cobertura do sinal.

Algumas das muitas aplicações que se tornaram viáveis devido ao poder e à flexibilidade desta tecnologia citada anteriormente são apresentadas abaixo:

- Em hospitais, informações sobre pacientes podem ser obtidas por médicos ou enfermeiras utilizando computadores com interface para redes sem fio.
- Para aumentar a produtividade de uma equipe de auditores ou pequenos grupos de trabalho, que utilizam a rede sem fio para consultar ou contabilizar as informações.
- As universidades começam a oferecer acesso sem fio às suas redes, como uma forma de facilitar o acesso às informações e ao aprendizado.
- Administradores de rede têm seu trabalho facilitado e minimizado, uma vez que as redes sem fio possuem uma instalação mais fácil comparada às redes que usam cabos.
- Distribuidoras de revendas usam redes sem fio para aumentar sua produtividade, trocando informações com o banco de dados central.
- Administradores de rede implementam redes sem fio como *backup* para aplicações de missão crítica que são executadas em redes cabeadas.
- Em salas de conferências, os executivos podem tomar decisões rápidas com informações em tempo real em suas mãos.

A estratégia da rápida divulgação junto a um mercado competitivo, o crescimento meteórico da Internet e dos serviços *on-line*, são fortes testemunhas dos benefícios de dados e recursos compartilhados. Com as redes sem fio o usuário pode ter acesso à informação compartilhada sem ter que procurar um conector para se plugar, e os administradores de rede podem instalar ou aumentar as redes sem precisar puxar ou mover cabos.

Com as melhorias proporcionadas pelos grupos de trabalhos formalizados pelo *IETF* (*Internet Engineering Task Force*), junto aos vários benefícios descritos anteriormente que são fornecidos pelas redes sem fio, essa tecnologia tem forças para se tornar ainda mais difundida. Sendo assim, a complexidade destas redes é aumentada e tanto as redes totalmente sem fio, como os *backbones* já existentes ampliados com essas redes passam a requerer um certo nível de qualidade de serviço

para a satisfação de seus usuários. Desta forma, torna-se imprescindível um gerenciamento que possa não só garantir uma boa interoperabilidade da rede, mas também o seu funcionamento ininterrupto e com qualidade.

Para a gerência de redes, vários foram os protocolos criados com a explosão dos equipamentos de rede, como o *SGMP* (*Simple Gateway Monitoring Protocol*), em 1987. A partir dele, surgiram três outros caminhos: um foi a generalização de um dos primeiros protocolos usados na Internet, o *HMP* (*Host Monitoring Protocol*), dando-lhe o nome de *HEMS* (*High-Level Entity Management System*); o segundo foi o *SNMP* (*Simple Network Management Protocol*); e o terceiro foi o *CMIP* (*Common Management Information Protocol*) sobre *TCP/IP* (*Transmission Control Protocol/Internet Protocol*), cujo nome é *CMOT* (*CMIP Over TCP/IP*). Este último padronizado pela *ISO* [5].

Entre todos os protocolos voltados à gerência de redes citados anteriormente, o *SNMP* é o que alcançou maior sucesso. Isto se deu graças à sua facilidade de implementação e ao fato de possibilitar, efetivamente, um gerenciamento de ambientes heterogêneos, além de ter sido o primeiro protocolo público, já que o *CMIP* apresentava uma alta complexidade e demorou a chegar ao mercado.

Por se tratar do protocolo de gerência mais empregado em redes de comunicação de dados, a utilização do protocolo *SNMP* se mostrou bastante interessante na etapa de coleta dos dados, a qual fará parte da Fase Um da metodologia de Análise de Desempenho que será proposta no Capítulo 4 desta dissertação.

1.2 – Objetivos do Trabalho e Estrutura da Dissertação

Com base no crescimento da utilização de redes sem fio, padrão IEEE 802.11, na estrutura de redes locais em ambientes corporativos e considerando, entre outros fatores, a necessidade de convivência com padrões já estabelecidos e a pouca maturidade das redes sem fio, este trabalho se propõe aos seguintes objetivos:

- Apresentar uma proposta de metodologia para Gerência de Redes e o estudo de Planejamento de Capacidade em redes locais IEEE 802.11.
- Analisar a estrutura de gerência de redes locais IEEE 802.11 tomando-se como base a existência de três tipos de *MIBs* (*MIB-II*, *MIB* IEEE 802.11 e *MIBs* proprietárias).

- Determinar os objetos que reflitam os Indicadores de Desempenho mais representativos do ambiente gerenciado.
- Estudo de ferramentas para o gerenciamento *SNMP* em redes IEEE 802.11.
- Identificar as formas de combinar ferramentas de Gerência *SNMP* com ambientes de simulação para a avaliação de desempenho e estudo de capacidade em redes locais baseadas no padrão IEEE 802.11.
- Mostrar com um estudo de caso, a necessidade e a viabilidade da adoção da metodologia proposta como parte de um sistema de apoio à decisão.
- Simular a influência dos diversos parâmetros da camada *MAC* no desempenho de redes IEEE 802.11, verificando a teoria discutida sobre estas redes.

Para uma melhor compreensão do propósito desta dissertação, a mesma foi organizada da seguinte maneira: no Capítulo 2 é apresentada uma visão geral sobre o padrão IEEE 802.11, em seguida, no Capítulo 3, uma visão geral sobre a Gerência de Redes utilizando o protocolo *SNMP* e a Análise de Desempenho utilizando ferramentas de simulação são apresentadas. No Capítulo 4, que é o mais importante, é proposta uma metodologia para a Análise de Desempenho de redes, voltada às redes IEEE 802.11, analisando algumas das *MIBs* públicas, específicas e proprietárias. Com a finalidade de validar a metodologia proposta é apresentado um estudo de caso no Capítulo 5. O Capítulo 6 mostra, através de simulações, os fatores que influenciam o desempenho das redes IEEE 802.11 e no Capítulo 7 são apresentadas as conclusões da pesquisa e também sugeridas algumas propostas para trabalhos futuros.

O texto apresenta ainda dois anexos onde são apresentados: um estudo sobre os softwares de gerência que podem ser empregados em redes IEEE 802.11 e alguns parâmetros e estatísticas coletadas para redes IEEE 802.11 no simulador *OPNET^{â} Modeler*.

Capítulo II

2 – Visão Geral sobre o Padrão IEEE 802.11

2.1 – Breve Histórico do Padrão IEEE 802.11

As tecnologias de redes sem fio estão evoluindo a passos largos e cada vez mais vêm sendo utilizadas na comunicação entre dispositivos dos mais variados tipos e tamanhos (computadores pessoais, portáteis e de mão, telefones, máquinas industriais e outros) em ambientes diferentes, como residências, edifícios e florestas. Por permitirem a mobilidade, estas redes facilitam a onipresença do poder computacional, tornando possível a aquisição de informações em lugares que antes a comunicação dificilmente chegaria. Vários padrões e tecnologias de redes sem fio surgiram nos últimos anos com a finalidade de acomodar a vasta gama de aplicações e principalmente ampliar as áreas de coberturas das redes cabeadas. Foram concebidas desde redes celulares de larga cobertura, passando pelas redes locais, até as redes *PANs* (*Personal Area Networks*) usadas na comunicação de equipamentos pessoais, como *PDAs* (*Personal Digital Assistants*), câmeras digitas, computadores e celulares. Neste cenário, o padrão para redes locais sem fio IEEE 802.11 (*WLANs*) obteve um enorme sucesso, com uma estimativa de cerca de 2 milhões de placas de rede instaladas até o final de 2002 [3]. A sua diversidade em termos de capacidade e cobertura junto ao baixo custo dos dispositivos de rede deu ao padrão 802.11 uma vasta empregabilidade, podendo ser encontrado em redes de acesso na telefonia celular de segunda e terceira gerações, em soluções residenciais e de campus, ou mesmo em soluções corporativas utilizando enlaces ponto-a-ponto de média distância.

2.2 – O Padrão IEEE 802.11

Como todos os padrões da família IEEE 802.x, o padrão IEEE 802.11 especifica as camadas físicas (*PHY*) e de controle de acesso ao meio (*MAC*). Este padrão para redes sem fio foi definido em 1999 e continua sendo desenvolvido por vários grupos de trabalho que têm como objetivo prover melhorias, como qualidade

de serviço (*Quality of Service* - *QoS*) e novas aplicações. A Figura 2.1 ilustra uma visão gráfica do padrão IEEE 802.x, contextualizado-o com o modelo de referência usado para interconexão de sistemas abertos, o *RM OSI* (*Reference Model for Open Systems Interconnection*) da *ISO* [5].

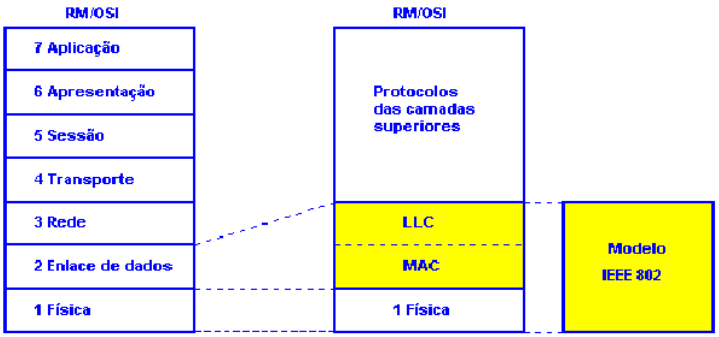


Figura 2.1 *– O Modelo IEEE 802.x com o RM OSI*

2.2.1 - A Arquitetura do Padrão IEEE 802.11

A arquitetura do 802.11 consiste de vários componentes que interagem para possibilitar a formação de uma rede local sem fio com suporte à mobilidade de estações de modo transparente para as camadas superiores [2]. As definições dos componentes dessa arquitetura são apresentadas a seguir:

- *AP – Access Point* são estações especiais responsáveis pela captura das transmissões realizadas pelas estações de sua célula destinadas às estações localizadas em outras células, retransmitindo-as utilizando o sistema de distribuição (*DS*).
- *STA – Station* é qualquer dispositivo que implementa as camadas física e de enlace do padrão 802.11, podendo ser um computador fixo com interface para rede sem fio, móvel (*notebooks*) ou mesmo um *AP*.
- *BSS – Basic Service Set* é um grupo de estações que estão sob o controle de uma função de coordenação (*Coordination Function* - *CF*), formando o modo de operação da rede sem fio denominado de Infra-estruturada.
- *IBSS – Independent Basic Service Set* como o próprio nome diz, trata-se de um grupo de estações independentes, ou seja, não utilizam a estrutura de comunicação provida pelo *AP*. Desta forma as estações se comunicam diretamente umas com as outras formando o modo de operação *Ad-hoc*.

- *ESS – Extended Service Set* é um conjunto de redes Infra-estruturadas (*BSS*), onde o *AP* de um *BSS* se comunica com o de outro, possibilitando assim uma mobilidade maior, dado que a cobertura da rede agora é estendida ao domínio do *ESS*. Para um equipamento do outro lado do *ESS*, o *ESS* e todas as estações se apresentam como uma simples rede local, onde todas as estações são fisicamente estacionárias. Assim, a mobilidade fica escondida de todas as estações do outro lado do *ESS*.
- *DS – Distribuition System* é um meio abstrato pelo qual um *AP* se comunica com outro, trocando informações de uma estação móvel de um *BSS* para a de outro e trocando quadros com a rede cabeada. O padrão IEEE 802.11 não especifica o sistema *DS*, podendo ser baseado em vários tipos de tecnologias, como por exemplo, a Ethernet.

A Figura 2.2 [7] ilustra melhor as definições feitas anteriormente.

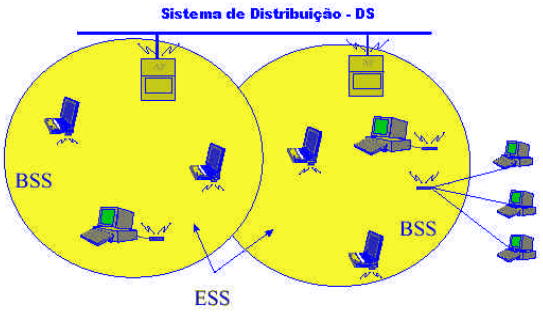


Figura 2.2 – *Arquitetura de uma Rede WLAN Estendida*

- *Portal* - é um dispositivo que tem a funcionalidade de uma *bridge*, interconectando uma rede sem fio a uma rede cabeada, por exemplo o padrão 802.3 [5]. A função do Portal pode ser executada também por uma estação especial (*AP*). A Figura 2.3 ilustra uma arquitetura com a utilização de um Portal.

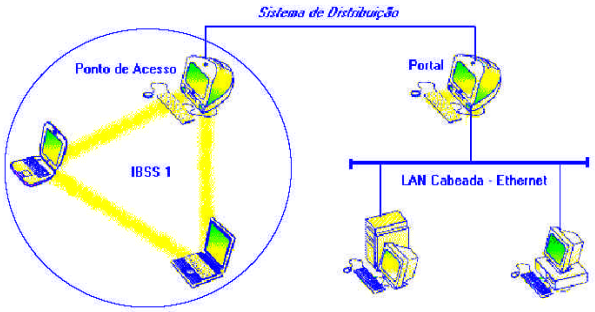


Figura 2.3 – *Rede IEEE 802.11 Conectada à Rede IEEE 802.3*

2.2.2 – A Camada Física do Padrão IEEE 802.11

Este padrão define três tipos de camada física: espalhamento de espectro por salto em freqüência (*Frequency Hopping Spread Spectrum – FHSS*), espalhamento de espectro por seqüência direta (*Direct Sequence Spread Spectrum – DSSS*) e infravermelho. Todas as camadas físicas do padrão 802.11 incluem a provisão de um sinal de avaliação de canal livre (*Clear Channel Assessment signal – CCA*), que é utilizado pela camada física para indicar se o meio está livre, prevenindo colisões. O padrão especificado para camada física oferece uma taxa de 1 ou 2 Mbps. Grupos de trabalho como o 802.11a e 802.11b [1] surgiram visando o aumento destas taxas.

O *FHSS* é uma técnica de espalhamento de espectro que divide a banda passante total em vários canais de pequena banda e faz com que o transmissor e o receptor utilizem um desses canais por um certo tempo e depois "saltem" para outro canal. Com isso, permite-se a coexistência de várias redes em uma mesma área, através da separação dessas redes por diferentes padrões pseudo-aleatórios de uso do canal chamados seqüências de saltos. O *FHSS* usa a banda *ISM* (*Industrial, Scientific and Medical*) de 2,4000 a 2,4835 GHz [2].

O *DSSS* é um método alternativo de espalhamento de espectro, no qual códigos são separados. Também faz o uso da banda *ISM* de 2,4 GHz. O espalhamento é feito com a divisão da banda disponível em 11 subcanais, cada um com 11 MHz, e do espalhamento de cada símbolo de dados usando uma seqüência de *Barker* de 11 chips dada por (+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1) [3]. A largura de um canal *DSSS* é de 20 MHz, limitando o uso máximo de três canais não sobrepostos, já que a distância entre portadoras deve ser de 30 MHz.

A especificação de infravermelho utiliza comprimentos de onda de 850 a 950 nano metro. O infravermelho foi projetado para ser usado em áreas fechadas e opera com transmissões não direcionadas que alcançam um máximo de aproximadamente 10 metros, caso não exista luz do sol interferindo, ou 20 metros, caso sejam utilizados receptores mais sensíveis [2] [3].

Das características apresentadas de cada técnica de transmissão pode-se concluir que uma estação se comunicando com uma das tecnologias de camada física, não consegue "falar" com a estação que faça uso de outra tecnologia de

camada física para transmitir os seus bits. Isto traz um grave problema na expansão destas redes, que é o fator de incompatibilidade entre fabricantes.

Vale ressaltar que tanto a tecnologia *FHSS* como a *DSSS* tem como uma de suas características o aumento do sigilo em suas comunicações. No entanto, esta característica não é aplicada pelo padrão 802.11, pois as estações transmitem de maneira que todas as outras estações no mesmo *BSS* possam receber os seus dados, bastando para isto que seu endereço *MAC* coincida com o endereço de destino contido no quadro enviado. Porém, o uso destas tecnologias tem por objetivo obter a diminuição da susceptibilidade à interferência e ao desvanecimento (*fading*) seletivo [3].

Ainda é especificada no padrão 802.11 a subcamada física *PLCP* (*Physical Layer Convergence Protocol*), que é responsável por mapear os dados da camada *MAC* para o formato do quadro de transmissão ou recepção e inclui a entidade de gerenciamento *PLME* (*Physical Layer Management Entity*), além da *PMD* (*Physical Layer Dependent*), que define as características e métodos de transmissão e recepção do meio sem fio. Ainda referente à camada física, existe uma entidade de gerência cuja função é anotar as estatísticas para a *MIB* desta camada. Na Figura 2.4 [2] pode-se observar melhor as camadas especificadas neste padrão [2] [4].

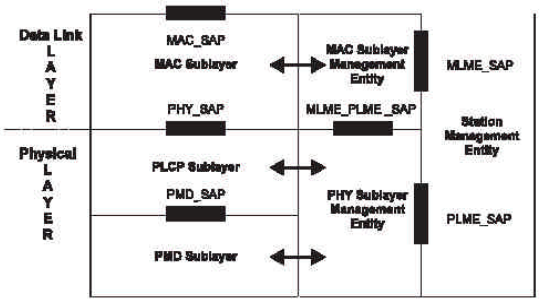


Figura 2.4 – *As Camadas do Padrão IEEE 802.11*

2.2.3 – A Camada *MAC* do Padrão IEEE 802.11

Esta camada define dois tipos de funções de acesso ao meio, como descrito a seguir: a função de coordenação distribuída (*Distributed Coordination Function – DCF*) e a função de coordenação de um ponto (*Point Coordination Function - PCF*).

2.2.3.1 – A Operação da Função de Coordenação Distribuída – *DCF*

O *DCF*, mecanismo básico de acesso ao meio do 802.11 é baseado em um acesso múltiplo com detecção de portadora (*Carrier Sense Multiple Access - CSMA*)

onde as estações “sentem” o meio para detectar se há outra estação transmitindo. Detectando a ausência de portadora no canal, a transmissão ocorre. No entanto, se duas estações detectarem que o canal está livre ao mesmo tempo, fatalmente ocorrerá colisão. Para diminuir a probabilidade de colisões, o padrão 802.11 define um mecanismo para evitar a colisão (*Collision Avoidance - CA*), ou seja, uma estação deverá permanecer “sentindo” o meio por um tempo aleatório antes de iniciar a sua transmissão. Embora o método de acesso com detecção de colisão *CSMA/CD* (*Carrier Sense Multiple Access with Collision Detection*) seja muito utilizado em redes IEEE 802.3, ele não é adequado às redes 802.11, pois neste caso a detecção de colisões é muito difícil por assumir que todas estações ouvem as outras, além de requerer um rádio que transmita e receba ao mesmo tempo (*full-duplex*), que é de custo elevado se comparado ao rádio *half-duplex*.

No padrão 802.11 há dois tipos de modo de acesso ao meio *DCF*: o baseado puramente no protocolo *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidance*), que é obrigatório, e um outro opcional que utiliza quadros de pedidos (*Request To Send*) e permissões (*Clear To Send*) para melhorar o desempenho na transmissão de pacotes maiores que um certo limiar. O funcionamento básico do *DCF* obrigatório é apresentado na Figura 2.5 [3] e sua descrição vem logo a seguir.

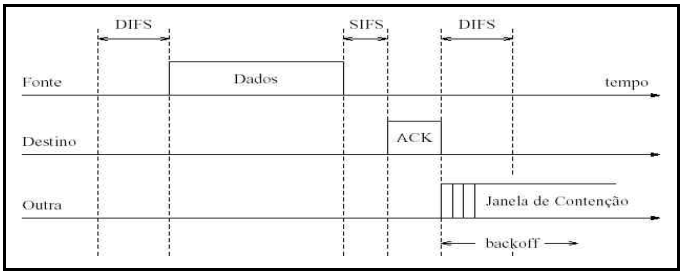


Figura 2.5 – *Operação Básica da Função de Acesso ao Meio – DCF*

Uma estação que deseje transmitir “sente” o meio por *DIFS* (*DCF Interframe Space*) segundos e, caso não ocorra outra transmissão, transmite. Após *SIFS* (*Short Interframe Space*) segundos, se a estação de destino recebeu os dados corretamente, baseado no cheque de redundância cíclica (*CRC*) [2], ela envia um quadro de reconhecimento (*ACK*) para a estação transmissora. Caso não receba o quadro *ACK*, a estação transmissora deduzirá que houve uma colisão, escalonará uma retransmissão e entrará no processo de *backoff* [2]. Além disso, todas as estações que desejarem transmitir durante a transmissão de outra estação, entrarão no

processo de *backoff* no instante em que “sentirem” o meio livre. O processo de *backoff* nada mais é do que um tempo gerado aleatoriamente com a finalidade de reduzir a probabilidade de colisão na próxima tentativa de transmissão das estações e de tornar a disputa pelo meio mais justa. Pela definição de espaço entre quadros, o tempo *SIFS* é menor do que *DIFS*, ou seja, o quadro *ACK* enviado pela estação receptora terá prioridade sobre uma nova transmissão de outra estação.

No *DCF* opcional, o protocolo *CSMA/CA* acrescenta ao algoritmo básico com reconhecimento um mecanismo que envolve a troca de quadros de controle *RTS* (*Request To Send*) e *CTS* (*Clear To Send*). Utilizando este mecanismo, a detecção de portadora pode ser feita tanto pela camada física (*CCA*), como pela camada *MAC* (virtual) [2]. O mecanismo de detecção virtual usa uma distribuição de informação de reserva de meio através da troca de quadros *RTS* e *CTS* antes do envio dos dados propriamente. Estes quadros contêm informações a respeito do nó de destino, de um tempo relativo ao envio do pacote de dados e de seu respectivo quadro de reconhecimento no campo *Duration* [2], o qual é utilizado para indicar o tempo que as outras estações deverão aguardar até o término da transmissão de dados que será feita. Cada estação controla o uso dos quadros *RTS* e *CTS* utilizando um limiar de *RTS* (*RTSthreshold*), o qual possibilita a estação não usar os quadros *RTS* e *CTS*, sempre utilizá-los ou ainda usá-los somente na transmissão de quadros maiores que o limiar de *RTS*.

O funcionamento *DCF* opcional é mostrado na Figura 2.6 [3] e ocorre da seguinte maneira: Uma estação após “sentir” o meio livre por pelo menos *DIFS* segundos envia um quadro *RTS* para a reserva do meio. O receptor estando pronto para receber os dados responde com um quadro *CTS* após o meio estar livre por *SIFS* segundos. Todas as estações que “ouvirem” os quadros *RTS*, *CTS* ou ambos irão utilizar a informação da duração relativa ao pacote de dados para atualizar o vetor de alocação de rede (*Network Allocation Vector – NAV*), o qual é utilizado para uma detecção virtual da portadora. Esta informação indica o período de tempo pelo qual uma transmissão não é iniciada por outra estação, não importando se o *CCA* indique que o meio está livre. Deste modo, qualquer estação escondida (*Hidden Station*) poderá adiar a sua transmissão para evitar colisões. O transmissor iniciará o envio dos pacotes de dados logo após receber o quadro *CTS* e o meio estiver livre por *SIFS*

segundos. Caso o transmissor não receba o quadro *CTS*, deverá entrar na fase de *backoff* [2] [3] e então retransmitir o quadro *RTS*.

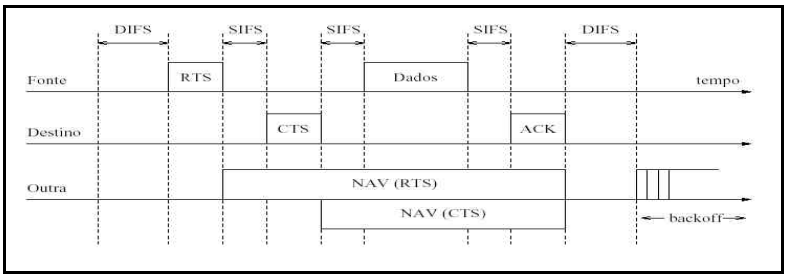


Figura 2.6 – *Operação da Função de Acesso ao Meio DCF na Reserva do Meio*

2.2.3.2 - A Operação da Função de Coordenação em um Ponto – *PCF*

Como no modo *DCF* utilizando quadros para reserva de meio, o *PCF* também é um tipo de acesso opcional da camada *MAC* do 802.11, ou seja, a sua implementação não é obrigatória pelo padrão. No modo *PCF*, um único ponto controla o acesso ao meio, através da consulta a cada estação, proporcionando a possibilidade de transmitir sem contenção. Ele é empregado em tráfego onde o atraso é um fator limitante na qualidade do serviço prestado pela rede, como ocorre no tráfego de voz.

O coordenador de ponto divide o tempo de acesso em períodos de superquadros. Cada superquadro compreende um período livre de contenção (modo *PCF*) e um período com contenção (modo *DCF*), como ilustrado na Figura 2.7 [3]. Durante o modo *DCF* as estações que precisam transmitir no modo *PCF* se registram junto ao coordenador de ponto, formando uma lista de consultas [8]. O coordenador de ponto inicia e controla o tempo livre de contenção. Ele "escuta" o meio por *PIFS* (*PCF Interframe Space*) segundos e então começa um período livre de contenção (*Contention Free Period – CFP*) através da difusão de um quadro de gerenciamento (*beacon*). De acordo com a lista de consultas, o coordenador de ponto dá o direito à estação de transmitir, enviando um pacote de dados, caso exista, dentro de um pacote de consulta (*piggyback*). A estação receptora envia um quadro *ACK*, também com dados se for o caso, depois de *SIFS* segundos. Por definição, o tempo *PIFS* é menor do que o *DIFS* e, portanto, o método de acesso *PCF* terá prioridade sobre o *DCF*. Todas as estações adicionam a duração máxima do período de contenção (*CFPmaxduration*) aos seus respectivos vetores de alocação da rede (*NAVs*). O período livre de contenção pode terminar a qualquer momento através do envio de

um quadro de fim de período livre de contenção (*CFend*) pelo coordenador de ponto. O atraso mostrado na Figura 2.7 [3] indica que o período livre de contenção pode ser adiado pela transmissão de qualquer estação que esteja no modo *DCF*.

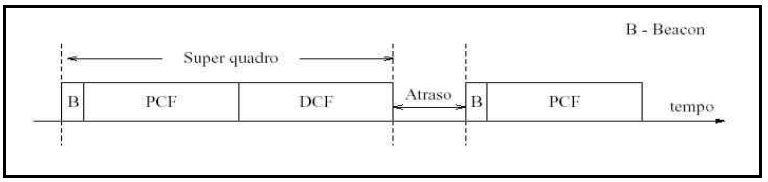


Figura 2.7 - *Modos PCF e DCF Operando Juntos*

Vale ressaltar que os espaços entre quadros podem ser utilizados para dar prioridade de transmissão a uma estação operando no modo *DCF*, ou seja, a que esperar por *SIFS* segundos terá maior prioridade, pois se trata do menor tempo [9], além de minimizar a probabilidade de ocorrer colisões. Os valores de tempo a que correspondem os espaços entre quadros são definidos no padrão IEEE 802.11 [2]. A seguir são relacionados esses tempos entre si, onde se observa que o tempo *DIFS* representa o maior valor [2] [3] [4].

- *SIFS - Short Interframe Space*
- *PIFS - PCF Interframe Space = SIFS + slot time*
- *DIFS - DCF Interframe Space = PIFS + slot time*

Onde:

SIFS – corresponde ao tempo de processamento gasto na camada *MAC* e na física.

Slot time - tempo máximo de ida e volta dentro de um *BSS*.

Ainda na camada *MAC*, existe a subcamada que inclui a entidade de gerenciamento *MLME* (*MAC Layer Management Entity*) responsável por promover a interface pela qual o gerenciamento no nível de camada *MAC* é realizado. A base de informação de gerenciamento (*MIB*) contém objetos gerenciáveis *SNMPv.2* com a finalidade de determinar o *status* e a configuração de uma estação sem fio [4].

2.2.3.3 – Tipos de Quadros mais Comuns

O formato do quadro *MAC* é apresentado na Figura 2.8 [2] e seus campos são descritos logo a seguir.

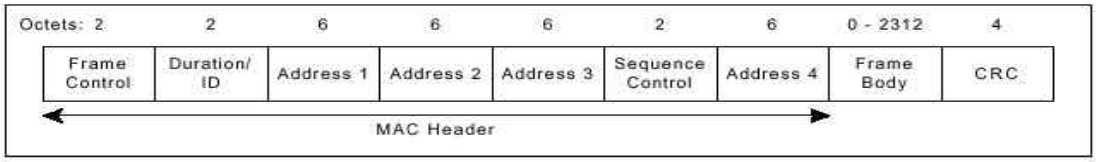


Figura 2.8 – *Formato do Quadro MAC*

- *Duration/ID* – em quadros do tipo *Power-Save* (*PS*) o seu conteúdo informa a identidade da estação que transmite o quadro. Em outros quadros o seu conteúdo é o valor da duração do tempo que ainda resta na transmissão, ou seja, informação para o vetor de alocação da rede (*NAV*).
- *Sequence Control* – é usado para representar a ordem de diferentes fragmentos de um mesmo quadro e para reconhecer quadros duplicados.
- *Frame Body* – contém os dados das estações que dependem dos tipos e subtipos de quadros.
- *CRC* – contém 32 bits usados para o cheque de redundância cíclica.

O conteúdo dos campos de endereçamento *address* 1, 2, 3 e 4 são ilustrados na Tabela 2.1 [2] e definidos logo a seguir.

Tabela 2.1 – *Campos de Endereçamento MAC*

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- 0 0 – os quadros de dados saem diretamente de uma estação para outra dentro da mesma rede (*BSS*).
- 0 1 – quadro de dados saindo do sistema de distribuição (*DS*).
- 1 0 – quadro de dados destinados ao sistema de distribuição (*DS*).
- 1 1 – quadro de dados sendo distribuído de um *AP* para outro *AP*.

Onde:

- *BSSID* – identifica cada *BSS* dentro do *ESS*. Em uma rede Infra-estruturada é o próprio endereço *MAC* do *AP* e em uma rede *Ad-hoc* é um endereço exclusivo alocado administrativamente pela estação que inicia a rede.
- *DA* – contém o endereço individual ou de um grupo que identifica uma entidade ou entidades *MAC* de destino final.

- *SA* – contém o endereço *MAC* da entidade que transmite uma mensagem ou fragmentos desta.
- *RA* – contém o endereço individual ou de um grupo que identifica a estação de destino imediata.
- *TA* – contém o endereço individual que identifica a estação transmissora dentro do próprio *BSS*.

O formato do quadro de controle é apresentado na Figura 2.9 [2] e a descrição de seus campos é mostrada logo a seguir.

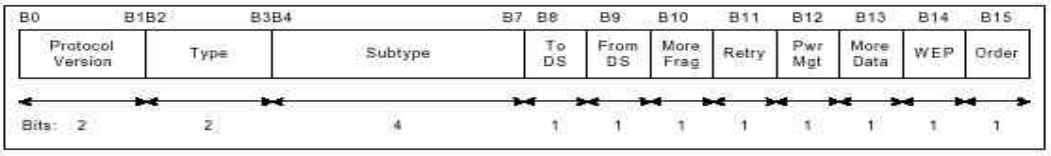


Figura 2.9 – *Formato do Quadro de Controle*

- *Protocol Version* – identifica a versão do protocolo de acesso ao meio, servindo para que os dispositivos destinatários de quadros com versão não suportada possam descartar estes quadros.
- *Type* e *subtype* – indicam os tipos de quadro (controle, dados ou gerenciamento) e os subtipos, como pedido de associação, *beacon* e outros que são mostrados na Tabela 2.2 [2].
- *To DS* – tem o valor 1 em quadros de dados destinados ao *AP* para serem enviados ao *DS* e 0 em outros quadros.
- *From DS* – tem o valor 1 em quadros de dados saindo do *AP* para a estação móvel e 0 em outros quadros.
- *More Fragments* – tem o valor 1 em quadros de dados ou gerenciamento que possuem outros fragmentos de mensagem e 0 em outros quadros.
- *Retry* – tem o valor 1 em quadros de dados ou gerenciamento que estão sendo retransmitidos e 0 em quadros que estejam sendo transmitidos pela primeira vez.
- *Power Management* – indica que a estação está no modo gerenciamento de potência. Se 1 a estação está economizando energia (*power-save*), se 0 a estação está ativa.
- *More Data* – indica para estação no modo *power-save* que o *AP* possui mais dados armazenados para ela.

- *WEP* – tem o valor 1 para qualquer tipo de quadro que contém uma mensagem ou fragmento processado pelo algoritmo *WEP* (*Wired Equivalent Privacy*).
- *Order* – tem o valor 1 para qualquer tipo de quadro que contém uma mensagem ou fragmento sendo transmitido entre estações que não suportem alteração na ordem dos quadros e 0 em outros tipos de quadros.

Tabela 2.2 - *Descrição dos Tipos e Subtipos de Quadros*

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

O formato do quadro *RTS* é apresentado na Figura 2.10 [2] e seus campos são descritos logo seguir.

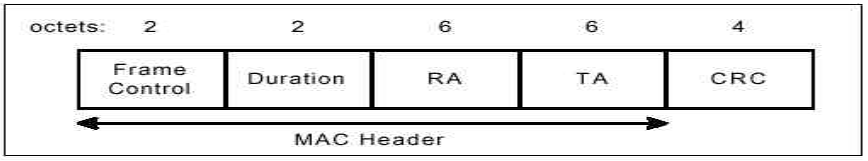


Figura 2.10 – *Formato do Quadro RTS*

RA (*Receiver Address*) – é o endereço da estação de destino no *BSS.*

TA (*Transmitter Address*) – é o endereço da estação transmitindo o quadro *RTS.*

Duration – é o valor do tempo em microssegundos (*ms*) necessário para transmitir o quadro de dados ou gerenciamento mais o tempo de um quadro *CTS*, um quadro *ACK* e três intervalos de tempo *SIFS.*

O formato do quadro *CTS* é apresentado na Figura 2.11 [2] e seus campos são descritos logo seguir.

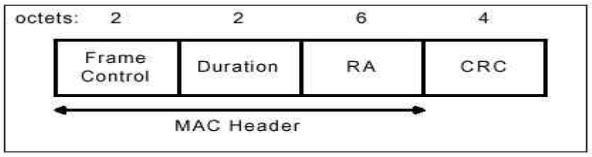


Figura 2.11 – *Formato do Quadro CTS*

RA – é o endereço *TA* do quadro *RTS* do qual o quadro *CTS* é a resposta.

Duration – este valor em microssegundos é obtido do campo *Duration* do quadro *RTS* imediatamente anterior, menos o tempo em microssegundos necessário para transmitir o quadro *CTS* e um intervalo de tempo *SIFS*.

O formato do quadro *ACK* é apresentado na Figura 2.12 [2] e seus campos são descritos logo seguir. Pode-se observar que o formato deste quadro corresponde ao do quadro *CTS*, sendo diferenciado pelo valor do campo *RA*.

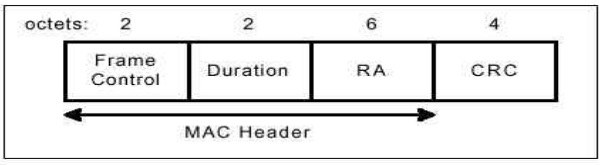


Figura 2.12 – *Formato do Quadro ACK*

RA – é o endereço (*address* 2) do quadro transmitido anteriormente.

Duration – é o valor do tempo em microssegundos necessário para transmitir o quadro de dados ou gerenciamento anterior, menos o tempo requerido para transmitir o quadro *ACK* e um intervalo de tempo *SIFS*.

2.2.3.4 – Fragmentação da Camada *MAC*

A fragmentação no nível da camada *MAC* é importante porque minimiza a probabilidade de erro devido ao enfraquecimento do sinal e ao ruído, pois quadros menores são transmitidos. A camada *MAC* provê suporte para a fragmentação de quadros em transmissão ponto-a-ponto e é responsável pela remontagem do quadro, o que acaba por tornar este processo transparente para as camadas superiores. O padrão obriga que todos os receptores tenham suporte a fragmentação, mas deixa como opcional a fragmentação nos transmissores [2]. Tanto a condição para se fragmentar um quadro quanto o tamanho máximo de um fragmento são dados por um

limiar de fragmentação (*FRAGMENTATIONthreshold*), ou seja, um quadro só será fragmentado se for maior do que esse limiar.

2.2.3.5 – Varredura (*Scanning*)

Esta função é necessária para que uma estação possa se juntar a um *BSS*, para inicialização e manutenção de uma rede *Ad-hoc* e para que uma estação possa encontrar um novo *AP* enquanto se desloca de um *BSS* para outro (*roaming*). Há dois tipos de varredura [3]:

- *Varredura Passiva* – estações ouvem quadros de gerenciamento (*beacons*) em cada canal e ao recebê-los armazenam o seu *timestamp*, *ESS-ID* e *BSS-ID*.
- *Varredura Ativa* – estações enviam uma consulta dentro de cada canal e esperam por resposta. As mesmas informações recebidas na varredura passiva são armazenadas.

2.2.3.6 – Associação

Após a varredura, a estação deve associar-se com um *AP*. A comunicação entre o *AP* e a estação ocorre da seguinte forma:

- Estação envia uma consulta (varredura ativa),
- *AP* envia resposta à consulta,
- Estação envia pedido de associação,
- *AP* envia resposta ao pedido.

A estação só poderá transmitir e receber dados após estar associada a um *AP*, isto já não será necessário para redes *Ad-hoc*, pois não necessitam de um ponto de acesso para se formarem [2].

2.2.3.7 – Autenticação

É um serviço muito importante em redes sem fio, pois trata da segurança das transmissões. Uma estação para fazer parte de um *BSS*, deverá se registrar junto ao *AP*, onde cada lado provê o reconhecimento de uma dada senha [2].

2.2.3.8 – Criptografia

É responsável por possibilitar confidencialidade aos dados, prevenindo o acesso aos dados por intrusos. A geração de dados criptografados basicamente é feita aplicando-se a um bloco de dados a operação boolena ou-exclusiva com uma seqüência chave pseudo-aleatória de igual comprimento. Esta seqüência chave é

gerada pelo algoritmo *WEP*, que é um algoritmo simétrico, ou seja, a mesma chave criptografa e descriptografa [2]. A idéia de se utilizar este algoritmo é aproximar a segurança das redes sem fio à de uma rede cabeada sem criptografia.

2.2.3.9 – Roaming

É o movimento de uma estação da área de cobertura de um *BSS* para a de outro sem que haja a perda de conexão [2].

2.2.3.10 – Sincronização

Garante que as estações associadas a um *AP* estejam sob um relógio comum. É implementada através do envio periódico de quadros de gerenciamento (*beacons*) carregando o valor do relógio do *AP*. No gerenciamento de potência, é utilizado para indicar o momento em que uma estação deve ligar o seu receptor para receber as mensagens armazenadas para ela [2].

2.2.3.11 – Gerenciamento de Potência

A necessidade das estações economizarem energia faz com que seus receptores não permaneçam sempre ligados. Para que seja possível o gerenciamento de potência é necessário que o *AP* armazene temporariamente quadros que estão endereçados às estações que se encontram poupando energia. O *AP* e as estações devem operar com seus relógios em sincronismo para que as estações possam ligar seus receptores no momento certo e receber quadros periodicamente [2].

2.3 - Os Grupos de Trabalho do Padrão IEEE 802.11

Adicionalmente ao padrão 802.11, outros padrões estão sendo desenvolvidos para aumentar as taxas de transmissão, melhorar a segurança, adicionar *QoS* ou mesmo prover interoperabilidade entre equipamentos de diferentes fabricantes. Muitos fabricantes estão oferecendo implementações destas características muito antes do *IEEE* (*Institute of Electrical and Electronics Engineers*) torná-las padrão. A seguir é apresentada uma breve descrição dos grupos de trabalho que buscam complementar a tecnologia IEEE 802.11 lançada em 1999 [4].

- **IEEE 802.11a** – padroniza a camada física na banda de 5 GHz. Especifica oito canais de rádio disponíveis e uma taxa máxima de transmissão de 54 Mbps por canal. Isto traz benefícios, como um maior *throughput* de dados e o maior

número de canais, o qual possibilita uma proteção melhor contra possíveis interferências de pontos de acesso vizinhos.

- **IEEE 802.11b** – padroniza a camada física na banda de 2,4 GHz, especificando três canais de rádio disponíveis. A taxa máxima de transmissão é de 11 Mbps por canal. No entanto, com o crescente número de usuários fazendo parte de redes sem fio ativas, o limite de três canais de rádio pode trazer interferência entre pontos de acesso vizinhos [4].
- **IEEE 802.11d** – realiza alterações na camada *MAC* 802.11 para promover o seu uso mundialmente, possibilitando que os *APs* se comuniquem em um canal de rádio permitido, com níveis de potência aceitáveis. Como o padrão 802.11 não pode operar legalmente em alguns países, a proposta do 802.11d é adicionar características e restrições necessárias para permitir que as *WLANs* consigam ampliar seus domínios e atingir novos países [4].
- **IEEE 802.11e** – vem complementar a camada *MAC* para prover suporte à qualidade de serviço em aplicações *LAN*. Será aplicado aos padrões físicos 802.11 a, b e g. A proposta é prover classes de serviço com níveis gerenciáveis de *QoS* para aplicações de dados, voz e vídeo. Este padrão deve prover algum mecanismo de diferenciação de tráfego para possibilitar a qualidade no serviço prestado pela rede [4].
- **IEEE 802.11f** – este documento visa alcançar interoperabilidade entre *APs* de diferentes fabricantes. Este padrão define o registro de pontos de acesso dentro de uma rede e a troca de informações entre *APs* quando uma estação sai de sua área de cobertura e vai para outra (*roaming*) [4].
- **IEEE 802.11g** – é um padrão para camada física na banda de 2,4 GHz e 5 GHz, onde são especificados três canais de rádio. A taxa máxima de transmissão é de 54 Mbps comparado com os 11 Mbps do 802.11b [4].
- **IEEE 802.11h** – padrão que vem complementar a camada *MAC* para obedecer as regulamentações Européias para *WLANs* na banda de 5 GHz, que exigem produtos com controle de potência e seleção de freqüência de forma dinâmica [4].

- **IEEE 802.11i** – padrão que complementa a camada *MAC*, visando a melhoria da segurança nos padrões a, b e g. Para isto é proposto uma alternativa para o *WEP* com novos métodos de criptografia e procedimentos de autenticação [4].
- **IEEE 802.11x** – propõe um sistema para regular o controle de acesso de estações à rede, fazendo o uso de métodos de autenticação mais complexos. Sendo aplicado aos padrões da camada física a, b e g [4].
- **IEEE 802.1p** – é um padrão para classes de tráfego e filtragem de *multicast* dinamicamente. Provê um método para diferenciar tráfego em classes de prioridade, oferecendo um suporte de *QoS*. É uma parte chave da proposta do 802.11e para a qualidade de serviço no nível da camada *MAC*, também sendo aplicado aos padrões da camada física a, b e g [4].

2.4 – Algumas Diferenças entre os Padrões 802.3 e 802.11

A primeira diferença que se observa está no meio de transmissão, que no caso do padrão para rede cabeada 802.3 [5] é um meio confinado, por exemplo, o par trançado (*10BASE-T*), e no 802.11 é via rádio, o que torna o sinal mais susceptível à interferências e também ao problema de alcance do sinal, o já citado terminal escondido (*Hidden Station*). Este problema ocorre quando uma estação "A" recebe sinal de "B", mas não de "C". A estação "C" recebe sinal de "B", mas não de "A". Então, por exemplo, a estação "A" não pode saber se "C" está em início de transmissão para "B", e também pode iniciar sua transmissão para "B", ocasionando colisões em "B". A Figura 2.13 ilustra este problema.

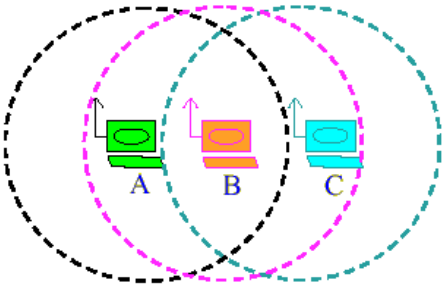


Figura 2.13 – *O Problema com Terminais Escondidos*

Com relação ao protocolo, existem diferenças nos métodos de acesso, pois o padrão 802.3 utiliza o *CSMA/CD* [5], enquanto o 802.11 faz uso do *CSMA/CA*. A principal diferença entre estes dois métodos de acesso é que no primeiro método

existe a possibilidade de se detectar a colisão enquanto se transmite, porém necessita-se de um transmissor *full-duplex*. Já no segundo método não se consegue detectar enquanto transmite, necessitando de um reconhecimento do receptor para informar a integridade dos dados. No entanto, o rádio utilizado poderá ser um *half-duplex*, que é mais barato e torna o produto mais acessível aos usuários.

Quanto a diferença entre os dois padrões no que se refere à gerência é muito grande, pois no padrão 802.11 as estações terão mobilidade e a quantidade destas estações não estarão limitadas a um barramento, mas sim pela área de cobertura de um *BSS*, onde a qualquer momento poderá estar entrando ou saindo uma estação, podendo comprometer a qualidade de serviço prestada pela rede e dificultando o seu gerenciamento. Além disso, existe a grande possibilidade da invasão de comandos de um gerente "falso" que se registra inadequadamente em um *BSS* ou mesmo um agente que envie parâmetros incorretos para o gerente, que geralmente está locado no *AP*. Isto ocorre devido ao fato da segurança nas redes sem fio ainda não estar satisfatoriamente resolvida, utilizando chaves de criptografia e mecanismos de autenticação mais robustos.

Capítulo III

3 – Visão Geral sobre Gerência de Redes *SNMP* e o Planejamento de Capacidade

3.1 – Gerência de Redes

A definição de Gerência de Redes depende do ponto de vista que se adota. Em alguns casos envolve constantes monitoramentos das atividades da rede utilizando um analisador de protocolo. Já em casos mais complexos há o envolvimento de uma base de dados distribuída e consultas aos dispositivos da rede, gerando gráficos em tempo real das mudanças ocorridas na topologia da rede e do seu tráfego. Em geral, o gerenciamento de rede é um serviço que emprega uma variedade de ferramentas, aplicações e dispositivos que ajudam no monitoramento e manutenção da rede.

De forma mais específica, a Gerência de Redes é encarada como uma coleção de atividades que são necessárias ao planejamento, organização, monitoramento, contabilização e controle das atividades e dos recursos da rede. O gerenciamento e o sistema de controle da rede consistem em uma coleção de técnicas, políticas e procedimentos que são integrados para permitir que os dispositivos da rede consigam realizar as suas funções. No centro do sistema encontra-se uma base de dados que possui vários arquivos no intuito de permitir ao Administrador da Rede o acesso às informações necessárias para o controle dos dispositivos gerenciados [10].

3.1.1 – Metas para o Gerenciamento

As principais metas de gerenciamento a serem alcançadas são resumidas nos tópicos seguintes [11]:

- **Maior disponibilidade dos recursos da rede**

O gerenciamento de rede visa garantir uma maior disponibilidade dos dispositivos sendo gerenciados, através do uso constante de monitoração de indicadores, como falhas e desempenho, e ajustes através da função de controle.

- **Redução dos custos operacionais da rede**

Vem sendo o principal motivo por trás da Gerência de Redes. Como a tecnologia muda rapidamente, é interessante ter um sistema de gerência que possa ser utilizado para gerenciar redes heterogêneas.

- **Redução do congestionamento**

A redução de gargalos na rede pode ser feita com a monitoração e ajustes dos componentes da rede, bem como na escolha do modelo de gerência, centralizado ou distribuído, de forma a se adequar melhor à rede.

- **Aumento da flexibilidade de operação e integração**

Tecnologias de rede estão mudando constantemente. Com a adoção de padronizações na gerência de redes é possível absorver tais tecnologias com custo mínimo. Por exemplo, a manipulação de impressoras em rede é muito comum, porém é desejável a integração de periféricos externos como copiadoras e máquinas de fax ao esquema de gerência.

- **Aumento da eficiência**

Em alguns casos, as metas de gerência de redes sobrepõem-se. Fica claro que a eficiência geral da rede é aumentada quando metas como redução do custo operacional, aumento da disponibilidade dos recursos da rede, entre outras, são alcançadas.

- **Facilidade de uso**

A interface final para o administrador da rede é crítica para o sucesso de uma plataforma de gerenciamento. A plataforma de gerência deve oferecer uma interface mais amigável possível, facilitando a análise dos dados coletados.

- **Segurança**

Algumas funções de gerenciamento precisam de características de segurança. Pode-se fornecer a segurança em dois níveis: no nível de computador e de rede. A segurança no nível de computador consiste da proteção das informações nos sistemas de softwares, enquanto no nível de rede fornece esquemas de segurança para as informações que trafegam na rede e para os nós sendo gerenciados.

3.1.2 – Recursos Gerenciados

O gerenciamento de redes de computadores envolve a monitoração e o controle de diferentes elementos de hardware e software, dentre os quais podem ser citados:

- Componentes de computadores, tais como dispositivos de armazenamentos, impressoras, etc.
- Componentes de interconexão e conectividade, tais como roteadores, concentradores (*hubs*), *switches*, *APs*, etc.
- Softwares de aplicação e ferramentas de desenvolvimento.

Do ponto de vista técnico, observa-se que as redes de computadores estão em constante expansão, tanto em abrangência física, como em complexidade. No entanto, para o usuário final, a rede é vista como algo simples, não importando os recursos que estão sendo gerenciados. Sendo assim, as redes de computadores devem estar disponíveis o tempo todo para auxiliá-lo a atingir objetivos como vendas, qualidade, rapidez e eficiência.

3.1.3 – As Áreas Funcionais da Gerência

De acordo com a *ISO* (*International Organization for Standardization*) são descritas cinco áreas de Gerência de Redes: Gerência de Falhas, Gerência de Contabilidade, Gerência de Configuração, Gerência de Desempenho e Gerência de Segurança [6] [10] [12] [13].

- **Gerência de Falhas**

O administrador da rede deve ser capaz de identificar e isolar o elemento sob condição de falha, além de reconfigurar a rede para que esta funcione enquanto os elementos atingidos estejam, o mais rápido possível, sendo reparados [13].

- **Gerência de Contabilidade**

É responsável por contabilizar a carga de utilização dos recursos da rede associada a cada usuário ou grupo de usuários, atribuindo valores pecuniários a essa utilização. Responde também pela imposição de limites de utilização dos recursos dependendo do perfil do usuário. Muitos de seus relatórios servem para auxiliar o planejamento do crescimento da rede [6].

- **Gerência de Configuração**

Tem a responsabilidade de obter, documentar e armazenar os parâmetros mais adequados ao funcionamento de cada um dos elementos de um sistema, bem como garantir a configuração ideal para um perfeito relacionamento entre elementos que funcionem de modo interdependentes. O início do funcionamento e o desligamento parcial ou total dos elementos da rede é a atividade de maior impacto realizada por esta área e que garante a sua operação com os parâmetros mais adequados [13].

- **Gerência de Desempenho**

A gerência de desempenho inclui o monitoramento e o controle de um aceitável nível desempenho da rede.

O monitoramento consiste em coletar informações tais como: utilização, tempo de resposta, taxa de erros, disponibilidade e perda de dados, comparando-as com os indicadores das condições normais e desejáveis de funcionamento dos recursos compartilhados.

Já o controle corresponde às ações no sentido de adequar as configurações e a capacidade da rede aos parâmetros de desempenho necessários, segundo informações obtidas no monitoramento.

O desempenho da rede é afetado por grande parte dos problemas relacionados às outras áreas da gerência. A gerência de desempenho deve ser praticada para as condições normais de operação da rede, avaliando o impacto dos indicadores de desempenho no funcionamento da mesma.

Uma das dificuldades no gerenciamento de rede está na escolha e utilização dos indicadores apropriados para medir o desempenho da rede. Na Tabela 3.1 são colocados alguns indicadores de desempenho e suas descrições.

Tabela 3.1 – *Indicadores de Desempenho de Rede*

	Orientado a Serviço
Disponibilidade	A percentagem do tempo que o sistema de rede, componente ou uma aplicação está disponível para o usuário.
Tempo de Resposta	Quanto tempo leva para a resposta aparecer no terminal do usuário depois que ele chama a aplicação.
Precisão	Percentagem do tempo sem ocorrência de erros na transmissão e recebimento da informação.
	Orientado a eficiência.
Vazão	Taxa que os eventos ocorrem (pacotes transmitidos, mensagens de transação, etc.).
Utilização	A percentagem da capacidade que está sendo usada.

Como se observa na Tabela 3.1, esses indicadores são divididos em duas categorias: indicadores orientados a serviço e indicadores orientados a eficiência. Os indicadores orientados a serviço estão relacionados com determinado nível de serviço para manter a satisfação do usuário da rede, e orientados a eficiência estão relacionados em manter esses níveis de serviço com baixo custo [6].

- Disponibilidade (*Availability*)

Disponibilidade pode ser expressa pela percentagem do tempo que o componente ou aplicação está disponível para um usuário. Está baseada na confiança dos elementos da rede. Confiança é a probabilidade de um componente desempenhar suas funções por um período de tempo e sobre determinadas condições. A falha de um elemento de rede pode ser expressa pelo tempo médio entre falhas (*mean time between failures* - *MTBF*). A disponibilidade, *A*, pode ser representada como [6]:

$$A = \frac{MTBF}{MTBF + MTTR},$$

onde *MTTR* (*mean time to repair*) é o tempo médio de reparo [6].

- Tempo de Resposta (*Response Time*)

É o tempo que o sistema leva para reagir a uma determinada entrada. Em uma transação interativa, pode ser definida como o tempo entre a última tecla digitada pelo usuário e o início do resultado mostrado pelo computador [6]. Outra medida que está embutida no tempo de resposta é o atraso fim-a-fim. Esta medida é mais fácil de ser obtida, já que não leva em conta, por exemplo, o tempo de processamento no servidor.

Obviamente, deseja-se que o tempo de resposta para qualquer aplicação seja curto. Entretanto, baixos valores de tempo de resposta geram um custo elevado.

- Precisão (*Accurancy*)

Uma transmissão precisa de dados entre computadores é essencial para qualquer rede. Por causa dos mecanismos de correção de erro em protocolos como os de enlace e transporte, precisão não é uma preocupação do usuário. Entretanto, é útil monitorar a taxa de erros, pois pode indicar uma falha intermitente na linha devido a uma fonte de ruído ou interferência a ser corrigida [6].

- Vazão (*Throughput*)

Vazão é uma medida orientada à aplicação. Alguns exemplos:

⇒ Número de transações de um dado tipo em um certo tempo;

⇒ Número de clientes de uma aplicação durante um certo tempo;

⇒ Número de chamadas para um ambiente de chaveamento de circuitos.

É útil verificar estas medidas no tempo para prever projetos de demanda e problemas de desempenho [6].

♦ Utilização (*Utilization*)

É uma medida mais simples que a vazão. Ela é responsável pela determinação da percentagem de uso do recurso.

Talvez o maior uso da Utilização seja na medição de gargalos, tornando possível a identificação das áreas de congestionamento. Isto é importante porque o tempo de resposta aumenta exponencialmente com o crescimento da utilização dos recursos da rede. Por causa desse comportamento exponencial, o congestionamento pode sair do controle se não for localizado e tratado rapidamente [6].

Ainda neste capítulo será apresentado um estudo maior sobre a Gerência de Desempenho e suas principais atividades, a qual será o foco da metodologia proposta no Capítulo 4.

- **Gerência de Segurança**

Neste caso a preocupação é com a integridade, autenticidade, disponibilidade e a confidencialidade das informações e recursos de uma rede. Além disso, promove o controle e o registro de acesso aos recursos e informações considerados importantes ou confidenciais em uma rede [6].

3.1.4 – Gerência Pró-ativa X Gerência Reativa

Um conceito importante na Gerência de Redes é a distinção entre gerência pró-ativa e gerência reativa. A gerência reativa é aquela onde o Administrador da Rede limita-se a reagir aos problemas que surgem. Utiliza-se de padrões e ferramentas de gerência para ser alertado de um problema, momento em que reage e passa a identificar as causas e soluções do mesmo.

A gerência pró-ativa é aquela onde o Administrador da Rede procura, rotineiramente, por informações que possam revelar com antecedência a possibilidade de um problema na rede. Essa forma de gerência concentra seus esforços nos estudos dos avisos (*warning*s), que são registros da ocorrência de uma situação anormal, porém não crítica. Também utiliza históricos, estatísticas e o

monitoramento freqüente dos eventos relevantes da rede, acompanhando sua mudança de comportamento.

A gerência pró-ativa é mais difícil de ser efetuada que a reativa. Entretanto, resulta em tempos menores de parada e economia geral de operação da rede.

3.1.5 – Sistemas de Gerência Centralizada X Distribuída

Normalmente são encontradas redes sendo gerenciadas por sistemas centralizados de gerenciamento que controlam uma quantidade potencialmente grande de elementos de redes através da manipulação dos agentes. Esses agentes possuem características predefinidas e fixas, como é o caso dos agentes *SNMP*. Tais sistemas de gerenciamento centralizado são na verdade inadequados para as grandes redes multi-serviço atuais e futuras.

Comparando os dois sistemas de gerenciamento, tem-se que o centralizado não consegue ser escalável para redes grandes. Esta desvantagem é bastante importante, pois com o aumento crescente das redes, a carga no gerente central pode aumentar a um ponto que já não seja mais possível gerenciar os agentes. O problema da escalabilidade fica ainda maior quando uma condição de erro é estabelecida, já que o gerente central deve iniciar e coordenar cada passo do procedimento de recuperação da rede a seu estado normal.

Outro problema do gerenciamento centralizado é a sua falta de flexibilidade, já que as funções de gerenciamento e características dos agentes são normalmente limitadas. Além destas desvantagens apresentadas, o gerenciamento centralizado apresenta um ponto de falha do sistema de gerência único, ou seja, se falhar a estação gerente, a rede fica toda prejudicada.

Na gerência distribuída, o gerente é uma aplicação que age no papel de gerente propriamente dito, realizando as tarefas de gerenciamento, e no papel de agente, de forma que ele possa ser controlado e monitorado remotamente, havendo a delegação de controle de uma estação de gerência para outra.

O sistema distribuído oferece alguns benefícios [6]:

- Diminuição do tráfego de gerenciamento, que se mantém local;
- Oferece escalabilidade;
- O uso de várias estações de gerência elimina o ponto único de falha dos sistemas centralizados.

Outra vantagem do sistema distribuído de gerência é que uma estação de gerenciamento pode ser configurada para realizar tarefas de gerenciamento mesmo quando a comunicação com a estação central de gerência for impossível ou deficiente. Portanto, mesmo em momentos em que a troca de informações entre as estações esteja comprometida, as operações de gerência de rede podem continuar sendo gerenciadas. A Figura 3.1 a seguir ilustra uma rede com gerência distribuída e várias tecnologias de rede.

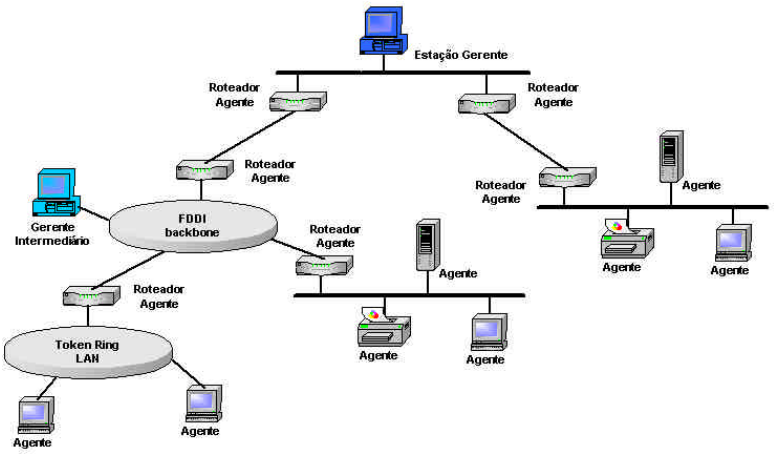


Figura 3.1 – *Configuração de um Gerenciamento de Rede Distribuído*

Na Figura 3.1 observa-se, como citado anteriormente, um gerente intermediário, que estará fazendo o papel de gerente para as estações que possuem agentes e estão sob a sua responsabilidade. No entanto, quando estiver no papel de agente, estará sendo controlado e monitorado pelo gerente responsável por toda a rede.

3.2 – Breve Histórico sobre o Protocolo de Gerência *SNMP*

Da criação de uma das primeiras redes de comutação de pacotes, a *ARPANET* (*Advanced Research Projects Agency NET*) [5], a uma rápida evolução em seu tamanho, pouco tempo se passou, indo de dezenas de computadores interligados para centenas e depois milhares, esta rede se transformou na Internet. Com diversos *backbones*, *gateways* e operadores, logo surgiu a necessidade de ferramentas para gerenciar esta rede. Documentos padronizados pelo *IETF*, como as *RFCs* (*Request For Comments*) 1028 e 1067, foram criados na tentativa de definir ferramentas baseadas no protocolo *SGMP* e *SNMP*, porém eles tiveram vida curta. Na *RFC* 1157 publicada em maio de 1990 fez-se uma definição da versão 1 do *SNMP* e com a *RFC*

1155, que trata de informações de gerenciamento, o *SNMP* passou a ter ampla aceitação comercial, se tornando um padrão de fato para o gerenciamento de redes baseado no *TCP/IP* [12].

Com o uso do *SNMPv.1*, as suas deficiências começaram a ser percebidas, e logo uma versão 2, mais aprimorada, foi definida nas *RFCs* 1441 a 1452 [14], sendo reafirmadas nas especificações atuais, *RFCs* 1902 a 1908 [12]. Esta versão tornou o *SNMP* bastante conhecido, porém ainda com falhas nas áreas de segurança, autenticação e privacidade. A busca para resolver estes problemas fez surgir a versão mais atual do *SNMP*, a versão 3.

3.2.1 – A Arquitetura *SNMP*

No modelo de arquitetura *SNMP* usado para redes *TCP/IP*, são apresentados quatro elementos chave: estação gerente, agentes de monitoramento, base de informação gerencial e o protocolo de gerenciamento. Este último é o responsável pela comunicação entre o agente e o gerente [15].

A estação gerente é tipicamente uma máquina na rede que deve possuir um conjunto de aplicações para análise das informações obtidas dos agentes, um banco de dados extraído das *MIBs* de todas as entidades gerenciáveis da rede, a capacidade de solicitar e alterar dados dos elementos da rede e uma interface para que o gerente possa, de fato, monitorar e controlar o processo de gerenciamento [15].

Os agentes de monitoramento são softwares capazes de responder às solicitações do gerente, bem como de informá-lo quando algo errado ocorrer no dispositivo. O agente pode estar localizado nos próprios elementos de rede, como roteadores e servidores; ou pode ser colocado em algum componente que monitora os elementos de rede.

A solicitação do gerente e resposta do agente, também conhecida como pedido (*request*) e resposta (*response*), caracterizam o *polling*. Uma outra operação muito importante é a notificação (*Event Report*), na qual o agente, periodicamente fornece um relatório ao gerente sobre sua situação atual [15].

A *MIB* é uma base de dados lógica que armazena, dentro de sua classe, os atributos de cada objeto que são característicos do comportamento do nó gerenciado da rede [12].

A Figura 3.2 mostra alguns dispositivos gerenciáveis na arquitetura *SNMP* [6].

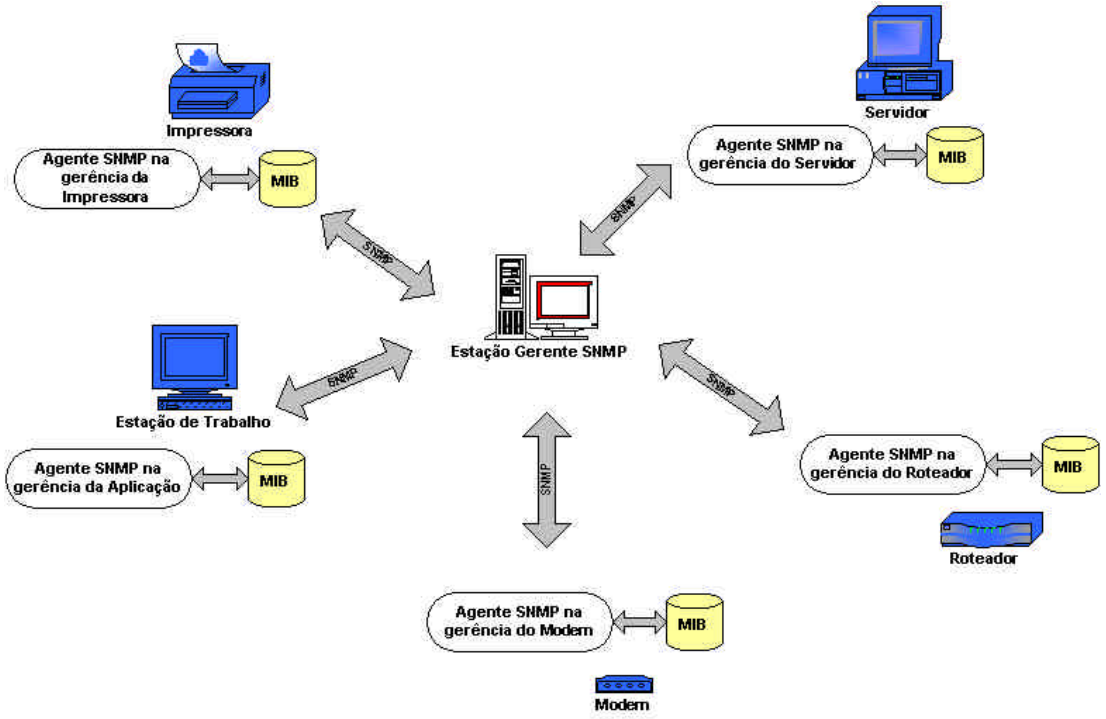


Figura 3.2 – *Exemplo de Rede Gerenciada Segundo Arquitetura SNMP*

Pode-se observar na Figura 3.2 que cabe à estação gerente fazer a coleta de dados de cada elemento gerenciado por intermédio do agente correspondente. O protocolo *SNMP* é então responsável pelo transporte das informações de gerenciamento entre o gerente e os agentes existentes nos elementos de rede, confirmando o que já havia sido descrito anteriormente.

O *SNMP* é um protocolo da camada de aplicação que opera sobre o protocolo da camada de transporte não orientado à conexão (*User Datagram Protocol - UDP*), o qual não garante a entrega da mensagem recebida. Cada agente deve implementar *SNMP*, *UDP* e *IP*, ou ainda, implementar o protocolo orientado à conexão (*Transmission Control Protocol – TCP*) para outras aplicações como transferências de arquivos (*File Transfer Protocol – FTP*) e um protocolo dependente do tipo de rede, como por exemplo: Ethernet, *FDDI* (*Fiber Distributed Data Interface*) e X.25 [15].

A Figura 3.3 mostra o contexto do protocolo *SNMP* organizado em camadas, com as operações oferecidas pelo mesmo e que são descritas na seção seguinte.

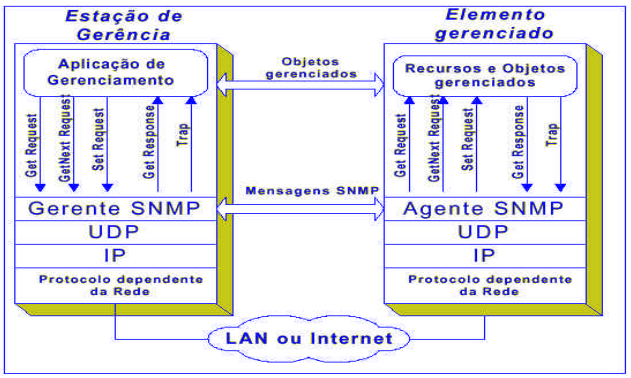


Figura 3.3 – *Protocolo SNMP sobre a Camada de Transporte*

3.2.2 – Descrição das Operações Disponíveis no Protocolo *SNMP*

No protocolo *SNMP*, as operações são consideradas atômicas, isto é, cada operação requisitada deve ser executada sobre todos os objetos citados na operação, caso contrário nada é feito. Não existem execuções parciais de um pedido. Se ocorrer algum erro durante a execução de uma operação, os resultados produzidos por esta operação serão ignorados e os indicadores de erro ajustados adequadamente [15].

Um cliente *SNMP*, ou seja, o gerente no caso das mensagens *get*, *get-Next* e *set*, deve construir e enviar o seu pedido ao servidor, ou seja, o agente. O gerente deve, então, esperar pela resposta de seu pedido e verificar se a resposta está de acordo com o esperado. Devido ao fato do protocolo de transporte *UDP* não garantir a entrega dos pacotes, o cliente deve implementar estratégias para saber que o pacote transmitido não foi recebido (*timeout*) e para retransmissão das mensagens que contém os pedidos [15].

As operações utilizadas pelo *SNMP* são mostradas a seguir:

- A operação *set-Request* é usada pelo agente para alterar um ou mais atributos de um objeto gerenciado.
- A operação *get-Request* é usada pelo agente para pedir o valor de um ou mais atributos de um objeto gerenciado.
- A operação *get-Response* é a resposta ou confirmação do agente às mensagens anteriores.
- A operação *get-NextRequest*, além de especificar o nome do objeto a acessar, também é utilizada para descobrir qual o próximo objeto na seqüência léxica e os valores dos seus atributos.

- A operação *trap* [6] é usada para informar a ocorrência de eventos, permitindo aos agentes *SNMP* enviarem informações para os gerentes sempre que ocorrer algum evento que origine alterações nos atributos dos objetos.

O padrão ainda especifica que todas as mensagens *SNMP*, com exceção da *trap*, deverão ser encaminhadas à entidade de destino em questão pela porta definida com o número 161 [14]. As notificações (*traps*) devem ser enviadas à porta número 162 do gerente, como se observa na Figura 3.4.

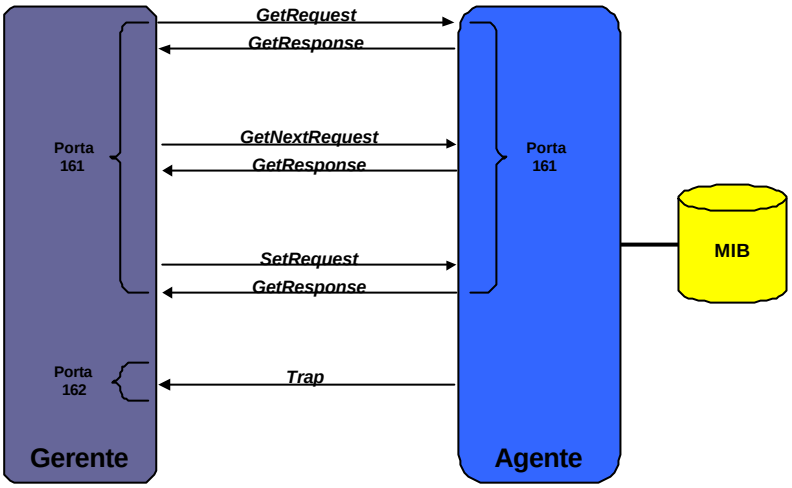


Figura 3.4 – *Operações do Protocolo SNMP*

3.2.3 – O Formato das Mensagens *SNMP*

Cada mensagem inclui o número da versão do *SNMP*, um nome de comunidade e um dos cinco tipos de unidades de dados do protocolo (*Protocol Data Unit - PDU*), como mostrado na Figura 3.5. Logo a seguir é colocado o significado de cada campo da mensagem do protocolo [6] [12] [16].

Version	Community	SNMP PDUs

(A) Mensagem SNMP

PDU type	Request-Id	0	0	variable bindings

(B) PDU das mensagens de GetRequest, GetNextRequest e SetRequest

PDU type	Request-Id	Error-status	Error-index	variable bindings

(C) PDU da mensagem GetResponse

PDU type	Enterprise	Agent addr	Generic trap	Specific trap	Time stamp	variable bindings

(D) PDU das mensagens de TRAP

Name 1	Value 1	Name 2	Value 2	…	Name N	Value N

(A) variable bindings

Figura 3.5 – *Formato das Mensagens e PDUs do SNMP*

- *Version* – versão do *SNMP*, a versão definida pela *RFC* 1157 é 1, no entanto, o valor do campo *version* por definição é 0 (zero).
- *Community* – nome da comunidade de modo a identificar o gerente para o agente.
- *PDU type* - o nome de uma das cinco mensagens definidas no *SNMPv.1*.
- *Request-Id* – é um número de seqüência inteira que permite associar os pedidos com as respectivas respostas e também o controle de fluxo das mensagens por parte de quem as envia (gerente).
- *Error-status* - é um número inteiro de 0 a 5 usado pelo agente para indicar condições de erro nas respostas geradas (*get-Response*).
- *Error-index* – é um número inteiro que indica em qual dos objetos ocorreu o erro, apontando-o na lista de objetos e valores do próximo campo da mensagem.
- *Variable-bindings* – é o campo mais importante, uma vez que ele comporta a carga útil (*payload*) ou a *VBL* (*Variable Binding List*), que são as variáveis *SNMP* identificadas por uma seqüência de números (*object identifier - OID*) e seus valores associados. Tais variáveis (*Variable-bindings*) são as informações que os gerentes lêem, escrevem e relatam.
- *Enterprise* – tipo de objeto que gerou a *trap*. Este valor é um objeto na *MIB*, normalmente o objeto *sysObjectID* do grupo *System*.
- *Agent-addr* ou *Network address* - possui o endereço *IP* do agente que enviou a mensagem de *trap*.
- *Generic-trap* – é um número inteiro que representa qual o tipo da *trap*. Os tipos padrões estão descritos na *RFC* 1157.
- *Specific-trap* – é um número inteiro que representa um tipo de *trap* especificada pelo fabricante do equipamento. Este campo permite que se definam mais opções para uma *trap*.
- *Time-stamp* – contém o valor do objeto *sysUpTime*, ou seja, é o tempo desde a última reinicialização da entidade de rede e da geração da *trap*.

3.2.4 – A Estrutura da Informação de Gerência

Os objetos da *MIB SNMP* foram organizados em uma estrutura de armazenamento do tipo árvore, chamada de *SMI* (*Structured Management Information*) [17], facilitando a identificação de cada um deles.

A informação de gerência é vista como uma coleção de objetos gerenciáveis, residentes num reservatório virtual de informações, a já citada *MIB*. A coleção de objetos relacionados é descrita em módulos de *MIB* de acordo com uma versão simplificada da linguagem utilizada para a definição de dados *ASN.1* (*Abstract Syntax Notation One*), padronizada pela norma *ISO*. A maneira como os dados são codificados em octetos para efeito de transmissão obedece às regras básicas de codificação *BER* (*Basic Encoding Rules*) e também constitui uma padronização *ISO*. Tais regras descrevem, de modo único, a forma como os dados devem transitar na rede, qualquer que seja o dispositivo ou tecnologia utilizada [5] [6] [18].

Segundo a *ASN.1* [5], cada objeto na *MIB* possui 3 atributos principais que o descrevem [6]:

- Nome do objeto (identificador): é uma seqüência de números inteiros separados por pontos, onde cada número é um identificador numa árvore hierárquica que serve para a classificação de objetos de redes. Esta árvore é, portanto, a estrutura de informação que contém todos os objetos existentes.
- Sintaxe do objeto: é o elemento que especifica o tipo de dados *ASN.1*, seu modo de acesso, seu *status* e seu nome descritivo, com as seguintes características:
    - Tipo de dado *ASN.1* pode ser inteiro (*Integer*), uma seqüência de octetos (*Octet String*), um identificador de objeto (*Object Identifier*) ou nulo (*Null*). Pode ser também uma sintaxe de aplicação (*Application Syntax*), podendo ser esta, um endereço de rede (*Network Adddress*), um contador (*Counter*), uma medida (*Gauge*), um intervalo de tempo (*Time-Ticks*) ou incompreensível (*Opaque*), além de um outro tipo de aplicação [12].
    - Modo de acesso: leitura (*read-only*), leitura e escrita (*read-write*), escrita (*write-only*) ou sem acesso (*not-acessible*).
    - *Status*: obrigatório, opcional ou obsoleto.
    - Nome textual: nome em caracteres para tornar a identificação do objeto mais legível.
- Codificação do objeto: formato de transmissão do objeto, segundo as regras *BER*, para todas as operações *SNMP*.

A *SMI* define algumas macro-instruções *ASN.1* com a finalidade de garantir a consistência da sintaxe e a semântica das definições *SNMP*. A declaração de um

objeto na *MIB*, por exemplo, é feita pela macro *OBJECT-TYPE*. O exemplo a seguir ilustra a utilização da macro *OBJECT-TYPE* para declaração do objeto *sysUptime*, que representa o tempo desde a última reinicialização de um elemento gerenciado. Este objeto pertence ao grupo *System*, que é o módulo contendo um grupo de objetos para identificação de um elemento ou sistema gerenciado [6] [18]:

sysUptime OBJECT-TYPE
SYNTAX Time-Ticks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"*The time (in hundredths of a second) since the network management portion of the system was last re-initialized.*"
::= { system 3 }

A sintaxe do objeto é definida pelas informações declaradas em cada uma das cláusulas da macro, assim especificadas [6]:

- *Descritor*: é a cadeia de caracteres (*string*) descritiva, contendo o nome textual do objeto. Vale lembrar que o identificador do objeto é a notação numérica separada por pontos que representa o objeto na árvore da *MIB*.
- *Sintaxe*: é a definição *ASN.1* do tipo de dado deste objeto.
- *Acesso*: é o mínimo grau de acesso que deve ser implementado para este objeto. As opções para este campo já foram descritas anteriormente.
- *Status*: é o estado de implementação atual do objeto. Esta situação pode mudar com a evolução da *MIB*. As opções são: *mandatory* (deve ser implementado), *optional* (pode ser implementado), *obsolete* (não precisa mais ser implementado) e deprecated (a informação apresentada por este objeto é redundante, mas ele ainda é obrigatório).
- *Descrição*: é um texto explicativo do objeto que visa esclarecer o que ele representa e como funciona. Deve estar entre aspas.

Um objeto na estrutura em árvore é referenciado por um identificador único composto de uma seqüência destes números separados por pontos, recebendo o nome de ordenamento lexicográfico. A Figura 3.6 ilustra esta organização, exemplificando a localização dos objetos do grupo *System* (1.3.6.1.2.1.1) na árvore da *MIB-II*.

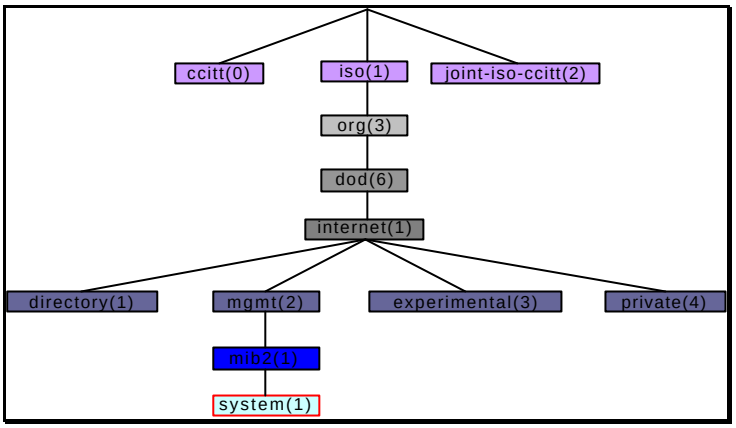


Figura 3.6 – *Exemplo da Localização de Objeto na Árvore da MIB-II*

3.2.5 – A Base de Informações de Gerência *SNMP*

A *MIB* é uma coleção estruturada de objetos gerenciados. Estes objetos representam os recursos sujeitos ao gerenciamento. Cada dispositivo gerenciável do sistema mantém uma *MIB* que reflete o estado dos seus recursos gerenciáveis. Uma entidade de gerenciamento pode monitorar os recursos de um dispositivo, lendo os valores dos objetos na *MIB* e pode controlar os seus recursos, modificando estes valores.

Como resultado da evolução da *MIB-I*, surgiu a *RFC* 1213, que define os objetos para a *MIB* padrão *SNMP* chamada de *MIB-II*. Esta *MIB*, total ou parcialmente, é implementada em produtos comerciais. Acréscimos podem ser feitos adicionando-se novos módulos da *MIB* utilizando novas padronizações definidas em *RFCs* pelos grupos de trabalho do *IETF* ou mesmo objetos proprietários criados por um determinado fabricante. Estes novos objetos são concatenados nas suas devidas posições na árvore, sem alterar de maneira nenhuma os objetos já existentes. Os objetos nunca são redefinidos, mesmo se um objeto for declarado obsoleto pelo *IETF*, sua identificação na árvore permanece.

Cabe observar que um determinado agente pode ter um conjunto de objetos que na verdade é uma parte do universo da *MIB* descrita na *RFC*. O que deve ser realmente implementado num agente são as informações pertinentes ao seu funcionamento e estado.

Inúmeras novas *MIBs* foram padronizadas para necessidades específicas de tecnologias emergentes. Assim, uma *MIB* pode conter exatamente os objetos de

interesse para um determinado equipamento ou componente da rede, tornando os dados um reflexo da realidade gerencial. A seguir são descritas duas *MIBs* especiais:

- As *MIBs* experimentais são aquelas que estão em fase de testes, com a perspectiva de serem adicionadas ao padrão e que, em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.
- As *MIBs* proprietárias são específicas dos equipamentos gerenciados, possibilitando que detalhes particulares a um determinado equipamento possam ser obtidos. É desta forma que é possível obter informações sobre colisões, configuração e várias outras de um roteador, por exemplo. Também é possível fazer um teste, desabilitar uma ou mais portas de um *hub* ou de um *switch* utilizando as *MIBs* proprietárias. Elas fazem parte da *MIB* estendida [6].

Deve-se notar que a informação de gerenciamento possui suas próprias regras de definição, o que torna as *MIBs* reservatórios de informações completamente desvinculados do protocolo de gerência. No princípio da definição do *SNMP*, pretendia-se facilitar a migração da infra-estrutura de informações de gerência do protocolo *SNMP* para um protocolo de gerência *OSI* [12] [15]. O tempo mostrou que isto não iria acontecer, mas esta aproximação facilitou a evolução da documentação da versão inicial do *SNMP* para as novas versões.

3.2.6 – A *MIB-II*

A *MIB-II* [18] define uma segunda versão da base de informação gerencial, sendo esta versão um grande conjunto da *MIB-I*, com alguns grupos e objetos adicionais [6].

Para que um objeto seja incluído na estrutura da *MIB-II*, este deve seguir alguns critérios. O objeto deve ser fundamental para a gerência de configuração ou para a gerência de falhas. Devido a problemas de segurança somente objetos que provoquem prejuízo limitado na rede, em caso de se alterá-los, são permitidos. Evidências de uso corrente e utilização são necessários. Estes objetos não podem derivar-se de outros, para que não haja redundância de variáveis. A implementação específica de objetos não é mais permitida, bem como pesadas seções de código devem ser evitadas [6].

A descrição dos grupos definidos na *MIB-II* é apresentada a seguir, e na Figura 3.7 são ilustradas as localizações desses grupos [6] [12] [14].

- *System*: grupo que armazena as informações do dispositivo gerenciável. Seus principais objetos são: nome, local, contato, tempo de atividade e serviços prestados.
- *Interfaces*: grupo que armazena dados sobre as interfaces de rede. Cada interface ganha um número e tem seus dados armazenados em objetos independentes. Os principais objetos são: octetos de entrada/saída, pacotes *unicast* de entrada/saída, erros de entrada/saída, descartes de pacotes de entrada/saída e velocidade de transmissão.
- *AT*: grupo que contém a tabela de associação entre endereços físicos e endereços de rede.
- *IP*: grupo responsável por armazenar objetos relativos ao protocolo *IP*, como números de pacotes descartados e razões, estatísticas sobre fragmentação e remontagem.
- *ICMP*: grupo que armazena as ocorrências de mensagens *ICMP* (*Internet Control Message Protocol*), como quantas mensagens foram enviadas.
- *TCP*: registra as estatísticas relativas ao protocolo *TCP*, como as conexões abertas, segmentos enviados e recebidos e estatísticas de erros.
- *UDP*: registra as estatísticas relativas ao protocolo *UDP*, como número de *datagramas* enviados, recebidos, os que foram recebidos com erro e as razões.
- *EGP*: registra as estatísticas relativas ao protocolo *EGP*, como informações sobre quantos pacotes saíram e quantos foram entregues corretamente.
- *Transmission*: na realidade, não é um grupo com um todo, mas simplesmente um nó na hierarquia da *MIB-II* que contém vários grupos específicos de interface. Enquanto o grupo *Interfaces* possui informações genéricas aplicáveis a todas as interfaces, estas *MIBs* específicas de interfaces possuem informações que relatam um tipo específico de rede. Um exemplo é a *MIB EtherLike* (*RFC* 1643).
- *SNMP*: registra as estatísticas relativas ao protocolo *SNMP*, como número de mensagens enviadas e tipos de mensagens.

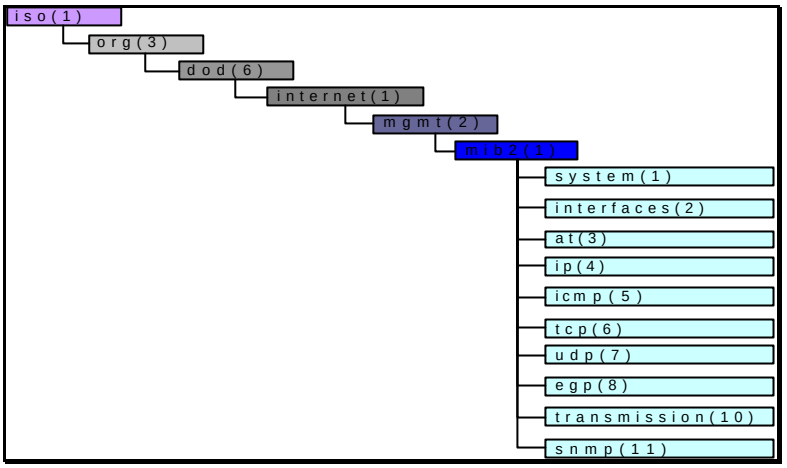


Figura 3.7 – *Grupos de Objetos da MIB-II na Árvore*

3.2.7 – O Grupo *System*

Como visto anteriormente, existem vários grupos da *MIB-II*, no entanto, aqui é descrito com mais detalhe o grupo *System*, que fornece informações sobre o dispositivo gerenciado, como se observa na Figura 3.8. Porém a descrição dos demais grupos é encontrada na *RFC* 1213.

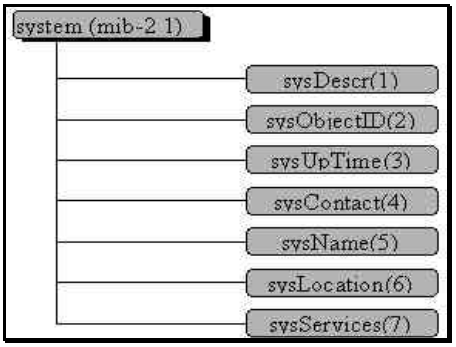


Figura 3.8 - *Grupo System da MIB-II*

Objetos do grupo *System*:

- *sysDescr* – fornece uma descrição da entidade, como tipo de hardware, sistema operacional e tipo de software de rede.
- *sysObjectID* – identificação autorizada do fornecedor do produto.
- *sysUpTime* – tempo desde a última reinicialização em centésimos de segundo.
- *sysContact* – contato da pessoa responsável pelo sistema.
- *sysName* – nome designado pela administração do sistema.
- *sysLocation* – localização física do equipamento.
- *sysServices* – informa o conjunto de serviços oferecido pelo equipamento.

3.2.8 – *SNMPv.2*

A necessidade de melhorias do *SNMPv.1* ultrapassava o compartimento usando módulos de *MIB*. Com isto, os engenheiros de redes de computadores descobriram a necessidade de mais funcionalidades do que aquelas que eram fornecidas a partir de extensões da *MIB*. Além disso, havia um desejo de que fosse adicionado ao padrão *SNMP* uma maior segurança no processo de gerenciamento. Sendo assim, o *IETF* formou dois grupos de trabalho: um grupo para desenvolvimento do *SNMP* versão 2 e outro para sua segurança.

Na realidade, o *SNMPv.2* não é um novo padrão, mas sim uma extensão ao *SNMPv.1* projetado para adicionar funcionalidade e segurança. Existe um bom número de vantagens específicas que emergiram do esforço de padronização no *SNMPv.2*, como [12]:

- A tradição oral em torno do *SNMP* original é agora completamente documentada. A importância deste esforço histórico não pode ser subestimada, pois ela fornece base para mudanças com coesão e bem planejadas no padrão *SNMP* existente à medida que o gerenciamento de rede continua a evoluir.
- Extensões úteis têm sido feitas na linguagem existente para definir objetos gerenciados. Dessa forma, tem se tornado mais fácil escrever, entender e implementar os dispositivos gerenciados.
- Mudanças de desempenho e outras melhorias também têm sido feitas no protocolo *SNMP* para fazer com que a troca de objetos gerenciados se torne mais eficiente.
- Passou a existir um melhor mecanismo de comunidade que apresenta uma identificação única tanto da origem quanto do formato da mensagem *SNMPv.2*, permitindo utilizar métodos de acesso mais convencionais aos objetos gerenciados, além de permitir o uso futuro de protocolos assimétricos de segurança.

A pilha de transporte necessária para executar softwares baseados no protocolo *SNMP* sempre foi o *UDP*. Nesta nova versão esta característica ficou mais flexível, onde outras pilhas de protocolos podem ser usadas. Entre as possibilidades de configuração de transporte *SNMPv.2*, estão [12]:

- Protocolos de transporte *OSI* [19]

- *Appletalk* – protocolo usado por máquinas *macintosh* [20]
- *IPX* – usado pelas redes *NOVELL* [21]

No que diz respeito ao protocolo, houveram mudanças substanciais. O conjunto de operações sofreu alterações e adições comparativamente à versão 1 [22], possibilitando a comunicação sólida, inclusive entre gerentes.

As seguintes alterações no conjunto de operações refletem estas preocupações [6] [12] [22]:

- *Get-Request*: não existe mais a perda da resposta toda, caso seja problemático obter o valor de apenas uma das variáveis. Se ocorrer problema na obtenção de um valor específico, o campo daquela variável é preenchido com códigos de erro.
- *Get-NextRequest*: se um pedido de *get-Next* ultrapassar o tamanho da *MIB*, o valor da variável será preenchido com o código *endOfMIBView* [6] e o *status* de erro será também o correspondente a sucesso (zero), ao contrário do que era feito antes na versão 1, que entendia a mensagem do fim da *MIB* como um erro.
- *Set-Request*: a operação de *set* é executada em duas fases: na primeira, as variáveis são testadas e na segunda, elas são propriamente "setadas". Caso alguma delas não passe no teste, toda a operação falha. Esta operação, como no *SNMPv.1*, continuou funcionando de forma atômica (tudo ou nada).
- *Response*: é o novo nome da operação *get-Response*.
- *SNMPv.2 - trap*: o formato das *traps* foi modificado para ficar semelhante ao usado em operações de *get* e *set*. Os campos especiais de *enterprise*, *agent-addr*, *generic-trap*, *specific-trap* e *time-stamp* foram eliminados e toda informação necessária é inserida no campo de variáveis da mensagem. Esta informação contém o nome da *trap* e o tempo de *sysUptime*, além da lista de variáveis definida para cada *trap* específica.

Além das alterações citadas anteriormente, o *SNMPv.2* adiciona dois novos tipos de operações ao protocolo. As mensagens denominadas *get-BulkRequest* e *inform-Request* permitem um aumento das funcionalidades dos agentes e gerentes e também a coleta de grandes quantidades de dados.

A nova mensagem *inform-Request* permite a um gerente enviar, de forma assíncrona, uma notificação de algum evento a outro gerente, algo análogo à mensagem *trap* só que entre gerentes. A diferença com relação à *trap* é que o *inform-*

Request é um serviço confirmado pelo gerente que recebe a mensagem. Isto quer dizer que é necessário o envio de uma mensagem *response* para o gerente que originou o *inform*. Esta nova possibilidade permite a hierarquização da estrutura gerencial do *SNMPv.2*, de forma que estações gerenciadoras locais enviem informações a uma estação gerenciadora central, como mostra a Figura 3.9.

Figura 3.9 – *Comunicação Hierarquizada entre Gerentes*

Já a nova mensagem chamada *get-BulkRequest* possibilita a recuperação de um volume considerável de variáveis, principalmente em relação à recuperação de entradas de tabelas. O pedido pode ser de variáveis individuais ou de linhas de uma tabela. A diferença entre as operações *get-BulkRequest* e *get-NextRequest* está na capacidade da primeira enviar linhas inteiras de uma tabela, além de "navegar" na *MIB* de forma seqüencial exatamente como *get-Next*. As operações possíveis do protocolo *SNMPv.2* são ilustradas na Figura 3.10.

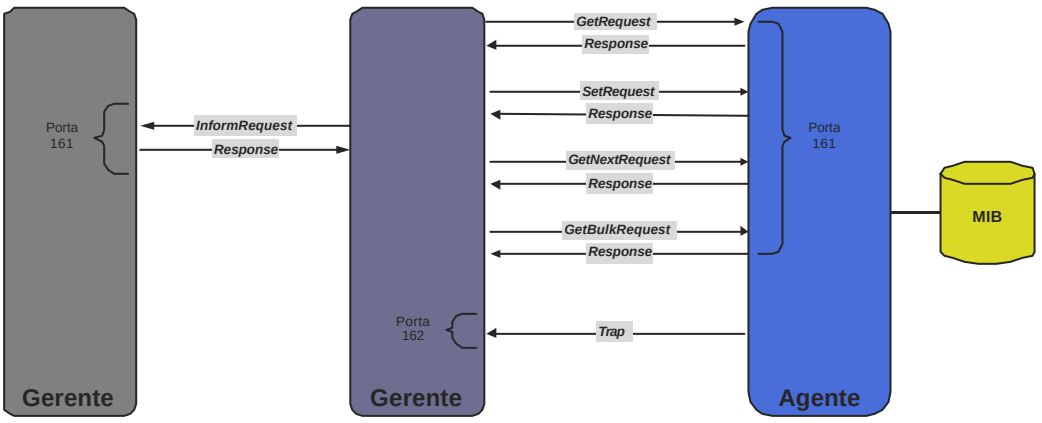


Figura 3.10 - *Operações do Protocolo SNMPv.2*

Com todas essas alterações, a *SMI* anteriormente proposta também sofreu modificações. Tipos de dados mais adequados e uma nova macro para convenções de

texto, a qual descreve melhor e com mais detalhes um tipo de dado específico definido pelo usuário, foram apresentados [23].

Com a possibilidade de comunicação entre dois gerentes, surgiu a necessidade de uma base de informação para a estação de gerência local. Desta forma, foi definida uma *MIB* denominada de *M2M* (*Manager to Manager*) [24], que suporta a distribuição de funções de monitoração entre os gerentes da rede. Tal monitoração é baseada em amostras realizadas nas variáveis do tipo *counter*, *gauge* e *timeticks* dos agentes. Os valores de tais atributos são comparados com valores limites configurados, e caso sejam atingidos, uma mensagem *inform-Request* é enviada pelo gerente que implementa a *MIB M2M* a outro gerente. Por essa razão, a *M2M* é composta de dois grupos de objetos: grupo *Alarm* e grupo *Events* [25]. O grupo *Alarm* contém objetos que permitem a configuração de qualquer gerente para o disparo de uma notificação em função dos valores de variáveis da *MIB*. O grupo *Events*, por sua vez, permite a definição do formato e da temporização destas notificações. Estas podem ser alarmes ou eventos determinados como a queda de um enlace (*link*). Com os novos desenvolvimentos, esta *MIB* alcançou o *status* de histórica, não sendo válida atualmente [12].

Vale ressaltar que antes da implementação do protocolo *SNMPv.2* com esquema de segurança baseado em *communities*, foi experimentada uma versão que possuía o conceito de *party* [15]. Este conceito visava a restrição das operações permitidas pelas entidades *SNMPv.2*, assim como as variáveis que elas enxergavam na *MIB* ou as partes com quem elas podiam trocar dados. Com as inovações do protocolo em termos de segurança foi preciso também alterar os formatos das mensagens. Isto fez surgir a necessidade de utilização de agentes *proxies* entre as versões 1 e 2 do protocolo *SNMP* [26]. Houve também um aumento da complexidade imposta às estações gerenciadas devido aos novos algoritmos de criptografia e autenticação empregados. Desta forma, foi preciso alterar o conceito de segurança proposto inicialmente pela versão 2 do protocolo *SNMP*.

O que aconteceu de fato com o *SNMPv.2* foi a aceitação das novas mensagens, como *get-BulkRequest*, a nova *SMI* e a nova *MIB*, mas mantendo o mesmo modelo administrativo e o mesmo esquema de segurança da versão 1 [12]. Contudo, apenas a estrutura de segurança foi rejeitada, pois originava grande

incompatibilidade entre a versão 1 e 2 do protocolo, já que as mensagens criptografadas não eram compreendidas pelas entidades do *SNMPv.1*. Desta forma, o que é empregado comercialmente na verdade é uma evolução do *SNMPv.2* na sua versão clássica, que possuía um esquema baseado em *parties*, para o *SNMPv.2* na sua versão mais atual, baseado em *communities* [12].

Embora possa se pensar que a coexistência entre as duas primeiras versões empregadas do *SNMP* seja passiva, ainda existe a necessidade da utilização do agente *proxy*. Isto se deve ao fato da conversão entre as mensagens da versão 1 e 2 do protocolo *SNMP* ser necessária. Caso contrário, para se alcançar esta coexistência será preciso que a estação gerente reconheça tanto as mensagens entre o gerente e o agente, como também as novas mensagens entre gerentes, ou seja, deverá "falar" o *SNMP* em sua versão 1 e 2 [6].

3.2.9 – *SNMPv.3*

As especificações para a versão 3 da arquitetura *SNMP* (*SNMPv.3*) [12] foram publicadas através do conjunto de *RFCs* 2271 a 2275 [14]. Esta nova versão do protocolo *SNMP* trouxe como principais vantagens aspectos ligados à segurança. Esta segurança busca evitar a alteração das mensagens enviadas. Além disso, barra-se o acesso a elementos estranhos à execução de operações de controle, que são realizadas através da primitiva *set-Request*. Evita-se também a leitura das mensagens por parte de estranhos, além de garantir ao gerente o direito de alteração da senha dos agentes. A segurança é conseguida com a introdução de mecanismos de criptografia como o *DES* (*Data Encryption Standard*) [5] e de algoritmos de autenticação que podem ser tanto o *MD* (*Message Digest*) na versão 5, quanto o *SHA* (*Secure Hash Algorithm*) [6].

O que acontece de fato com esta nova versão não é uma substituição das anteriores, mas sim a incorporação da solução dos problemas de segurança no acesso aos objetos às versões anteriores.

Com todas as inovações da versão 3 [6] [12], não foi possível fugir da complexidade. Os agentes serão mais complexos e os dispositivos gerenciáveis deverão contar com plataformas de processamento mais robustas. O grande aliado dessa nova versão é sua capacidade de operar em ambientes híbridos [6], ou seja,

que contenham entidades das versões anteriores. Apesar da melhora significativa sobre as versões anteriores, a aceitação do *SNMPv.3* ainda é uma incógnita.

3.2.10 – *Proxies*

O uso do *SNMP*, independente da sua versão, exige que todos os agentes, bem como as estações de trabalho, suportem uma pilha de protocolos em comum, ou seja, o *UDP* e o *IP*. Isto limita o gerenciamento direto de certos equipamentos e exclui outros, como *bridges* e modens, que não suportem qualquer parte do conjunto de protocolos do *TCP/IP* [15].

De modo a permitir a gerência de sistemas que não suportem a implementação do *SNMP* ou mesmo versões distintas deste protocolo, foi definido o conceito de *proxy* [15]. Neste esquema, o agente *SNMP* funciona como um *proxy* para um ou mais equipamentos. A Figura 3.11 mostra a arquitetura usual envolvendo *proxies*.

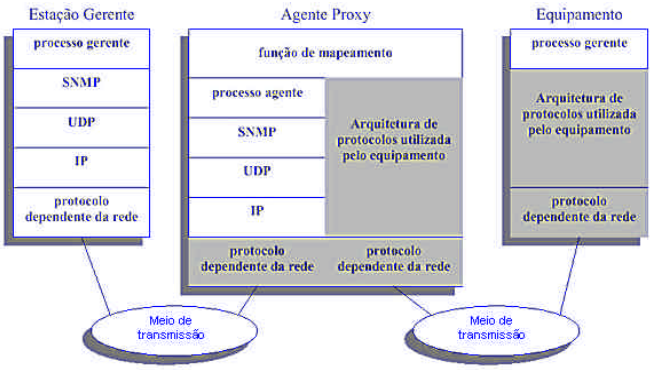


Figura 3.11 – *Configuração de Proxy para Gerenciamento SNMP*

Neste caso, a estação de gerenciamento manda requisições para o equipamento onde está o *proxy*. O *proxy* converte a requisição para o protocolo de gerenciamento ou versão do protocolo que é utilizado pelo equipamento. Assim que a resposta é recebida pelo agente (*proxy*) ele a converte em resposta padrão *SNMP* e repassa para a estação gerente. Da mesma forma, ao ocorrer algum evento no equipamento, a mensagem será recebida pelo agente e reenviada no formato das mensagens de *trap* adequadas ao protocolo *SNMP* e sua versão, para o gerente.

3.3 - Ferramentas Auxiliares na Gerência de Redes

Mesmo utilizando o protocolo *SNMP* como ferramenta principal na coleta dos dados, pode-se estar fazendo o uso de outras duas ferramentas no auxílio à gerência

da rede como um todo. Essas duas ferramentas, *RMON* e *Sniffers*, estarão sendo apresentadas a seguir, sendo observadas a possibilidade de serem empregadas na gerência de redes sem fio.

3.3.1 - *RMON*

A especificação *RMON* (*Remote Network Monitoring*) [6] é a adição mais importante ao conjunto básico dos padrões *SNMP*. Esta especificação oferece suporte à implementação de um sistema de gerenciamento distribuído. Nela, fica atribuída aos diferentes elementos, tais como estações de trabalho, *hubs*, *switches* ou roteadores das redes locais remotas a função de monitor remoto. Cada elemento *RMON* tem, então, as tarefas de coletar, analisar, tratar e filtrar informações de gerenciamento da rede e apenas notificar à estação gerente os eventos significativos e situações de erro. No caso de existirem múltiplos gerentes, cada elemento *RMON* deve determinar quais as informações de gerenciamento devem ser encaminhadas para cada gerente.

Os elementos *RMON* são empregados para estudar mais a fundo o tráfego nas redes locais e são chamados de Monitores de Redes, também referidos como Analisadores de Redes ou *Probes*. Esses elementos operam no modo promíscuo, "enxergando" todos os pacotes que passam pela rede e acumulando estatísticas preestabelecidas. Todos os cálculos são efetuados pelos *Agentes RMON*, sendo armazenados em objetos da *MIB* específica, chamada *MIB RMON* (*RFC* 1271). Esta estratégia possibilita a consulta de informações mais elaboradas, usando, ainda, as primitivas *SNMP*.

Dois padrões básicos de monitoramento remoto são especificados: *RMON1* e *RMON2*, que são funcionalmente complementares [6].

O *RMON1* opera na camada *MAC* [6], oferecendo recursos ao administrador da rede para monitorar o tráfego e coletar informações estatísticas da operação de um segmento de rede local, além de realizar o diagnóstico remoto de falhas e erros ocorridos no segmento de rede a partir das funcionalidades de um analisador de protocolo suportadas pelo correspondente elemento *RMON*.

O fato do *RMON1* trabalhar na camada *MAC*, significa que ele apresenta somente as estatísticas para o tráfego agregado aos protocolos deste nível, não apresentando estatísticas para camadas diferentes de várias pilhas de protocolos (ex.

IP, *FTP*, *IPX*). Isto também significa que por não serem capazes de monitorar a camada de rede, os dispositivos *RMON1* não distingüem o tráfego neste segmento que passa por um roteador, o que é uma grande deficiência. Assim, muitas aplicações usuais como uma medição do tempo de resposta cliente/servidor ou uma provisão de estatística para as sete camadas, não é possível utilizando este protocolo unicamente.

O *RMON2*, por sua vez, opera no nível da camada de rede e camadas superiores, complementando, portanto, o *RMON1*. Desta forma, existe a possibilidade da coleta de informações estatísticas, o monitoramento da comunicação fim-a-fim e o tráfego gerado por diferentes tipos de aplicação. A Figura 3.12 ilustra o escopo das atuações do *RMON1* e *RMON2* de acordo com as camadas propostas pelo modelo *OSI*.

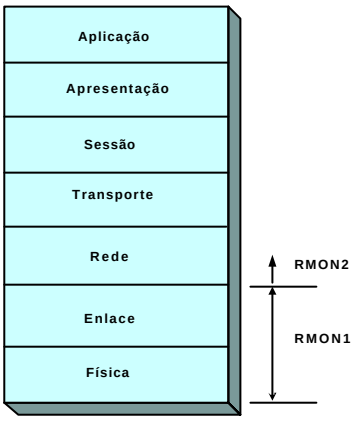


Figura 3.12 – *Abrangência da Atuação do RMON1 e RMON2*

Apesar da difusão do *RMON* ainda ser muito prejudicada pelos custos de implementação, implicando diretamente nos custos dos equipamentos fabricados com suporte a esse padrão, o *RMON* se apresenta como uma união bastante interessante entre o protocolo *SNMP* e os Monitores, tornando-se uma ferramenta poderosa na gerência de redes e que pode estar sendo empregada também em redes sem fio. Para a sua implementação em redes IEEE 802.11, deverá ser levado em consideração os aspectos referentes ao protocolo utilizado na rede, ou seja, o formato do quadro *MAC*. Desta forma, vários monitores de rede baseados no *RMON* que possuem analisadores de protocolo embutido, e que serão utilizados para a análise de redes sem fio, deverão possuir analisadores específicos acoplados, possibilitando a decodificação do protocolo.

3.3.2 - *Sniffers*

É uma tecnologia que se caracteriza por atuar em meios físicos compartilhados como os de uma *LAN*. São capazes de coletar dados apenas referentes aos quadros capturados, os quais correspondem às informações sobre os dados e protocolos que trafegam no meio de comunicação. Sua presença física no segmento de rede que se quer monitorar é indispensável.

A Figura 3.13 ilustra uma rede sendo gerenciada em parte com o auxílio de *Sniffers*.

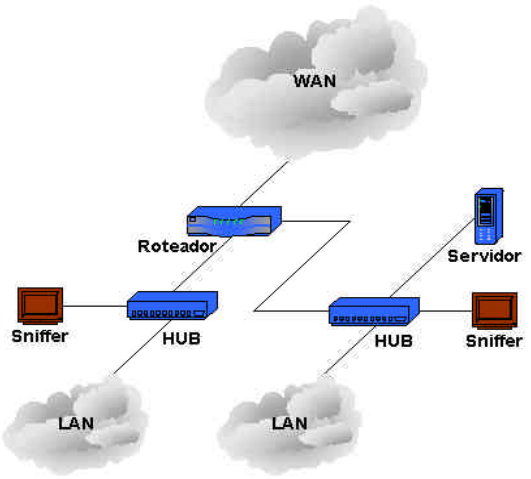


Figura 3.13 – *Estrutura de Rede Usando Sniffer*

Um *Sniffer* não é capaz de enviar comandos a um dispositivo, não podendo, assim, efetuar alterações de configuração ou operações remotas. Sua maior utilidade é implementar operações ligadas à gerência de desempenho e contabilidade em relação ao tráfego e serviços utilizados. Além disso, pode ser utilizado para identificar erros nos elementos da camada física da rede. Alguns *Sniffers* apresentam a capacidade de enviar alarmes para o Administrador da Rede, por exemplo, indicando alguma ocorrência de erro [27].

Contudo, as informações trocadas entre computadores consistem de conjuntos de bits aparentemente aleatórios que, sozinhos, de forma alguma ajudariam no entendimento das informações capturadas. Para que essas informações passem a ter algum valor, os *Sniffers* são acompanhados por softwares analisadores de protocolos, que interpretam as informações a partir da seqüência aparentemente embaralhada de bits trafegados, tornando possível sua leitura e entendimento.

Diferentemente das gerências *SNMP* e *RMON*, o monitoramento com *Sniffer* funciona de forma passiva, não havendo envio de pacotes de gerência pela rede. Esta é uma grande vantagem do *Sniffer*, visto que nesse caso não há consumo de recursos da rede monitorada.

Um fato importante é que as informações coletadas pelos *Sniffers* pertencem aos mais variados tipos de protocolos. Por isto, podem haver dados que não poderão ser decodificados devido a falta de compatibilidade por parte do *Sniffer*, em relação àquele protocolo. Deve-se observar que apesar do uso de S*niffers* na coleta de dados ter sido voltado às redes que seguem o padrão IEEE 802.3 [28], uma vez que esse padrão de *LAN* é predominante no mercado, o conceito de *Sniffers* é genérico e pode ser aplicado em outras tecnologias, como é o caso do *Spliter*, que é utilizado para coletar dados que trafegam em meios de comunicação que utilizam fibra ótica [27]. Isto faz surgir a necessidade de *Sniffers* específicos para determinadas análises de protocolos, como ocorre no caso de redes sem fio.

Na Tabela 3.2, pode-se observar de forma resumida as vantagens e desvantagens entre o uso da arquitetura *SNMP* e de *Sniffers* na gerência de redes.

Tabela 3.2 – *Tabela Comparativa entre o SNMP e Sniffers*

Ferramenta de Gerência	Vantagens	Desvantagens
SNMP	⇒ Possibilita a gerência remota, sem a necessidade de se locomover até o local onde se encontra o equipamento. ⇒ Um único *host* pode gerenciar toda a rede. ⇒ A maioria dos equipamentos gerenciáveis é adequada ao padrão *SNMP*.	⇒ Consome recurso da rede, ou seja, parte da largura de banda da rede será utilizada pelo tráfego *SNMP*. ⇒ A maioria das ferramentas que fazem gerência *SNMP* não é projetada para coleta de dados periódicos. ⇒ Consegue obter somente os dados disponíveis na *MIB* dos equipamentos.
Sniffers	⇒ Captura tudo que passa no barramento, podendo obter-se, após o tratamento dos dados, todas as informações relevantes para a avaliação da rede. ⇒ Não consome recursos da rede.	⇒ Necessidade de se ter um *host* executando o *Sniffer* em cada segmento a ser monitorado. Conseqüentemente, há um grande trabalho e perda de tempo com transporte de equipamento quando o trabalho é realizado em empresas de grande extensão. ⇒ Dificuldade de sincronizar vários *Sniffers*, ou seja, monitorar vários segmentos simultaneamente.

3.3.3 - Diferenças entre *RMON* e *Sniffers*

De fato, quando se compara o conteúdo dos objetos da *MIB RMON* com as coletas realizadas pelos *Sniffers*, verifica-se uma grande semelhança entre eles.

Ambos dão suporte a coletas complexas como a geração de uma matriz de tráfego da rede monitorada, lista dos computadores que mais consomem recursos da rede e tamanho médio dos pacotes trafegados, por exemplo. Além disso, os *Sniffers* atuais são capazes de enviar alarmes de notificação quando da detecção de falhas ou situações não usuais, da mesma maneira que é feita no *RMON*.

Num ambiente real de monitoramento pode surgir uma questão muito interessante: se as coletas oferecidas pelo *RMON* e *Sniffers* são tão parecidas, quando utilizar *RMON* e quando utilizar *Sniffers*? A resposta para essa questão deve ser baseada na análise do ambiente monitorado. Por exemplo, para realizar a Gerência *RMON* é necessário que os componentes da rede ofereçam suporte para tal, caso contrário a Gerência *RMON* pode ser descartada. No caso de suporte ao *RMON* pelos componentes da rede, se deve ainda verificar a estrutura lógica da rede. Caso a rede possua muitos enlaces, ou seja, baseada em *switches*, ou ainda uma rede muito extensa, uma *WAN* (*Wide Area Network*) por exemplo, a operação com *Sniffers* ficaria prejudicada, pois, além de ser necessária a colocação de *Sniffers* em cada um desses enlaces, não seria possível a utilização de gerência distribuída, aconselhável nessa situação. Já no caso de poucos enlaces, ou seja, com uso predominante de *hubs*, a técnica de *Sniffer* deve ser escolhida devido a uma de suas principais características: a não utilização de recursos da rede para efeito de monitoramento. Vale ressaltar que a utilização de ambos recursos simultaneamente, não deve ser descartada, pois possibilitaria a averiguação mútua dos dados coletados.

Do exposto anteriormente, conclui-se que tanto o *RMON*, o *Sniffer* e o *SNMP* não são tecnologias de gerência de redes concorrentes, mas sim, complementares. Desta forma, consegue-se obter um auxílio na gerência de redes que utiliza o *SNMP*, refletindo coletas mais complexas das informações sobre o tráfego de dados e podendo também, estar possibilitando uma carga menor na rede a respeito das mensagens de gerência trocadas.

Esta dissertação volta-se ao estudo sobre a arquitetura *SNMP*, que além de disponibilizar os objetos para a Metodologia de Análise de Desempenho que será proposta no próximo capítulo, está sendo empregada por grande parte dos fabricantes de softwares de gerência de redes IEEE 802.11 pesquisados. No Anexo A é apresentada uma análise sobre alguns softwares de gerência de redes.

3.4 – A Gerência de Desempenho

Uma rede de comunicação de dados moderna é composta por uma grande variedade de componentes que se interligam e compartilham dados e recursos. Boa parte da eficiência das aplicações que são executadas neste ambiente está ligada ao seu bom desempenho.

3.4.1 - Conceitos Fundamentais sobre a Gerência de Desempenho

O entendimento do funcionamento de um ambiente de rede é o primeiro passo para a definição dos conceitos envolvidos na Gerência de Desempenho.

3.4.1.1 - Serviço

Um serviço é um conjunto de procedimentos computacionais e de telecomunicações que permite a um usuário do sistema realizar uma determinada tarefa. Exemplos típicos de serviços são: correio eletrônico, serviço de impressão, serviço de armazenamento seguro de arquivos e muitos outros. Os serviços podem variar em complexidade e utilização de recursos de hardware, software ou ambos [29].

3.4.1.2. - Ocupação de Recursos e Caracterização de Serviços

Para a realização de uma determinada instância de um serviço, um ou mais recursos computacionais serão ocupados por determinado período de tempo. A natureza dos recursos ocupados e também o período de tempo que dura essa ocupação caracterizam o comportamento do serviço [29].

3.4.1.3 - Indicadores de Qualidade de Serviço

Cada tipo de serviço requer parâmetros mínimos de operação, tais como: tempo de resposta, velocidade de transmissão, taxa de erros, etc; para realizar com sucesso seu objetivo final. Caso esses requisitos mínimos não sejam atendidos pelo ambiente, o serviço sofrerá degradação, acarretando, até mesmo, a não execução da tarefa desejada [6]. Os Indicadores de Qualidade de Serviço são os parâmetros, extraídos do ambiente de rede, que revelam a qualidade corrente do serviço fornecido aos usuários de um determinado serviço.

3.4.1.4 - Demanda sobre os Serviços

Os usuários de um ambiente de rede têm à sua disposição um ou mais serviços que o ambiente lhe oferece. Dois ou mais usuários de um mesmo serviço

podem, coincidentemente, utilizá-lo ao mesmo tempo. Isso implica na necessidade de ocupação simultânea dos recursos de mesma natureza.

A demanda por um serviço é a medida da utilização ou tentativa de utilização (demanda reprimida) daquele serviço. Trata-se de um fenômeno aleatório, pois, na grande maioria das vezes, não se sabe exatamente quando um usuário irá utilizar um determinado serviço. Igualmente difícil é dizer exatamente quando dois ou mais usuários utilizarão o mesmo serviço. Existem apenas probabilidades de que tais situações ocorram durante um certo período de tempo [30].

Intuitivamente é possível notar que quanto maior for o número de usuários, maiores serão as probabilidades de utilização dos serviços oferecidos a esses usuários. Isso implica que quanto maior for o número de usuários, maior será a demanda pelos serviços oferecidos.

3.4.2 - As Principais Atividades da Gerência de Desempenho

Dentre as atividades mais importantes da gerência de desempenho de redes estão [6] [31]:

- Monitoramento do Desempenho
- Caracterização da Carga-de-Trabalho (*workload*)
- Ajuste de Parâmetros do Sistema
- Identificação de Gargalos
- Comparação de Desempenho entre Sistemas Alternativos
- Dimensionamento de Componentes do Sistema
- Previsão de Crescimento.

Tais atividades podem ser agrupadas em três grandes áreas: Monitoramento de Eventos Relevantes ao Desempenho de Sistemas, a Análise de Desempenho e o Planejamento de Capacidade.

3.4.2.1 - Monitoramento de Eventos Relevantes ao Desempenho de Sistemas

Consiste na coleta sistemática de informações que possam revelar os indicadores correntes de qualidade de serviço de uma rede ou caracterizar a carga de trabalho para uma instância de serviço.

3.4.2.2 - Monitoramento para Verificação de Desempenho

Essa atividade exige a coleta de informações que possam, claramente, apontar se o desempenho do sistema está abaixo do necessário ou desejado. Para isso, torna-se preciso um conhecimento sobre os padrões de qualidade de cada um dos serviços oferecidos pela rede e das ferramentas de monitoramento. Nem sempre é possível coletar diretamente os indicadores desejados. Muitas vezes é necessário coletar um conjunto de dados, relacionados ao indicador pretendido, dos quais é possível inferir o que se deseja realmente monitorar.

Para que se tenha uma gerência pró-ativa de desempenho, é necessário que o monitoramento seja feito com uma freqüência muito grande. Porém, vale observar que em se tratando do protocolo *SNMP*, a estratégia de monitoramento deve considerar a carga gerada na rede.

3.4.2.3 - Monitoramento para Caracterização da Carga-de-Trabalho (*workload*)

Outra atividade contida nessa área é a caracterização da carga-de-trabalho, atividade fundamental para a Análise de Desempenho e Planejamento de Capacidade. Consiste em levantar as características de um serviço, apontando como é, estatisticamente, a demanda sobre o mesmo e quanto se consome, em termos de recursos da rede, quando um usuário típico do serviço o utiliza.

Para se realizar essa tarefa, é necessário o monitoramento dos eventos de interesse, coletando, na rede, os dados relevantes para a captura da essência desse comportamento. Depois, é necessário aplicar as ferramentas estatísticas convenientes, conformando as informações obtidas [30] [31].

Na prática, a caracterização de uma carga-de-trabalho não é trivial. Isso se deve ao fato do analista ter que definir exatamente o que é o serviço que ele deseja estudar, definindo, implicitamente, quem são os seus usuários e como eles utilizam esse serviço. Assim, um sistema de banco de dados pode ser considerado como um serviço. Porém, em outra situação, o acesso ao disco do servidor de banco de dados é que pode ser considerado como o alvo do estudo.

Uma vez definido o escopo do serviço que se deseja caracterizar, a linha principal para a caracterização da carga-de-trabalho é associar os dados da utilização de recursos com o número de usuários presentes no sistema no momento do

monitoramento. Sempre que a caracterização apresentar comportamento estatístico muito variante, os usuários devem ser divididos por classes de comportamento (*clusters*). Não existem fórmulas para isso, assim, deve-se escolher dois ou mais recursos de grande importância para o serviço em estudo e se classificar os usuários em grupos que apresentem as mesmas características de utilização desses recursos [31].

Essa atividade deve ser feita com bastante rigor, a fim de que as etapas que dependem dela não sejam prejudicadas.

3.4.3 - Análise de Desempenho

A Análise de Desempenho é responsável por avaliar a capacidade instalada de uma rede (nós, enlaces e demais equipamentos) e, utilizando a carga-de-trabalho, caracterizada para os serviços suportados pela mesma, identificar gargalos (recursos responsáveis pela degradação dos serviços), ajustar parâmetros de configuração e comparar o desempenho de recursos de mesma natureza que poderiam ser adquiridos. Para alcançar suas conclusões, a Análise de Desempenho lança mão da construção de modelos matemáticos ou computacionais e suas respectivas metodologias de análise.

3.4.4 - Planejamento de Capacidade

O Planejamento de Capacidade baseia-se também na caracterização da carga-de-trabalho, para indicar, quantitativa e qualitativamente, as alterações necessárias para que o ambiente forneça a qualidade de serviço desejada [30] ou apontar a capacidade excedente [31]. Em ambos os casos, o que se deseja é ter uma previsão de crescimento e um cronograma de alterações na capacidade do sistema.

Geralmente, o Planejamento de Capacidade é usado em complemento à Análise de Desempenho, quando essa constata a falta de capacidade instalada. Ele também pode ser utilizado para definição de capacidades de um ambiente de rede que está em fase de projeto. Para isso, utilizará a carga-de-trabalho e a previsão do número de usuários obtidos de ambientes semelhantes.

Assim como a Análise de Desempenho, o Planejamento de Capacidade também utiliza técnicas matemáticas e computacionais para obter seus resultados.

3.4.5 - Técnicas Auxiliares da Gerência de Desempenho

As técnicas auxiliares da Gerência de Desempenho são o suporte matemático e computacional à resolução dos problemas propostos por essa área. Desta forma, são apresentadas duas formas básicas para análise de desempenho:

- Campanhas de medição em sistemas reais e operacionais;
- Construção de um modelo para um sistema proposto ou existente.

Cada uma dessas duas formas de avaliação de sistemas discretos possui características próprias que definem sua aplicabilidade. A primeira alternativa avalia o desempenho das redes de computadores utilizando campanhas de medições (*benchmarks*). A segunda alternativa, a de se construir um modelo do sistema, pode ser mais interessante devido à possibilidade de se construir modelos que projetem as diversas configurações e situações do sistema, de forma relativamente simples e econômica.

Um modelo representa as características fundamentais do comportamento de um sistema, e pode ser avaliado a partir de duas alternativas:

- Técnicas de simulação digital;
- Estudos analíticos, baseado na teoria de filas.

A alternativa de estudos analíticos se apresenta como a mais econômica e eficiente. Entretanto, a aplicação da solução analítica em sistemas complexos pode se tornar inviável, uma vez que essa alternativa geralmente impõe limitações ao modelo. Com isso, para viabilizar o estudo de sistemas complexos, muitas vezes, a simulação digital se apresenta como a melhor solução.

3.4.6 – A Simulação Digital

A simulação digital é baseada na construção de modelos que mostram o comportamento dos sistemas reais ou fictícios. Esses modelos permitem realizar experimentos automatizados sobre sistemas complexos, que foram implementados ou não. E ainda, a simulação digital permite realizar experimentos de um sistema diversas vezes, até se obter a melhor condição de funcionamento desse sistema.

Um modelo representa uma abstração do sistema real, reunindo um conjunto de características relevantes definidas para a modelagem. O escopo do modelo depende do que se pretende modelar, ou seja, depende do problema que se pretende dimensionar.

Para construir um modelo é necessário definir o nível de abstração desejado. Vários níveis de abstração podem ser usados, desde um nível mais alto até um nível mais baixo. O nível mais alto reflete um menor número de parâmetros considerados do sistema real, criando uma distância maior entre a realidade e o modelo. Desta forma, quanto mais alto for o nível de abstração, menor será a confiabilidade dos resultados gerados pelo modelo. A filosofia adotada é a de se construir o modelo a partir do nível mais abstrato possível, realizando melhorias até chegar no nível mais baixo, possibilitando uma maior aproximação com o sistema real e revelando os detalhes de seu funcionamento.

O detalhamento do modelo depende do nível de abstração atingido, já que quanto menor este nível, maior será o tempo utilizado na criação do modelo. Com isso, pode-se observar que o sucesso da simulação depende muito do esforço de elaboração do modelo. Além disso, é necessário um conhecimento elevado da ferramenta de simulação utilizada, requisito fundamental para otimização do tempo total usado no processo de simulação.

3.4.7 – Simuladores

Os simuladores são ferramentas de softwares usadas para construir e simular modelos dos sistemas [32]. Cada ferramenta oferece um conjunto de recursos necessários para que os sistemas sejam representados, processados e analisados.

A adoção da abordagem orientada a objetos na construção de simuladores revela a possibilidade de adicionar novos elementos ou funcionalidades, permitindo simular um conjunto maior de sistemas.

Um exemplo de um ambiente de simulação de propósito geral, voltado para a modelagem e avaliação de desempenho de qualquer sistema é o *Arena*$^{\hat{a}}$ [33]. Este ambiente foi projetado com abordagem orientada a objetos, usando linguagem C++. Tendo sido projetado especificamente para plataforma *Windows*$^{\hat{a}}$, o *Arena*$^{\hat{a}}$ utiliza a tecnologia *ActiveX*, o que lhe permite uma fácil integração com programas que também utilizam essa tecnologia, como o editor de texto *Winword* e a planilha de cálculo *Excel*, sendo ambos produtos da empresa *Microsoft Corporation*.

Outros simuladores se voltaram para sistemas específicos, a exemplo de redes de computadores. A seguir são apresentadas informações sucintas de dois

simuladores conhecidos que também adotaram a abordagem orientada a objetos nos seus desenvolvimentos:

- *Network Simulator* (*NS*) [34]: trata-se de uma ferramenta de código aberto construída em C++. O *NS* oferece módulos de simulação para diversos tipos de sistemas, com ênfase em redes *TCP/IP*. Atualmente o *NS* já modela redes sem fio. Aos poucos vem ganhando interfaces gráficas interessantes. Seu uso é bastante popular, principalmente no meio acadêmico, no entanto, necessita de um bom conhecimento da linguagem de *script OTcl.*
- *OPNET*$^{\hat{a}}$ *Modeler* [35]: é uma ferramenta comercial que oferece vários módulos para simulação. Possui excelentes recursos gráficos, possibilitando a criação gráfica de redes, nós, enlaces, sub-redes, protocolos, equipamentos, serviços e a ilustração geral dos modelos. Atualmente o *OPNET*$^{\hat{a}}$ *Modeler* trabalha com modelagem orientada a objetos e tem um módulo voltado à simulação de redes IEEE 802.11.

Para a simulação realizada nesta dissertação, um estudo sobre as ferramentas de simulação citadas anteriormente foi necessário, a fim de verificar a facilidade de seu entendimento, utilização e as possibilidades de sua aquisição. Contudo, a utilização do *OPNET*$^{\hat{a}}$ *Modeler* foi a que se mostrou mais interessante, já que abrange uma grande gama de parâmetros do padrão IEEE 802.11 e possui uma interface bastante amigável com relação às demais.

3.4.8 – A Simulação de Redes Utilizando o *OPNET*$^{\hat{a}}$ *Modeler* 9.1

Como já citado, será utilizado o *OPNET*$^{\hat{a}}$ *Modeler* em sua versão 9.1 educacional para a realização das simulações.

Como não existem dados reais coletados em uma rede sem fio, serão criados dados fictícios como parâmetros de entrada para a modelagem do perfil do usuário. Caso houvesse dados reais, poderia ser utilizada a facilidade fornecida pelo *OPNET*$^{\hat{a}}$ *Modeler* de importação do tráfego de dados e até mesmo de cenários.

A realização da simulação é uma parte importante na análise da capacidade futura da rede em absorver o impacto de novas aplicações e o aumento do número de usuários, verificando o seu desempenho perante as possíveis alterações em seus elementos. Contudo, torna-se necessário um planejamento de capacidade da rede, a fim de verificar, por exemplo, quando a rede vai apresentar gargalos e quais os

possíveis pontos. Com a simulação não será preciso modificar a estrutura da rede e muito menos adquirir novos equipamentos antes da verificação de sua necessidade. Um exemplo interessante é quando se deseja diminuir o tempo de resposta de uma aplicação e logo se pensa no aumento da capacidade do enlace. Pode ser que este aumento resolva, no entanto, o próximo nó da rede poderá se apresentar como um novo ponto de estrangulamento. Ao simular a rede haverá a condição de estar prevendo esta situação e verificar a curto e em longo prazo a validade das alterações propostas.

Capítulo IV

4 – Análise de Desempenho de Redes IEEE 802.11 Combinando a Gerência *SNMP* e Ferramentas de Simulação

Embora as redes sem fio já existissem desde 1980, elas ainda eram bastante primárias. No entanto, com as melhorias na sua padronização em 1990, houve um aumento na implementação dessas redes. Com isso, os dispositivos sem fio passaram a se tornar cada vez mais populares e com a confirmação do poder de conectividade destas redes, novas e mais elaboradas ferramentas de gerência se tornaram necessárias.

4.1 – Problemas com o Gerenciamento de Redes IEEE 802.11

A gerência de uma rede sem fio é, por várias razões, uma tarefa significantemente mais difícil do que gerenciar uma rede cabeada. Um dos principais problemas é o comportamento instável do canal sem fio devido ao desvanecimento, interferência de faixa estreita e condições atmosféricas. A qualidade do sinal pode variar drasticamente, e inesperadamente reduzir a eficiência da operação de gerenciamento. A largura da banda de transmissão dos enlaces sem fio é outra questão que sempre será limitada pelas propriedades do meio de transmissão e limitações do espectro de rádio. Portanto, é necessário que os protocolos utilizados nessas redes façam uso da banda disponível de forma eficiente. Sendo assim, o emprego do *SNMP* se mostra interessante, pois se trata de um protocolo que traz pouca carga à rede.

Outro grande problema no gerenciamento de redes sem fio é determinar onde estará situado o gerente e o número de estações que estarão sendo gerenciadas num determinado momento. Geralmente uma estação possui capacidade de processamento limitada, ficando difícil instalar um software gerente ou mesmo agente, além do que não se sabe se as estações que entram em um *BSS* dispõem do software agente, ou seja, de um agente *SNMP* [36].

4.2 – O Protocolo *SNMP* e o Desempenho de Redes IEEE 802.11

Dentre as versões do protocolo *SNMP*, a versão 2 foi a que levantou maior interesse, pois apresenta uma série de vantagens sobre a versão 1 e a versão 3 que, embora seja superior no quesito segurança, ainda não foi comercializada [4]. Além disso, a *MIB* IEEE 802.11 é baseada na estrutura de gerenciamento do *SNMPv.2* e na *RFC* 1213 [37].

4.2.1 - Motivações para se Utilizar a Versão 2 do Protocolo *SNMP*

A gerência de redes sem fio requer alguns cuidados e por se tratar de uma rede altamente escalável, ou seja, um sistema distribuído em potencial, necessita também de uma gerência distribuída. Isto irá trazer benefícios, pois a estação gerente não sendo única, deixa de haver um único ponto de falha para o sistema de gerência. Através das características apresentadas no capítulo anterior sobre o *SNMPv.2*, verifica-se a possibilidade do gerenciamento hierarquizado. É importante observar que o gerenciamento distribuído fornecido pelo *SNMPv.2* é limitado entre um gerente principal, gerentes intermediários e agentes, ou seja, fica limitado a apenas dois níveis hierárquicos [38]. A Figura 4.1 [39] ilustra uma possibilidade de gerenciamento hierárquico. Como se pode observar, os dois *BSSs* fazem o uso de dois pontos de acesso (*APs*) para se conectarem ao barramento Ethernet e também para a realização de gerenciamento no nível intermediário. Assim, os dois *APs* possuem gerentes intermediários, que também serão agentes para o gerente final. Esta estação gerente fica responsável por receber todas as informações dos gerentes intermediários por meio da troca de informações *inform-Request* e *Response* [6] [12], além de gerenciar normalmente os outros dois dispositivos ligados ao barramento Ethernet.

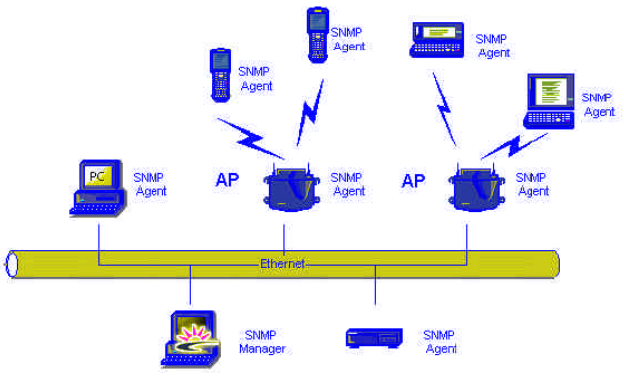


Figura 4.1 – *Esquema de Gerência para Redes Sem Fio*

Ao mesmo tempo em que o protocolo *SNMP* se mostra capaz de gerenciar tais redes, ele também apresenta limitações. Um agente na rede sem fio pode não suportar todos os objetos definidos pelas *MIBs* que implementam, o que iria requerer memória e poder de processamento, resultando em custo. Com a finalidade de se evitar este problema, um conjunto de implementações limitadas foi definido na *RFC* 1904 (*Conformance Statements for Version 2 of the Simple Network Management Protocol*) [14].

Além dos benefícios já descritos, a versão 2 do protocolo *SNMP* ainda possibilita uma segurança maior comparada à versão 1, empregando algoritmos de criptografia mais complexos, embora ainda seja utilizado um esquema de segurança baseado em *communities*. Outra vantagem é que as operações não são mais atômicas, ou seja, tudo ou nada. Isto se torna interessante em redes sem fio devido ao problema da qualidade de seus enlaces de rádio, possibilitando que mesmo uma busca de grandes conteúdos de dados na *MIB* não se torne um processo demorado, pois não terá que buscar novamente todo o conteúdo. Desta forma, será necessária uma nova busca apenas da parte que tenha sido perdida.

4.2.2 – O *SNMP* na Gerência de Redes Padrão IEEE 802.3 (Ethernet)

Utilizando o protocolo *SNMP* é possível buscar informações gerais necessárias ao gerenciamento nas *MIBs* I e II, além de informações que possibilitam o gerenciamento mais completo de um equipamento da rede, com a *MIB* proprietária, e informações específicas do meio de transmissão, com a *MIB EtherLike* [37]. Por exemplo, com a *MIB EtherLike* consegue-se obter informações sobre colisões, configuração, varredura das portas e muitas outras de um *hub*. Também é possível fazer testes, reinicializar ou desabilitar uma ou mais portas de um *hub* gerenciável, com a *MIB-II*. A obtenção de outras informações julgadas importantes pelo seu fabricante, tais como a versão do equipamento, níveis do sinal transmitido, o número total de portas e quais portas estão falhando podem ser encontradas em sua *MIB* proprietária.

Mesmo a *MIB-II* oferecendo variáveis que lidam com a configuração da interface, tráfego, *status* e erros comuns, deve-se fazer o uso das *MIBs* específicas a uma determinada tecnologia. Elas são necessárias porque existem diferenças de configuração, condições de *status* particulares, além de erros que são específicos de

cada tecnologia. Além disso, alguns testes que são primordiais em determinada tecnologia, não fazem sentido de serem executados em outra. Por exemplo, a *MIB EtherLike* inclui tabelas que contam o número de ocorrência de vários tipos de problemas, gera um histograma da distribuição de freqüência do número total de colisões que ocorrem ao se tentar transmitir um quadro (*frame*) e define um teste de reflectometria usado para detectar rupturas de cabos. No caso da *MIB* específica para redes locais *Token Ring*, as colisões não são um problema, mas sim a perda dos quadros de dados e de controle (*tokens*).

Os objetos que formam a base para caracterizar o meio de transmissão da rede, como o da Ethernet, estão referidos na *MIB EtherLike* (*RFC* 1643), que é uma das *MIBs* referidas sob o nó *transmission* na hierarquia da *MIB-II.* O grupo *Transmission* na verdade não é um grupo como um todo, mas simplesmente um nó na hierarquia da *MIB-II* sob o qual vários grupos com informações específicas das interfaces são bcalizados [6]. A Figura 4.2 [37] ilustra a estrutura em árvore correspondente à *MIB EtherLike,* onde se observa a localização dos objetos correspondentes à rede IEEE 802.3 logo abaixo do nó *transmission*.

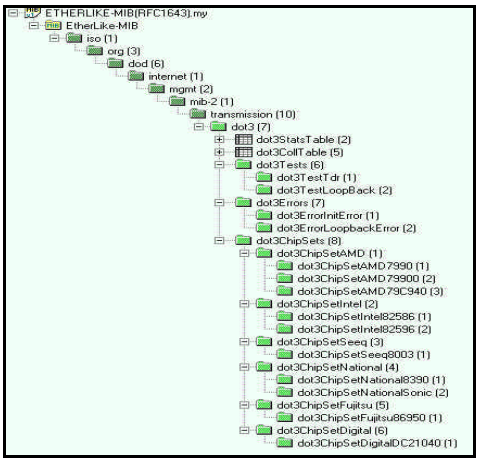


Figura 4.2 – *A Estrutura em Árvore da MIB EtherLike*

Um equipamento sendo gerenciado em uma rede Ethernet poderá conter a *MIB-II*, a *MIB EtherLike, a MIB Bridge*, além de sua *MIB* proprietária. Na Figura 4.2, observa-se objetos que representam os atributos de uma interface que utiliza o protocolo *CSMA/CD*, refletindo estatísticas observadas na interface entre o agente e o meio de transmissão, como tráfego e colisões. Por exemplo, as estatísticas do tráfego observado na interface entre o agente e o meio de transmissão são gravadas na tabela *dot3StatsTable*. A instância do objeto *SingleCollisionFrames* é um

contador do número de quadros transmitidos com sucesso antes de ter ocorrido uma tentativa de transmissão sem sucesso, devido a uma possível colisão [6]. Da mesma forma que este contador é incrementado, o contador do grupo *Interfaces ifOutUcastPkts* também é incrementado. Similarmente, o *dot3StatsMultipleCollision-Frames* é incrementado para cada quadro transmitido com sucesso antes de ter ocorrido mais de uma tentativa de transmissão sem sucesso. Simultaneamente o contador *ifOutUcastPkts* também será incrementado. Desta forma, conclui-se que para a análise de desempenho que será proposta mais adiante neste capítulo, devem ser utilizados os objetos mais genéricos, os quais serão encontrados na *MIB-II*, ao invés de somar os atributos de objetos com informações parciais para obter o mesmo resultado. Isto fará com que se minimize o trabalho com a manipulação dos dados.

Deve-se observar que as documentações sobre as *MIBs* não são estáticas, ou seja, sempre estão surgindo novas *RFCs.* Isto torna obsoletas as *RFCs* anteriores, nas quais foram baseadas os novos documentos. Assim, alguns objetos são suprimidos e outros adicionados, de forma que o modelo de gerência *SNMP* consiga acompanhar as evoluções tecnológicas, tanto na teoria como na implementação em seus agentes e gerentes.

4.2.3 – O *SNMP* na Gerência de Redes Padrão IEEE 802.11 (*WLAN*)

As melhorias promovidas na arquitetura *SNMP* com novos documentos (*RFCs*) sendo lançados, permitiu o acréscimo de novos tipos de interfaces e objetos. Como grande parte dos agentes *SNMP* dos dispositivos de redes sem fio suportam a *MIB-II*, mas não distingüem quais são seus objetos, ou seja, qual a *RFC* implementada, considerou-se a *RFC* 1213 sem as alterações da *IANA* (*Internet Assigned Numbers Authority*). Isto significa dizer que as alterações realizadas na *MIB-II* pela *IANA*, como a mudança da sintaxe do *ifType* para *IANAifType*, indicando novos tipos de interfaces para a *MIB* utilizada pelo protocolo *SNMPv.2* ao invés de renomear a *MIB-II*, não foram consideradas [6].

Desta forma, foi analisada a *MIB-II* definida em 1991 e verificou-se que a interface com o tipo de protocolo *CSMA/CA* não estava disponível, como se observa na Tabela 4.1. Com isto, deve-se fazer o uso do tipo *other*, indicando nenhuma das interfaces seguintes na tabela. O objeto *ifSpecific* do grupo *Interfaces* será responsável por indicar o local onde se encontra a parte específica do meio de

comunicação usado pela interface, podendo ser um nó do grupo *Transmission* ou receber o seu próprio endereço (*OID*).

Tabela 4.1 – *Alguns Tipos de Interfaces de Rede*

Number	Type	Description
1	Other	None of the folowing
2	Regular1822	The original ARPANET interface protocol between a host and na Interface Message Processor (IMP)
3	hdh1822	Revised version of 1822, using a synchronous link scheme
4	ddn-x25	Version of X.25 specified for the Defense Data Network
5	rfc877-x25	Version of X.25 defined in RFC 877, intended for carrying IP datagrams
6	EthernetCsmacd	Ethernet Medium Access Control (MAC) protocol
7	iso88023Csmacd	IEEE 802.3 CSMA/CD MAC Protocol
8	iso88024TokenBus	IEEE 802.4 Token Bus MAC Protocol
9	iso88025TokenRing	IEEE 802.5 Token Ring MAC Protocol
10	iso88026Man	IEEE 802.6 DBQD MAC Protocol for MAN's
11	StarLan	1 Mbps twisted pair version of Ethernet
12	Proteon-10Mbit	10 Mbps optical fiber token ring LAN developed by Proteon

Vale observar que a Tabela 4.1 não apresenta todas as interfaces descritas pela *MIB-II*, somente algumas, no intuito de ilustrar a possibilidade de outras interfaces (*other*).

Como foi mencionado, novos tipos de interfaces podem ser encontrados em novas *RFCs* definidas através da *IANA*, como a *RFC* 1573 (*Evolution of the Interfaces Group of MIB-II*), que evoluiu mais tarde para *RFC* 2233 (*The Interfaces Group MIB using SMIv.2*) [14]. A Figura 4.3 [37] ilustra parte dos tipos de interfaces definidos pela *IANA*. Caso mais detalhes sejam requeridos quanto às interfaces, podem ser encontrados na *RFC* 1213 com algumas alterações da *IANA* proposta pela *Cisco Systems* [6].

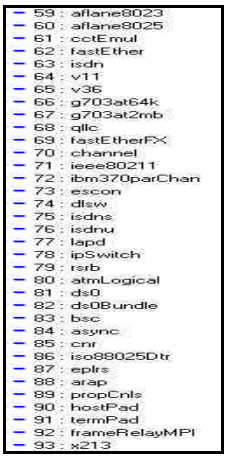


Figura 4.3 – *Parte dos Tipos de Interfaces Definidos pela IANA*

Na Figura 4.3 observa-se que o tipo de interface para redes locais sem fio recebe o número 71, podendo ser utilizado em equipamentos que disponham da *MIB-II* definida em 1994 pela *Cisco Systems* [37].

Os equipamentos para redes sem fio, tais como os *APs*, apresentam o suporte a várias *MIBs*. Um exemplo que pode ser citado é o *AP-10 Pro.11* da série *BreezeNet Pro*, da *BreezeCom Wireless Communications*, cujo agente *SNMP* suporta a *MIB-II*, *MIB Bridge*, além de sua *MIB* proprietária. Já o *AP* da *Black Box Network Services* da série *Pro* e *Pro.11* tem seus agentes *SNMP* suportando a *MIB-II*, *MIB Bridge*, *MIB* proprietária, além da *MIB* IEEE 802.11.

A *MIB Bridge* [40] é uma *MIB* pública, que será responsável por parte dos objetos referentes ao gerenciamento do *AP* atuando como uma *bridge*. Embora possa parecer desnecessária a utilização de tantas *MIBs*, para que o gerenciamento seja mais completo torna-se necessário pelo menos os grupos *Interfaces* e *System* da *MIB-II*, além dos grupos apresentados pela sua *MIB* proprietária.

Observa-se na Figura 4.4 [37] parte da estrutura em árvore da *MIB* IEEE 802.11. Estes objetos são responsáveis pelas informações gerais sobre a camada *MAC* e a camada física deste tipo de rede local.

Figura 4.4 – *Parte da SMI da MIB IEEE 802.11*

As informações da camada *MAC* da *MIB* IEEE 802.11 compreende duas partes: os atributos de gerenciamento de uma estação e os atributos *MAC*. Os atributos de gerenciamento da estação estão associados com a configuração de opções do *MAC*, na operação do gerenciamento *MAC* e seu desempenho [4].

Já as informações da camada física da *MIB* IEEE 802.11 compreende os objetos responsáveis por refletirem dados gerais a respeito das tecnologias utilizadas para a transmissão e recepção dos bits.

Contradizendo a teoria descrita sobre a *MIB-II* para informações específicas do meio de transmissão de cada interface, como a Ethernet, observa-se na estrutura em árvore da *MIB* IEEE 802.11, ilustrada na Figura 4.4, que os seus objetos não são colocados logo abaixo do nó *transmission*, mas sim, seguem o ordenamento lexicográfico 1.2.840.10036 adquirido pelo grupo de padronização IEEE 802.11, independente da *MIB-II*.

A análise de alguns objetos da *MIB* específica para redes IEEE 802.3 permitiu concluir que a utilização dos objetos com informações mais genéricas do grupo *Interfaces* da *MIB-II* fornecem resultados mais fáceis de serem manipulados. O mesmo raciocínio pode ser empregado para redes IEEE 802.11. Por exemplo, o objeto com informação parcial: *Dot11ReceivedFragmentCount* é um contador que deverá incrementar a cada quadro de dados ou de gerenciamento recebido com sucesso. No entanto, para se obter o total de quadros recebidos em uma interface para rede sem fio, seria preciso ainda somar os quadros de controle. Além disso, como o que importa é o número de bytes recebidos na interface, ainda deveria ser feito um tratamento matemático para conseguir um resultado que diretamente é alcançado com o objeto *ifInOctets* do grupo *Interfaces* da *MIB-II*, que é parte do indicador de utilização da interface.

4.2.4 – As *MIBs* Proprietárias

A falta de interoperabilidade entre fabricantes de dispositivos de rede gerenciáveis pode surgir quando suas *MIBs* são baseadas em estruturas de informação de gerenciamento diferentes. Por exemplo, os fabricantes podem se basear nos seguintes documentos [6]:

- A especificação original da estrutura e identificação de informação de gerenciamento *SNMP*, *RFC* 1155;
- Em um formato conciso de *MIB*, *RFC* 1212;
- E na especificação da estrutura e identificação de informação de gerenciamento *OSI*.

Uma solução para se evitar a falta de interoperabilidade é que todas as *MIBs* proprietárias a serem criadas se baseiem em um documento comum e, para as *MIBs* que já estão no mercado há algum tempo, torna-se necessária a conversão de documentos para um formato que possibilite a interoperabilidade. No entanto, esta conversão irá requerer um alto grau de conhecimento de ambos os documentos.

Como já citado nesta dissertação, as *MIBs* proprietárias são específicas dos equipamentos gerenciados, fazendo-se necessárias para que detalhes peculiares a um determinado equipamento possam ser obtidos. A título de ilustração é apresentada na Figura 4.5 [37] parte da estrutura em árvore da *MIB* proprietária do *AP* da *Cisco Aironet*â.

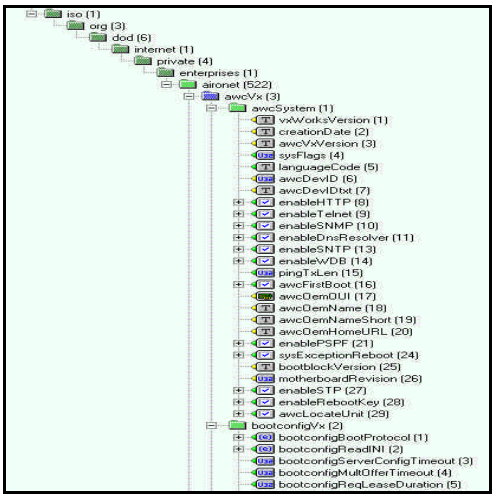


Figura 4.5 – *Parte da MIB do AP da Cisco Aironet*â

Entre os objetos apresentados na Figura 4.5 podem ser destacados alguns que refletem informações específicas do *AP* da *Cisco Aironet*â, tais como:

- *VxWorksVersion* – indica a versão do sistema operacional *VxWorks.*
- *AwcDevID* – indica se o sistema está configurado para atuar com toda a capacidade que é dotado, ou seja, um Portal pode ser configurado para ser usado somente como um *AP*.
- *AwcEtherMIB* – é uma classe de objetos definidos sob a árvore da *Cisco Aironet*â, responsável pelo controle da interface Ethernet existente neste *AP*, já que ele pode atuar como um portal, interligando uma rede sem fio a uma rede cabeada.
- *AwcOemName* – indica o nome completo do revendedor pelo qual o sistema foi registrado.

Vários outros objetos podem ser encontrados em outras *MIBs* proprietárias de equipamentos para redes sem fio, de forma a trazer características que segundo o fabricante sejam necessárias ao melhor gerenciamento, tais como a tecnologia utilizada pela camada física e mobilidade. A seguir são apresentados alguns objetos da *MIB* proprietária do *AP* da *BreezeCom* [41].

- *KnownAPsQuality* – este atributo especifica a atual qualidade de recepção dos quadros transmitidos pelo *AP*. Sendo que para a estação, um bom valor indica a sua possibilidade de associação com o *AP*.
- *BrzAvrgRssi* – este valor representa o nível médio do sinal dos pacotes recebidos de um *AP*. Este atributo é aplicável somente a uma estação. No caso de um *AP*, será sempre retornado o valor 255.
- *BrzMobilLvl* – indica o nível de mobilidade esperado do sistema. O valor padrão é estacionário, mas vários outros podem ser atribuídos, tais como: portátil, móvel, multi-célula e especial.
- *BrzAProamingInTRAP* – é uma notificação para o gerente, que normalmente está locado no *AP*, indicando que uma estação entrou na área de cobertura daquele *AP*.
- *BrzAPassociatedTRAP* – é uma notificação do *AP*, indicando que uma nova estação se associou com este *AP*.
- *BssNumOfStations* - o número de estações que estão atualmente associadas com o *AP*.
- *BssNumOfStationsPeak* - o número máximo de estações que podem associar com o *AP*.
- *StCurTxRate* - indica a taxa atual utilizada pelo *AP* para transmitir seus pacotes para a estação.
- *StMaxRate* - indica a taxa máxima na qual uma estação transmite dados no meio sem fio.

Não existe a pretensão de citar todos os objetos existentes nestas *MIBs*, mas sim de trazer a informação sobre a possibilidade de serem encontrados objetos específicos de determinados equipamentos com a finalidade de auxiliar na sua gerência. Além disso, outros objetos melhorados da *MIB* pública ou mesmo sendo apenas renomeados, podem ser encontrados na *MIB* proprietária do equipamento.

Isto torna possível, por exemplo, que um equipamento não disponha da *MIB* IEEE 802.11, mas contenha em sua *MIB* proprietária os objetos da *MIB* IEEE 802.11 julgados necessários pelo fabricante para fornecer um completo gerenciamento, já que alguns objetos têm sua implementação opcional.

4.2.5 – Diferenças entre o *SNMP* sobre Redes Padrão IEEE 802.3 e 802.11

Com relação à coleta dos dados na *MIB* do equipamento pode-se observar que existem diferenças principalmente quanto às suas *MIB*s específicas, que terão objetos que reflitam meios de transmissão diferentes, juntamente com as *MIBs* proprietárias. Alguns objetos da *MIB* IEEE 802.11 [37] ilustram essas diferenças a seguir:

- *Dot11RTSSuccessCount* – este contador deverá incrementar quando o quadro *CTS* é recebido em resposta a um quadro *RTS*. Pode-se observar que este objeto faz parte do protocolo *CSMA/CA* no seu modo de operação *DCF* opcional. No caso da rede local Ethernet, sua *MIB* não teria este objeto, pois esta tecnologia de rede utiliza o protocolo de acesso ao meio *CSMA/CD.*
- *Dot11AssociationResponseTimeout* – objeto também particular das redes sem fio, indicando o tempo que o pedido de uma estação deve esperar pela resposta a um pedido de associação.
- *Dot11PowerManagementMode* – é outro objeto específico das redes sem fio, que indica se a estação se encontra em modo de economia de energia (*power-save*).

Observa-se que os objetos da *MIB* pública e da proprietária do equipamento para redes sem fio possuem informações redundantes e isto já havia sido observado na *RFC* 1573 definida pela *IANA*, onde a implementação do objeto *ifSpecific* da *MIB-II* tornou-se *deprecated* (a informação apresentada por este objeto é redundante, mas ele ainda é obrigatório), pois continha menos informações que o objeto *ifType*, que era mais completo [6].

A *MIB-II* será comum aos dispositivos gerenciáveis das redes IEEE 802.3 e 802.11, pois contém informações genéricas sobre os equipamentos gerenciados, incluindo informações de configuração e estatísticas dos eventos das interfaces. A implementação do grupo *Interfaces* é obrigatória para todos os sistemas, de forma a possibilitar um gerenciamento mais completo.

Das análises feitas na *MIB* proprietária da *Cisco Aironet*$^{\hat{a}}$, da *BreezeCom* e na *MIB* IEEE 802.11, foram encontrados poucos objetos que poderão auxiliar na análise

de desempenho que será proposta. Já na *MIB-II*, é encontrada a maioria dos objetos utilizados, como poderá ser visto na seção 4.4.2.2.

4.2.6 – Requisitos de uma Estação de Gerenciamento

As estações de gerenciamento fornecem ao administrador da rede uma interface para todo o sistema de gerenciamento e devem, portanto, prover um acesso mais flexível e amplo às informações relevantes. As seguintes características devem ser incluídas em uma estação de gerenciamento [6]:

- **Suporte à *MIB* estendida**

O completo gerenciamento *SNMP* será alcançado somente se a sua *MIB* suportar objetos da *MIB* proprietária do equipamento gerenciado, ou seja, uma estação de gerenciamento deve ser capaz de carregar as definições das *MIBs* para a *MIB* estendida definida pelos agentes de outros fabricantes.

- **Interface intuitiva**

A interface de gerenciamento para o administrador da rede deve ser tão fácil e poderosa quanto possível. O administrador da rede utilizando uma interface de janela gráfica deve ter a possibilidade de abrir janelas separadas para cada parte da rede que desejar monitorar. A interface deve ser capaz de mostrar a topologia da rede, com a localização de seus dispositivos. Ícones inteligentes podem ser utilizados para representar componentes chaves tais como *APs*, *bridges* e usuários, de forma que ao clicar nestes ícones o sistema deverá mostrar a situação atual do dispositivo e opções para o seu controle.

- **Descoberta automática**

Uma estação de gerenciamento deve ser capaz de descobrir, ao ser instalada, todos os agentes com base numa dada seqüência para se construir o mapa da rede e configurar os seus ícones.

- **Eventos programáveis**

O administrador da rede deve ser capaz de definir as ações a serem tomadas quando certos eventos ocorrerem. Por exemplo, no evento de uma falha de um roteador, a estação de gerenciamento poderia mudar a cor do ícone do roteador, enviar uma mensagem por *e-mail* para o administrador da rede e ainda acionar um alarme.

- **Controle de rede avançado**

Idealmente, a estação de gerenciamento da rede deve desempenhar algumas funções predefinidas sob certas condições. Por exemplo, o administrador da rede deve ser capaz de configurar a estação de gerenciamento automaticamente para desligar um *hub* em mau funcionamento ou isolar todo um segmento da rede de forma que não prejudique toda a rede.

4.3 – Grupos de Recursos Gerenciáveis da Rede

Para que se consiga obter uma visão clara da metodologia que será proposta, é necessário definir o que estará sendo gerenciado. A Figura 4.6 [42] ilustra a interação de três grupos de recursos, os quais são abstraídos com base nos elementos gerenciáveis de um sistema distribuído.

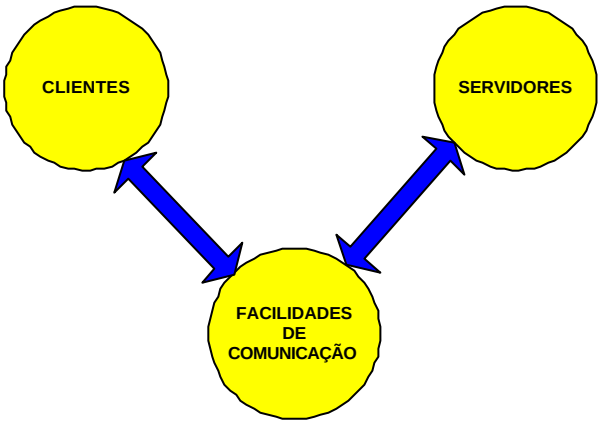


Figura 4.6 - *Modelo dos Grupos de Elementos de um Sistema de Gerência*

A seguir é apresentada a descrição dos três grupos referentes às possibilidades de elementos gerenciáveis em cada um.

4.3.1 - Clientes

É o grupo composto por terminais e/ou estações, ambos usuários dos serviços disponíveis na rede. Por isso recebem o nome de “Clientes”. Os elementos desse grupo podem ou não apresentar capacidade de processamento e realização de tarefas, ficando sujeito, nos casos afirmativos, à gerência de desempenho. O papel dos “Clientes” é representar as fontes de geração de demanda sobre os serviços de rede, refletindo no grau de utilização dos recursos classificados nos demais grupos. Os “Clientes” enxergam apenas as solicitações de serviço emitidas e as respostas recebidas. Apesar de terem como intermediários os recursos do Grupo Facilidades de

Comunicação, o Grupo Clientes se comporta como se tivesse uma interface direta com o Grupo Servidores, abstraindo-se dos serviços prestados pelo Grupo Facilidades de Comunicação.

4.3.2 - Facilidades de Comunicação

Representa os elementos envolvidos na tarefa de escoar e encaminhar o tráfego da rede. Nesse grupo estão classificados desde os meios de comunicação até os equipamentos ativos de rede. Por terem uma visão do tráfego bruto entre "Clientes" e "Servidores", possuem um ponto de vista privilegiado, além de fornecer dados de gerência de seus próprios elementos, e disponibilizar informações úteis sobre os demais grupos. Não é comum encontrar elementos desse grupo que sejam geradores de tráfego. Assim, do ponto de vista de desempenho, são elementos que prestam o serviço fundamental das redes: o transporte de dados. Logo, este serviço necessita ser muito bem planejado e ser submetido a um processo rigoroso de avaliação de desempenho.

4.3.3 - Servidores

São os equipamentos responsáveis por fornecer os serviços utilizados pelos "Clientes". Em um grande número de situações, esses elementos corresponderão aos tradicionais servidores de rede. Os "Servidores" recebem requisições ou chamadas através de seus elementos de acesso a serviços. Observando os parâmetros fornecidos pelas requisições ou chamadas, efetuam operações e/ou procedimentos, retornando informações aos "Clientes" que iniciaram o processo. Para cumprir seu papel, esses elementos são dotados de capacidade de processamento e realização de tarefas, sendo, portanto, alvo da gerência de desempenho. Assim como os "Clientes", os "Servidores" também geram tráfego sobre a rede, geralmente em resposta às requisições de seus clientes. Dessa forma são também usuários dos serviços básicos fornecidos pelo Grupo Facilidades de Comunicação.

Dentre os aspectos mais relevantes desse modelo vale destacar a visão privilegiada que o Grupo Facilidades de Comunicação tem em relação aos demais grupos. Sendo o grupo intermediador de todo o processo, é bastante adequado utilizá-lo como ponto de partida para o monitoramento de desempenho de todo o sistema.

4.4 – A Metodologia Proposta para Análise de Desempenho

Baseado no que foi citado até agora nesta dissertação, é apresentada uma proposta de metodologia para a análise de desempenho de redes, visando as redes IEEE 802.11 e combinando a gerência *SNMP* com ferramentas de simulação.

Esta metodologia é composta por quatro fases, que são organizadas de acordo com as etapas a serem cumpridas por uma estação de gerência. Estas etapas vão desde a verificação de quais objetos são relevantes para a composição dos indicadores de desempenho desejados, passando por um tratamento matemático dos dados coletados e obtendo esses indicadores. Com base na interpretação dos resultados, o administrador da rede terá condições de tomar a decisão de entrar ou não no processo de simulação da rede. Esta metodologia visa minimizar a intervenção humana no processo de análise de desempenho, já que não é desejável eliminá-la por completo. Para isto, torna-se necessário a sua implementação em software, entretanto, esta implementação não faz parte do escopo desta dissertação.

Um diagrama em blocos é apresentado na Figura 4.7, esquematizando o envolvimento das quatro fases propostas.

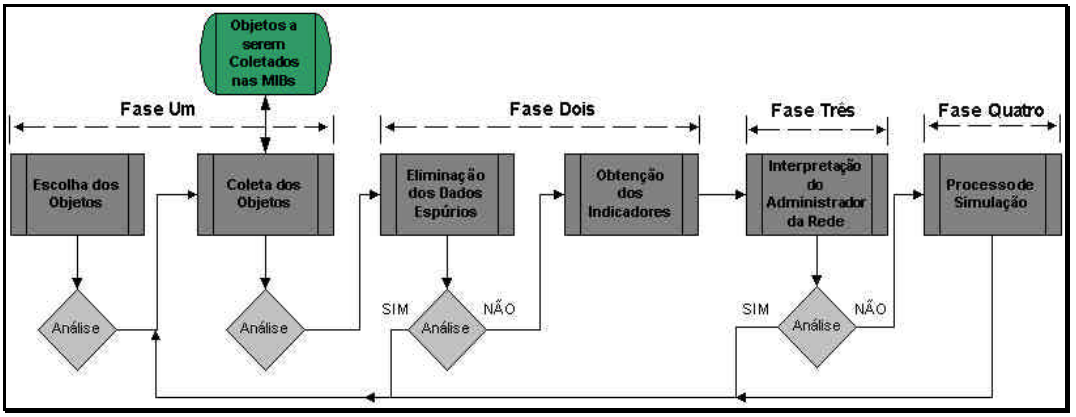


Figura 4.7 – *Esquema Proposto para Análise de Desempenho*

4.4.1 – A Fase Um (Escolha e Coleta dos Objetos)

Esta é a fase inicial da metodologia proposta e para que tudo ocorra bem com as etapas seguintes, é importante o bom conhecimento de todos os dispositivos gerenciáveis da rede. Assim, o administrador da rede terá melhores condições para solucionar problemas que porventura venham a ser identificados.

4.4.1.1 - Etapa Um (Escolha dos Objetos)

Esta etapa se refere a escolha dos objetos nas *MIBs* suportadas pelos agentes *SNMP* e ainda é dividida em três passos.

- **Passo Um** – inicialmente deve ser escolhido qual dos Grupos será alvo da gerência.
- **Passo Dois** – o administrador da rede deverá adquirir um bom conhecimento sobre as *MIBs* suportadas pelos agentes na rede.
- **Passo Três** – com este conhecimento, torna-se necessário a escolha sobre quais serão os objetos responsáveis pela obtenção dos indicadores de desempenho desejados.

No esquema proposto para análise de desempenho apresentado na Figura 4.7, a Análise simboliza a necessidade de intervenção do administrador da rede para a obtenção do sucesso nas etapas e o avanço da metodologia.

4.4.1.2 - Etapa Dois – (Coleta dos Objetos)

Contando com o bom conhecimento do administrador da rede sobre as *MIBs*, ele deverá realizar uma boa escolha sobre as possíveis ferramentas *SNMP* capazes da realização da coleta destes dados.

Existem várias ferramentas capazes de coletar diretamente os indicadores desejados, porém, muitas vezes, são ferramentas caras e de difícil acesso. Já outras ferramentas, como as baseadas no protocolo *SNMP*, podem ser encontradas livremente na Internet. Em vários casos elas não permitem a coleta direta dos indicadores escolhidos, tornando necessário relacionar e computar os dados coletados para a produção dos indicadores monitorados.

Na implementação desta etapa, recomenda-se, além da utilização de ferramentas que atendam os padrões *SNMP*, o uso de *Sniffers*. Para minimizar a carga gerada na rede com a coleta dos dados, torna-se necessário que o administrador da rede otimize o tempo de consulta (*polling*) ao banco de dados e ainda consiga realizar a tomada de decisão baseada em dados mais atuais possíveis (gerência pró-ativa).

4.4.1.3 - O Tempo de *Polling*

Devido à limitação do número de *traps* definidas pelo protocolo *SNMP*, a maioria das informações adquiridas pelo administrador da rede é empregando o

polling. Como o *polling* é feito apenas no momento de inicialização ou em resposta a uma *trap*, a estação de gerência pode ter uma visão desatualizada da rede [6].

Desta forma, surge a necessidade da definição de uma política para a freqüência com que a estação de gerência deve fazer o *polling*. Esta, por sua vez, está relacionada com o tamanho da rede e o número de agentes que podem ser efetivamente gerenciados pela estação de gerência. É difícil estabelecer o desempenho da estação, pois este depende de diversos fatores como velocidade de processamento, a velocidade de transferência de vários segmentos da rede, o nível de congestionamento na rede, entre outros. Entretanto, pode-se fornecer uma fórmula que dará uma idéia do valor escalar para esse tempo.

Para simplificar o problema, supõe-se que uma estação possa lidar apenas com um agente por vez. Isto é, quando o gerente requisita algo ao agente, ele não faz outra coisa até ter terminado o *polling* com este agente. Desta forma, consegue-se determinar o número máximo de agentes que a estação pode gerenciar, considerando a situação em que a estação de gerência está engajada o tempo todo (*full-time*) no *polling* [43].

Assumindo que T seja o intervalo de *polling* desejado para um mesmo agente e Δ o tempo médio para uma simples requisição, o número de agentes N pode ser obtido pela expressão $N \leq T/\Delta$. A quantidade Δ depende de diversos fatores [43]:

- Tempo que a estação de gerência leva para gerar um pedido;
- *Delay* do gerente ao agente;
- Tempo de processamento do agente para interpretar a mensagem;
- Tempo de processamento do agente para gerar a resposta;
- *Delay* do agente ao gerente;
- Tempo de processamento do gerente para receber e interpretar a resposta;
- Número de pedidos/respostas trocados para se obter toda a informação desejada do agente.

Observa-se que os fatores mencionados anteriormente serão limitados pela distância entre o gerente, que pode estar locado no *AP*, e o agente que pode estar a uma distância variável com relação à posição do *AP*, caso seja uma estação móvel. Outro fator limitante será a capacidade de processamento dos agentes locados em uma estação móvel e em uma estação fixa, trazendo também possíveis diferenças nos

tempos de processamento, pois poderão existir estações com capacidades de processamento diferentes. Em ambos os casos, surge a necessidade de realizar o cálculo utilizando um tempo médio.

A Figura 4.8 ilustra possíveis informações trocadas entre a estação gerente e os agentes em uma rede utilizando o protocolo *SNMPv.2*.

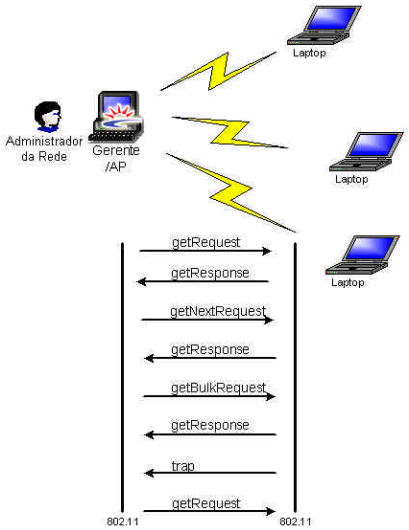


Figura 4.8 - *Possíveis Operações em uma Rede IEEE 802.11*

O tempo de *polling* é um fator importante para se conseguir analisar o desempenho da rede de forma pró-ativa. Desta forma, é preciso obter um tempo de *polling* otimizado, visando uma tomada de decisão pelo administrador da rede baseada em dados mais atuais possíveis.

4.4.2 – A Fase Dois (Eliminação de Dados e Obtenção dos Indicadores)

4.4.2.1 - Etapa Três (A Eliminação dos Dados Espúrios)

Nesta etapa, após a análise dos dados, pode-se retornar à Etapa Dois para uma nova coleta dos dados que tenham sido descartados por serem considerados espúrios e, portanto, inutilizáveis. Estes dados são, geralmente, amostras que não possuem significado físico. Um exemplo seria uma amostra de taxa de erros maior que a quantidade de quadros enviados ou recebidos pela rede no mesmo período. Se os dados coletados estão de acordo com esperado, o avanço para etapa seguinte é possível. Neste caso, pode-se obter todos os objetos responsáveis pelo indicador de desempenho de uma só vez, ou seja, sem a espera pela coleta de novos dados. A escolha dos novos dados a serem coletados dependerá da experiência do administrador da rede que estará conduzindo essa atividade. Administradores de rede

mais experientes podem investigar e diagnosticar os problemas de desempenho coletando um menor número de informações adicionais às já coletadas na fase anterior.

4.4.2.2 - Etapa Quatro (O Tratamento dos Dados Coletados)

Observa-se que para a obtenção do indicador de utilização da interface, por exemplo, deve-se relacionar as informações obtidas de três variáveis, *ifOutOctets, ifInOctets e ifSpeed.* É preciso lembrar que o protocolo *SNMP* não dá nenhuma garantia de tempo de entrega dos dados requisitados. Assim, torna-se necessário que as informações tenham sido requisitadas juntamente com seu tempo (*time stamp*) de registro na coleta dos objetos. Isto é importante, pois permitirá que os dados coletados na Fase Um possam ser relacionados em função de seu tempo de registro e não apenas por sua ordem de coleta. Ao chegar nesta etapa, considera-se que os dados são suficientes para serem tratados, tornando-se importante a escolha das ferramentas que podem realizar este tratamento. Recomenda-se que os dados coletados sejam consolidados por ferramentas já conhecidas como o *MS-EXCEL*, o *STAR-OFFICE* e outros softwares já dominados pelo público de informática. Haverá nesta etapa, além da obtenção dos indicadores de desempenho desejados, o tratamento dos dados a fim de fornecer uma interface amigável através da Média, Desvio Padrão e Coeficiente de Variação ao administrador da rede.

A seguir é apresentada a manipulação matemática que deve ser realizada para cada um dos indicadores de desempenho de redes mais comuns, relacionando-os com os objetos (variáveis) contidos na *MIB-II.*

- **Utilização (*Utilization*)**

Os objetos *ifOutOctets, ifInOctets* e *ifSpeed* serão utilizados para formar o indicador de utilização da interface. Os dois primeiros citados são contadores e são incrementados a cada grupo de oito bits (octetos) que atravessem a interface. Assim, pode-se pegar a quantidade de octetos, dividir pelo intervalo de tempo de observação e multiplicar por oito. Com isto, obtém-se o número de bits por segundo que passam pela interface no intervalo de tempo observado. Este valor ainda será dividido pela velocidade da interface (*ifSpeed*), que normalmente é a sua taxa de transmissão nominal. Com este procedimento, obtém-se a utilização da interface de forma

adimensional. Pode-se ainda, multiplicar este valor por 100 para encontrar o percentual de ocupação da interface [44].

- **Taxa de erros (*Accurancy*)**

Os objetos *ifInErrors* e *ifOutErrors* fornecerão a quantidade de pacotes com erros recebidos e enviados, respectivamente. Para saber a percentagem de pacotes que tiveram erros, esses valores deverão ser divididos pela quantidade total de pacotes que passaram pela interface. Esse total de pacotes será obtido somando as quantidades dos objetos *ifInUcastPkts, ifInNUcastPkts, ifOutUcastPkts* e *ifOutNUcastPkts* [44].

- **Vazão (*Throughput*)**

Para compor o indicador *Vazão*, que neste caso será vazão de pacotes, é preciso obter os valores de quatro objetos do grupo *Interfaces* da *MIB-II* que são: *ifInUcastPkts, ifInNUcastPkts, ifOutUcastPkts* e *ifOutNUcastPkts.* Os dois primeiros somados e divididos pelo tempo de observação nos darão a vazão de entrada em pacotes por segundo, enquanto os outros dois, a vazão de saída da interface [44].

- **Disponibilidade (*Availability*)**

Com o objeto *ifOperStatus*, pode-se verificar o *status* da interface. A disponibilidade da interface ao longo do tempo que o sistema se manteve operacional será obtida dividindo-se o somatório dos tempos em que a interface esteve em funcionamento (operacional) pelo tempo total de operação do sistema. No grupo *System*, consegue-se obter o objeto *sysUpTime*, o qual informa a quanto tempo o sistema está funcionando. Com o objeto do grupo *Interfaces ifLastChange* [44], sabe-se quando a interface mudou seu estado operacional. Portanto, utilizando esses objetos obtém-se o intervalo de tempo em que a interface ficou disponível para o usuário. Na Figura 4.9 ilustra-se essa possibilidade.

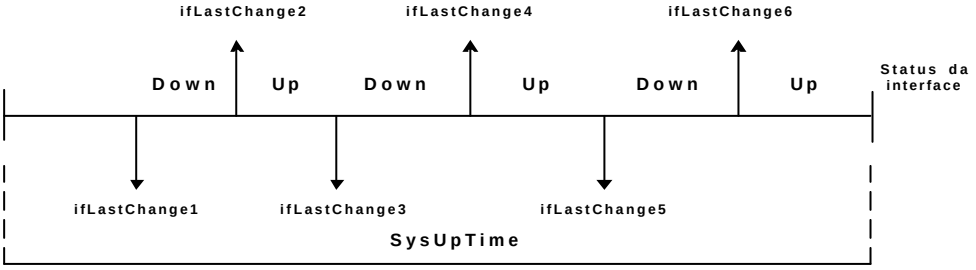


Figura 4.9 - *Exemplo das Alterações do Status de uma Interface*

Quando o *status* da interface é alterado, o instante de tempo em que isto ocorre é registrado no objeto *ifLastChange*. Além deste dado, é necessário registrar também qual era o *status* da interface, se operante (*Up*) ou inoperante (*Down*). Assim, será obtida a disponibilidade de uma interface ao longo de um certo tempo de funcionamento do sistema (*sysUptime*). É importante observar que o agente deverá ser capaz de armazenar os diversos valores do *ifLastChange* relacionando-os com o *ifOperStatus* durante o tempo de observação do sistema. Assim, quando o administrador da rede acionar a ferramenta de coleta, haverá como saber o intervalo de tempo no qual a interface permaneceu disponível.

- **Tempo de resposta (*Response Time*)**

Outro indicador de desempenho interessante para análise seria o Tempo de Resposta. O *SNMP*, através da *MIB-II*, não possui objetos que forneçam dados referentes a tempos de resposta e atraso fim-a-fim. E através dos objetos da *MIB* IEEE 802.11 e da proprietária, também não são encontrados tais objetos. Desta forma, torna-se impossível a obtenção deste indicador, a não ser que seja feito o uso de outras soluções. Uma possibilidade seria a construção de uma ferramenta de software que, uma vez instalada na máquina do cliente, pudesse contar o tempo de resposta para cada requisição lançada na rede. A elaboração de uma aplicação que envie mensagens *ICMP* que tragam como informação o tempo de resposta também pode ser usada. Outra alternativa mais simples, porém mais grosseira, seria cronometrar os tempos de resposta do ponto de vista do grupo dos agentes.

Por exemplo, existem outros indicadores de desempenho que possuem valores padrões de qualidade estabelecidos, como se observa na Tabela 4.2. Estes indicadores são típicos de *LANs* 802.x inspirados na obra de Jain [31].

Tabela 4.2 – *Indicadores de Desempenho e Padrões de Qualidade*

Indicadores	Padrões de Qualidade
Erros Físicos	$<10^{-4}$ por segundo
Tempo de Resposta	<15 segundos
Utilização da Banda Passante	<65% em redes sem disputa por meio físico ou <20% em redes com disputa pelo meio físico
Colisões (Quando Aplicável)	<15 por segundo
Tempo de Circulação do Token (Quando Aplicável)	<250 milisegundos

Estes padrões de qualidade visam estipular medidas limites para os indicadores selecionados, garantindo assim, caso as medidas coletadas da rede estejam abaixo desses limites, um desempenho que não comprometa a qualidade de serviço da rede. O usuário final enxerga a qualidade de serviço fornecida pela rede como disponibilidade e baixo tempo de resposta.

Existem dois indicadores de qualidade: Colisões e Tempo de Circulação do *Token*, que dependem da tecnologia *LAN* adotada pela rede em estudo. É muito importante manter o menor número possível de indicadores de qualidade, mantendo um compromisso entre a utilidade das informações coletadas e a garantia de um processo suficientemente rápido para permitir sua execução pró-ativa.

Na Tabela 4.3, pode-se observar os objetos (variáveis) que devem ser coletados para formarem esses indicadores de desempenho.

Tabela 4.3 – *Indicadores de Desempenho e Objetos (Variáveis)*

Indicadores	Objetos (variáveis)
Erros Físicos	ifInErrors + ifOutErrors
Utilização da Banda Passante	(ifInOctets + ifOutOctets)/ (Tempo * Banda Passante do Meio)
Colisões (Quando aplicável)	IfCollision
Tempo de Circulação do Token (Quando aplicável)	IfTokenHolding

4.4.3 – A Fase Três (Interpretação do Administrador da Rede)

Agora pode ser considerado que o administrador da rede possui os indicadores de desempenho juntamente com as medidas estatísticas que facilitam o entendimento do que está acontecendo com a rede. Nesta fase, é importante poder contar com uma boa experiência do administrador da rede, de forma a possibilitar a interpretação correta e rápida do que está acontecendo com a mesma. Uma simples reconfiguração de capacidades instaladas ou ajuste de parâmetros de serviços pode devolver ao sistema a condição de desempenho desejada. Com isto, existe a possibilidade de retorno à Etapa Dois para a realização de novas coletas com o tempo de *polling* atualizado com a nova situação da rede. Desta forma, o administrador da rede pode confirmar se o problema foi resolvido. Caso o problema de capacidade da rede não seja resolvido, ou se deseje ampliar o *backbone* da mesma, tem-se a

necessidade de execução da Fase Quatro da metodologia. Muito embora o administrador da rede possa ter à sua disposição uma boa gama de indicadores de desempenho, no entanto, quando se refere ao Planejamento de Capacidade, será importante monitorar os dispositivos pertencentes ao grupo Facilidades de Comunicação. Estes dispositivos são responsáveis por apresentarem possíveis pontos de gargalo na rede, sendo que o indicador de desempenho Utilização pode refletir esta situação rapidamente.

4.4.4 – A Fase Quatro (Processo de Simulação)

O objetivo desta fase é caracterizar o tráfego, permitindo o Planejamento de Capacidade do ambiente através de simulação digital. De posse dos resultados da simulação, o administrador da rede terá informações capazes de lhe auxiliar a tomar as decisões mais cabíveis para a manutenção de desempenho da rede a curto e em longo prazo. Com todas as alterações realizadas na rede, torna-se necessário o retorno à Etapa Dois para coletar os dados que formarão os mesmos indicadores de desempenho empregados antes de sua modificação. Desta forma, é preciso que haja um armazenamento dos dados coletados para a situação inicial e atual da rede, possibilitando a criação do seu histórico. Isto permitirá uma comparação e a caracterização ou não da solução do problema de capacidade da rede.

Para a execução desta fase, é necessária a realização das seguintes etapas:

- **Etapa Um** - Coletar as informações necessárias à caracterização dos eventos a serem estudados.
- **Etapa Dois** - Modelagem estocástica dos eventos, incluindo, quando pertinente, seus relacionamentos com os demais objetos relevantes ao estudo (matrizes de fluxo, relações temporais e etc.).
- **Etapa Três** - Simulação para ajuste do modelo (tantas vezes quanto for necessário para aferir o modelo em questão).

Na etapa de simulação haverá a abertura em cinco passos, os quais são necessários ao processo de simulação:

- **Passo Um** – realizar a geração do tráfego e a montagem da topologia da rede baseados na situação real da rede.
- **Passo Dois** – selecionar as estatísticas importantes a serem coletadas pelo simulador.

- **Passo Três** – coletar as estatísticas para formar um padrão inicial. Assim, futuras modificações na rede, como o aumento do número de usuários e o emprego de novas aplicações, podem ser comparados a uma situação anterior.
- **Passo Quatro** – realizar as alterações no modelo, comparar com o modelo inicial e detectar os problemas.
- **Passo Cinco** – propor as soluções e analisar os novos resultados.

No final da etapa de simulação, o administrador da rede, contando com a implementação prática da solução proposta com base na simulação, deverá retornar à etapa de coleta dos dados atualizados com a nova situação da rede e verificar se as alterações na rede (tanto com a adição de capacidade quanto com a alteração de cargas e topologia) foram bem sucedidas.

Esta fase pode requerer uma caracterização estocástica do tráfego da rede. Recomenda-se aqui o uso de um *Sniffer* ou do padrão *RMON* para alguns relatórios complementares. É importante caracterizar no início dessa fase a carga de trabalho gerada por cada estação, bem como sua composição em termos de serviço. A grande maioria dos *Sniffers* é capaz de construir registros (*logs*) detalhados sobre o tráfego que está passando. Os arquivos resultantes da coleta devem ser de padrão aberto, permitindo o tratamento dos dados por outro software, caso seja necessário.

O tratamento de dados dessa fase consiste nas seguintes etapas:

- Separar, dentre os dados coletados, o tráfego de cada estação;
- Dentre os dados de cada estação, separar o tráfego de cada serviço;
- Dentre os dados de cada serviço, calcular a média, o desvio padrão e o coeficiente de variação do volume de dados trafegados para cada ocorrência do serviço, tempo entre ocorrências do serviço e as curvas aproximadas de distribuição de probabilidade para esses dois parâmetros.

Muitas vezes duas ou mais estações apresentarão comportamentos muito semelhantes. Nessa situação é possível representá-las como uma única entidade com o dobro ou n vezes mais cargas que o normal. Isso facilita na construção do modelo de simulação. Porém, deve-se considerar que quanto mais simplificações (utilizando agrupamento em perfis de usuários) forem feitas, menor fica a flexibilidade de manobra na inferência de novos cenários no ambiente de simulação.

É muito importante que todo o modelo de simulação seja aferido. A aferição visa garantir que os resultados obtidos do modelo reflitam a realidade do processo. Várias rodadas de simulação devem ser feitas para que o modelo atinja um comportamento próximo da realidade. Assim, quando o comportamento próximo ao real for atingido, ou seja, com diferentes rodadas de simulação os resultados apresentarem poucas variações, o modelo poderá ser considerado aferido.

Após a etapa de aferição, novos cenários podem ser testados, até que uma solução interessante possa ser encontrada. Mais uma vez, para cada cenário testado, várias rodadas de simulação devem ser efetuadas, garantindo a validade dos dados obtidos diante dos processos aleatórios envolvidos.

Caso o simulador possua a facilidade de importação dos dados compatível com o arquivo gerado pelo software de coleta dos dados, não haverá a necessidade da caracterização estocástica do tráfego da rede.

Capítulo V

5 – Aplicação da Metodologia Proposta

A fim de validar a metodologia proposta, foi criado um estudo de caso que na realidade é dividido em duas partes. Na primeira, é utilizado um arquivo fornecido pela ferramenta de coleta *MRTG*[â] (ver Anexo A) em uma rede IEEE 802.11 no intuito de apresentar uma possibilidade de tratamento dos dados. Na segunda parte, supõe-se a necessidade do processo de simulação. Para isto, foi criado um cenário baseado em um tráfego de dados fictício, visando mostrar o Planejamento de Capacidade utilizando o processo de simulação, proposto na Fase Quatro da metodologia. O estudo de caso focou na análise da *MIB* do *AP* da *BreezeCom*, onde se buscou os objetos que pudessem auxiliar na obtenção dos indicadores escolhidos e em especial nos objetos que trouxessem informações sobre a taxa de transmissão e o tempo de *polling*.

5.1 – A Fase Um (Escolha e Coleta dos Objetos)

5.1.1 - Etapa Um (Escolha dos Objetos)

- **Passo Um (Escolha do Grupo Gerenciado)**

O grupo de aplicação da metodologia será o Facilidades de Comunicação, devido à sua visão privilegiada do processo de transação que ocorre na rede. Além disso, através dos resultados obtidos com a aplicação da metodologia nesse grupo, será mais fácil localizar os problemas de desempenho, mesmo que esses residam em outro grupo de elementos.

- **Passo Dois (Estudando as *MIBs*)**

De acordo com a proposta, é necessário um estudo inicial sobre as *MIBs* para se conhecer os objetos que podem ser utilizados. Como identificado na proposta, os objetos mais interessantes pertencem ao grupo *Interfaces*, o qual contém os objetos responsáveis pelo gerenciamento de desempenho de uma rede e é parte integrante da *MIB-II*. No entanto, observa-se na *MIB* proprietária da *BreezeCom* [41], que há

objetos capazes de informar de forma mais detalhada sobre quais são os pacotes que entram ou que saem das interfaces. Como exemplo, são observados os seguintes objetos:

- *BrzRetryOnWlan* – contém o número total de fragmentos retransmitidos na rede sem fio.
- *BrzRxWlanCnt* – informa o número total de quadros de dados e gerenciamento que foram recebidos com sucesso da rede sem fio.
- *BrzRxMSDUFromWlan* – informa o número total de quadros de dados que foram recebidos pelo *AP* com sucesso da rede sem fio.
- *BrzRxFragFromWlan* – possui o mesmo significado do objeto *aReceivedFrame-Count* da *MIB* IEEE 802.11, informando o número de fragmentos de quadros de dados e gerenciamento que foram recebidos sem erro da rede sem fio.
- *BrzRxBadFragFromWlan* – é um contador incrementado quando um erro é detectado em um fragmento recebido da rede sem fio.
- *BrzRxDuplicateFragFromWlan* – possui o mesmo significado do objeto *aFrame-DuplicateCount* da *MIB* IEEE 802.11, sendo um contador incrementado quando um fragmento duplicado é recebido da rede sem fio.
- *BrzDiscarded* – conta o número de quadros de dados que são internamente descartados no sistema, não sendo transmitidos pela rede sem fio. Um alto valor deste contador indica a possibilidade de estar havendo um alto volume de tráfego ou um ambiente ruidoso impedindo as transmissões.
- *BrzFailedCountOnWlan* – possui o mesmo significado do objeto *aFailedCount*. Conta o número de quadros que não são transmitidos, devido ao número de tentativas de retransmissões excederem ao valor do *RetryMax*.

Vários outros objetos são encontrados na *MIB* proprietária da *BreezeCom*. No entanto, somente alguns são descritos no intuito de apresentar as suas utilidades no gerenciamento. Alguns objetos nas *MIB*s IEEE 802.11, pública e proprietária são opcionais e possuem informações idênticas. Desta forma, verifica-se a importância do conhecimento do administrador da rede sobre os objetos implementados nas *MIBs* dos dispositivos gerenciados.

A Figura 5.1 ilustra o grupo *Interfaces* da *MIB-II* e os objetos que fazem parte deste grupo são mostrados na Tabela 5.1 com suas respectivas descrições. Destes objetos, os que interessam ao desempenho são descritos no próximo item.

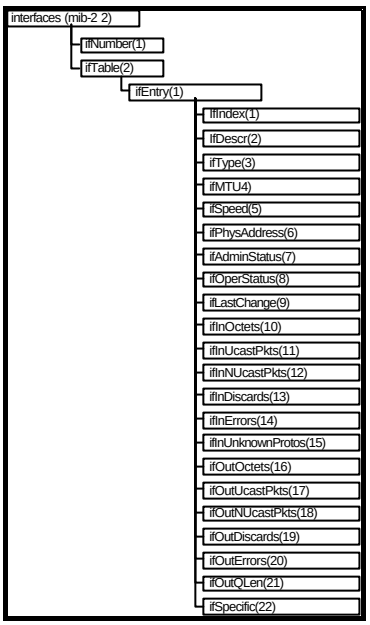


Figura 5.1 – *Grupo Interfaces da MIB-II*

Toda informação contida no grupo *Interfaces* é genérica e assim aplicável a qualquer tipo de interface.

Tabela 5.1 – *Descrição dos Objetos do Grupo Interfaces*

Objeto	Descrição	Acesso
ifNumber	Número de interfaces de rede	RO
ifTable	Uma lista de entradas de interface	NA
ifEntry	Uma entrada de interface	NA
ifIndex	Um valor único para cada interface	RO
ifDescr	Informação sobre a interface, incluindo nome do fabricante, nome do produto e versão da interface de hardware	RO
ifType	Tipo da interface, diferenciada de acordo com o protocolo de acesso e de enlace	RO
ifMtu	O tamanho da unidade de dados do protocolo (PDU), em octetos, que pode ser enviado e recebido pela interface	RO
ifSpeed	Largura de banda da interface em bits por segundo	RO
ifPhysAddress	Endereço da interface na camada de protocolo logo abaixo da camada de rede	RO
ifAdminStatus	Estado desejado da interface *(up(1), down(2), testing(3))*	RW
ifOperStatus	Estado atual da interface *(up(1), down(2), testing(3))*	RO
ifLastChange	Valor de *sysUpTime* quando a interface entrou em modo de operação	RO
ifInOctets	Número total de octetos recebidos pela interface	RO
ifInUcastPkts	Número de pacotes unicast recebidos	RO
ifInNUcastPkts	Número de pacotes no-unicast recebidos	RO
ifInDiscards	Número de pacotes descartados de entrada	RO
ifInErrors	Número de pacotes recebidos com erros	RO
ifInUnknownProtos	Número de pacotes descartados por causa de protocolo desconhecido	RO
ifOutOctets	Número total de octetos enviados pela interface	RO
ifOutUcastPkts	Número de pacotes unicast enviados	RO
ifOutNUcastPkts	Número de pacotes no-unicast enviados	RO
ifOutDiscards	Número de pacotes descartados na saída	RO
ifOutErrors	Número de pacotes não transmitidos por causa de erros	RO
ifOutQLen	Tamanho da fila de pacotes de saída	RO
IfSpecific	Referencia para MIB específicas de meios de comunicação sendo usado na interface	RO

- **Passo Três (Objetos Selecionados para a Análise de Desempenho)**

Para a realização do monitoramento de desempenho é preciso coletar as informações de alguns objetos do grupo *Interfaces* da *MIB-II*, além de outros objetos da *MIB* IEEE 802.11 e da *MIB* proprietária do equipamento. Esses objetos formarão os indicadores de desempenho [37] [41] [43] [44] [45] citados no Capítulo 3 e na metodologia proposta.

De acordo com a descrição dos objetos da Tabela 5.1, da *MIB* IEEE 802.11 e da *MIB* proprietária da *BreezeCom*, obtêm-se os objetos referentes aos indicadores de desempenho: Utilização, Taxa de Erros, Vazão e Disponibilidade. Estes objetos tornam-se interessantes em uma possível coleta e são ilustrados na Tabela 5.2. Para o Tempo de Resposta não foram encontrados objetos.

Tabela 5.2 – *Possíveis Objetos Utilizados para Formar os Indicadores de Desempenho*

Utilização	Taxa de erros	Vazão	Disponibilidade	Tempo de resposta
IfOutOctets	IfInErrors	IfInUcastPkts	SysUpTime	Não há objetos
IfInOctets	IfOutErrors	IfInNUcastPkts	IfLastChange	---
IfSpeed	IfInUcastPkts	IfOutUcastPkts	IfOperStatus	---
IfSpecific	IfInNUcastPkts	IfOutNUcastPkts	---	---
Dot11OperationalRateSet	IfOutUcastPkts	---	---	---
StCurTxRate	IfOutNUcastPkts	---	---	---
StMaxRate	---	---	---	---

A partir dos objetos ilustrados na Tabela 5.2, deve-se realizar as manipulações matemáticas de forma a obter os indicadores de desempenho desejados, como será apresentado na Fase Dois. Vale observar que o equipamento de determinado fabricante poderá disponibilizar *MIBs* com objetos que possuam a mesma informação, porém com nomes diferentes ou mesmo objetos que informem de forma mais direta os indicadores de desempenho. Sendo assim, torna-se necessário que os objetos sejam bem definidos por parte do usuário do sistema de gerência.

Com a escolha do grupo Facilidades de Comunicação, torna-se interessante verificar a utilização, por exemplo, da interface de um dispositivo de rede que reflita

a ocupação de um determinado enlace. Com isto, os objetos responsáveis pelo indicador de desempenho Utilização (*ifOutOctets, ifInOctets e ifSpeed*) deverão ser coletados, minimizando a carga gerada na rede com a coleta dos demais objetos que para a situação criada é desnecessária.

5.1.2 - Etapa Dois (Coleta dos Objetos)

Para a realização desta etapa é importante um estudo sobre alguns softwares capazes de coletar os dados referentes aos indicadores desejados, de forma a possibilitar o seu emprego consciente. Esta análise, apresentada no Anexo A, resultou na escolha do software *MRTG*[â] para a realização da etapa de coleta dos objetos. O *MRTG*[â] fornece a possibilidade da obtenção da taxa de bytes que entra na interface do *AP* através de um *script*.

5.1.2.1 - O Cálculo do Tempo de *Polling*

Com a utilização do *MRTG*[â], não haverá um cálculo para o tempo de *polling*, já que a consulta à *MIB* é gerada a cada 30 segundos e a coleta será em cima de um *AP* e não de estações de redes sem fio. A fim de mostrar como este cálculo pode ser realizado utilizando objetos da *MIB* da *BreezeCom*, são apresentadas a seguir algumas possibilidades.

Partindo do princípio que o *AP* e cada estação sem fio suportem a arquitetura *SNMP*, pode-se obter diretamente, na já citada *MIB* proprietária da *BreezeCom*, o número de estações que estão atualmente associadas com seu *AP*, determinando o número de agentes *SNMP*, este objeto recebe o nome de *bssNumOfStations* [41]. Com isto, torna-se possível otimizar o tempo de *polling*, já que ele deverá respeitar a relação descrita na seção 4.4.1.3. Pode-se ainda estimar um tempo de *polling* para o pior caso, onde se supõe o número máximo de estações, utilizando o objeto *bssNumOfStationsPeak* da *MIB* proprietária da *BreezeCom*. Deve-se notar que o intervalo de *polling* será tanto maior quanto maior o número de agentes *SNMP*, fazendo que a freqüência com que o número de consultas realizadas a cada agente diminua. Isto pode trazer uma carga de gerência menor à rede sem fio. Por outro lado, a coleta de informações pode ser prejudicada, considerando-se uma rede sem fio com muitas estações em *roaming* e com alta mobilidade. Este mesmo raciocínio é utilizado para o cálculo do tempo de *polling* em redes cabeadas. No entanto, a entrada e a saída de estações não estaria ocorrendo de forma dinâmica através de

informações trocadas com o *AP* no nível da camada *MAC*, mas pela atuação mecânica de alguma pessoa que dá suporte à rede. Sendo assim, pode-se calcular um tempo de *polling* e este permanecer inalterado ao longo de boa parte da operação da rede cabeada, enquanto nas redes sem fio este tempo deverá ser ajustado freqüentemente.

5.2 – A Fase Dois (Eliminação de Dados e Obtenção dos Indicadores)

5.2.1 - Etapa Três (A Eliminação dos Dados Espúrios)

Como não haverá a coleta de dados em um ambiente real, será proposto um tratamento de dados reais retirados do endereço eletrônico http://hpnms02.Hartfordschools.org/mrtg/wlan/aa_aironet01_10.224.40.23.log, a fim de ilustrar uma maneira de realizar esse tratamento.

Nesta etapa não foram encontrados dados que fossem considerados espúrios. No entanto, como o arquivo do tráfego gerado pela coleta feita através do *MRTG*â corresponde a um período de mais de três dias, propõe-se a eliminação de alguns dados, deixando somente os referentes às 24 horas mais atuais. A justificativa para esta necessidade será apresentada na etapa seguinte.

5.2.2 - Etapa Quatro (O Tratamento dos Dados Coletados)

De posse dos dados coletados, pode-se realizar o tratamento voltado à obtenção dos indicadores de desempenho, gráficos e medidas estatísticas sobre o tráfego na rede de forma a facilitar o gerenciamento.

Dentre as possíveis coletas de dados realizadas pelo *MRTG*â, a obtenção direta da taxa de bytes que passa pelo *AP* (Portal) é ilustrada na Figura 5.2.

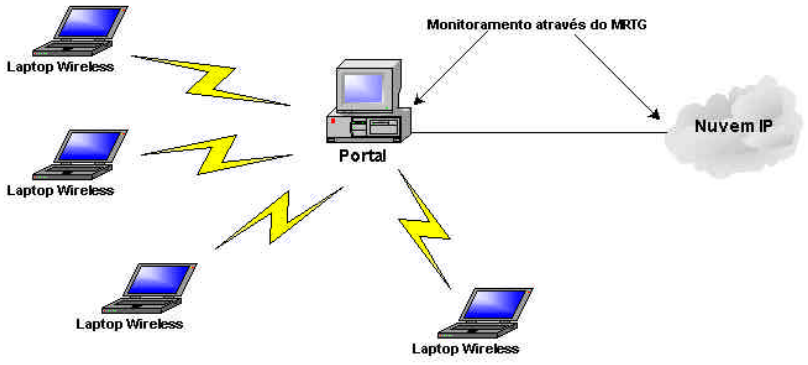
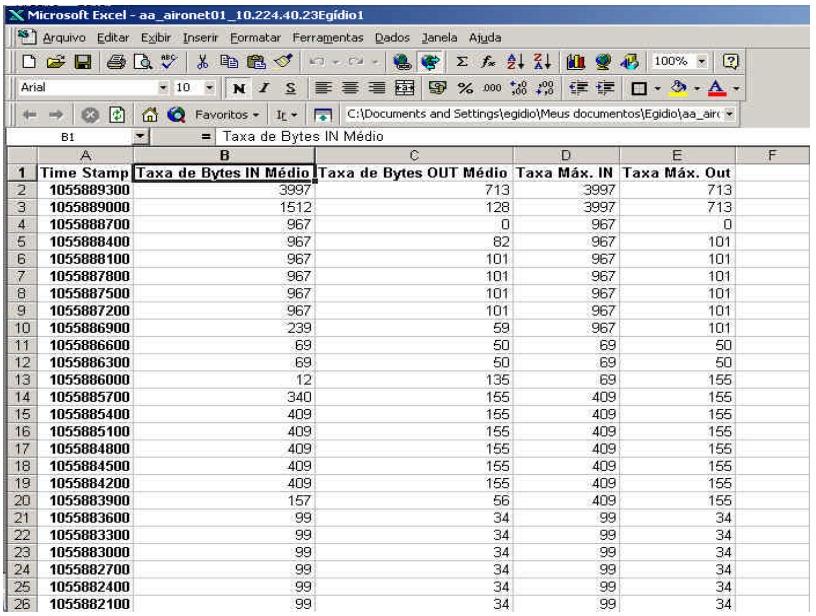


Figura 5.2 - *Coleta de Dados através do MRTG*â *para o Tráfego da Rede IEEE 802.11*

Embora os dados do *MRTG*â forneçam tanto um arquivo de registro como também os gráficos referentes a este arquivo, é preciso tratar estes dados para uma melhor visualização utilizando a média, desvio padrão e o coeficiente de variação do indicador de desempenho Utilização. Além disso, a obtenção de todos os indicadores de desempenho propostos requer o tratamento dos dados. Desta forma, propõe-se o tratamento baseado na utilização dos recursos gráficos do *Microsoft*â *Excel*. Esta escolha favorece a automatização do tratamento dos dados coletados através da criação de macros (programação em *Visual Basic* nativo), além de possuir funções matemáticas para o cálculo direto das medidas estatísticas sobre os dados. Essas macros geram as informações a partir de arquivos (*.TXT*) [46].

A Figura 5.3 ilustra parte do tráfego coletado pelo *MRTG*â e importado para o *Excel* sem o tratamento dos dados. Esse tráfego passa pelo *AP* da *Cisco Aironet*â *DSSS*, o qual compõe uma rede Infra-estruturada IEEE 802.11b.



	A	B	C	D	E	F
1	Time Stamp	Taxa de Bytes IN Médio	Taxa de Bytes OUT Médio	Taxa Máx. IN	Taxa Máx. Out	
2	1055889300	3997	713	3997	713	
3	1055889000	1512	128	3997	713	
4	1055888700	967	0	967	0	
5	1055888400	967	82	967	101	
6	1055888100	967	101	967	101	
7	1055887800	967	101	967	101	
8	1055887500	967	101	967	101	
9	1055887200	967	101	967	101	
10	1055886900	239	59	967	101	
11	1055886600	69	50	69	50	
12	1055886300	69	50	69	50	
13	1055886000	12	135	69	155	
14	1055885700	340	155	409	155	
15	1055885400	409	155	409	155	
16	1055885100	409	155	409	155	
17	1055884800	409	155	409	155	
18	1055884500	409	155	409	155	
19	1055884200	409	155	409	155	
20	1055883900	157	56	409	155	
21	1055883600	99	34	99	34	
22	1055883300	99	34	99	34	
23	1055883000	99	34	99	34	
24	1055882700	99	34	99	34	
25	1055882400	99	34	99	34	
26	1055882100	99	34	99	34	

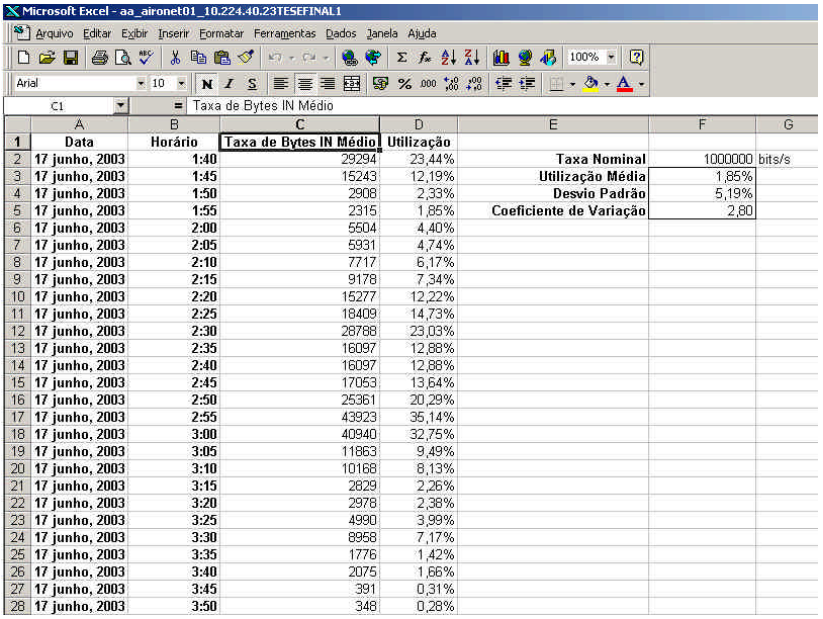
Figura 5.3 - *Tráfego Importado para o Excel sem Tratamento*

Agora, é preciso obter as medidas estatísticas sobre estes dados, de forma a apresentar algo mais palpável ao administrador da rede. Vale observar que os dados apresentados em cada campo das colunas B, C, D e E do *Excel* são referentes à média da taxa dos bytes coletados no intervalo de 5 minutos.

A Figura 5.4 mostra a tabela do *Excel* com o tratamento da coluna C (Taxa de Bytes IN Médio), o mesmo procedimento pode ser feito para as demais colunas.

Como os gráficos gerados pelo *MRTG*$^{\hat{a}}$ trazem informações por dia, semana, mês e até ano, tornou-se interessante exemplificar uma situação onde fossem mostradas informações na escala de horas em um período de 24 horas entre dois dias. Isto pode ser feito também para um dia específico, bastando que sejam selecionados somente os dados correspondentes ao dia em questão. Observa-se na coluna A da Figura 5.3, onde é colocado o valor em segundos referente à coleta (*Time Stamp*), que este valor é decrescente, ou seja, o tempo mostrado em A2 é o mais atual. Sendo assim, inicialmente foram invertidas as seqüências das colunas A e B, e para facilitar o entendimento do Administrador de Rede, também houve a conversão do *Time Stamp* em data e hora, como se verifica na Figura 5.4.

Toda a planilha corresponde a 922 linhas de dados coletados, contudo foram utilizadas apenas 288, correspondendo às 24 horas de coleta mencionadas. Na coluna D tem-se o valor da Utilização Instantânea, no entanto, a referência foi feita somente ao termo Utilização, já que este valor, como dito anteriormente, corresponde a uma taxa média em 5 minutos de observação. Vale ressaltar que a Utilização é referente aos bits que entram na interface.


Microsoft Excel - aa_aironet01_10.224.40.23TESEFINAL1

Arquivo Editar Exibir Inserir Formatar Ferramentas Dados Janela Ajuda

C1 = Taxa de Bytes IN Médio

	A	B	C	D	E	F	G
1	Data	Horário	Taxa de Bytes IN Médio	Utilização			
2	17 junho, 2003	1:40	29294	23,44%	Taxa Nominal	1000000	bits/s
3	17 junho, 2003	1:45	15243	12,19%	Utilização Média	1,85%	
4	17 junho, 2003	1:50	2908	2,33%	Desvio Padrão	5,19%	
5	17 junho, 2003	1:55	2315	1,85%	Coeficiente de Variação	2,80	
6	17 junho, 2003	2:00	5504	4,40%			
7	17 junho, 2003	2:05	5931	4,74%			
8	17 junho, 2003	2:10	7717	6,17%			
9	17 junho, 2003	2:15	9178	7,34%			
10	17 junho, 2003	2:20	15277	12,22%			
11	17 junho, 2003	2:25	18409	14,73%			
12	17 junho, 2003	2:30	28788	23,03%			
13	17 junho, 2003	2:35	16097	12,88%			
14	17 junho, 2003	2:40	16097	12,88%			
15	17 junho, 2003	2:45	17053	13,64%			
16	17 junho, 2003	2:50	25361	20,29%			
17	17 junho, 2003	2:55	43923	35,14%			
18	17 junho, 2003	3:00	40940	32,75%			
19	17 junho, 2003	3:05	11863	9,49%			
20	17 junho, 2003	3:10	10168	8,13%			
21	17 junho, 2003	3:15	2829	2,26%			
22	17 junho, 2003	3:20	2978	2,38%			
23	17 junho, 2003	3:25	4990	3,99%			
24	17 junho, 2003	3:30	8958	7,17%			
25	17 junho, 2003	3:35	1776	1,42%			
26	17 junho, 2003	3:40	2075	1,66%			
27	17 junho, 2003	3:45	391	0,31%			
28	17 junho, 2003	3:50	348	0,28%			

Figura 5.4 - *Tráfego Importado para o Excel com Tratamento*

A Figura 5.5 ilustra em gráfico de barras as diferenças dessas medidas estatísticas.

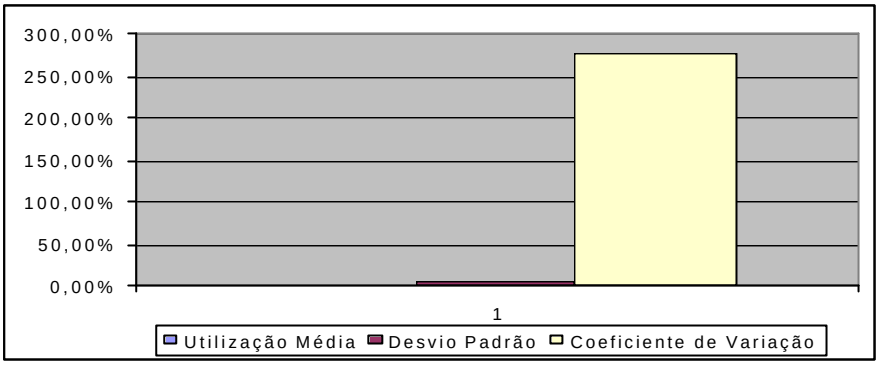


Figura 5.5 – *Comparação das Estatísticas Geradas por um Período de 24 Horas de Observação*

A Figura 5.6 ilustra o gráfico da utilização do enlace no sentido *IN* (bytes que entram no *AP*) entre os dias 17/06 e 18/06 por um período de 24 horas.

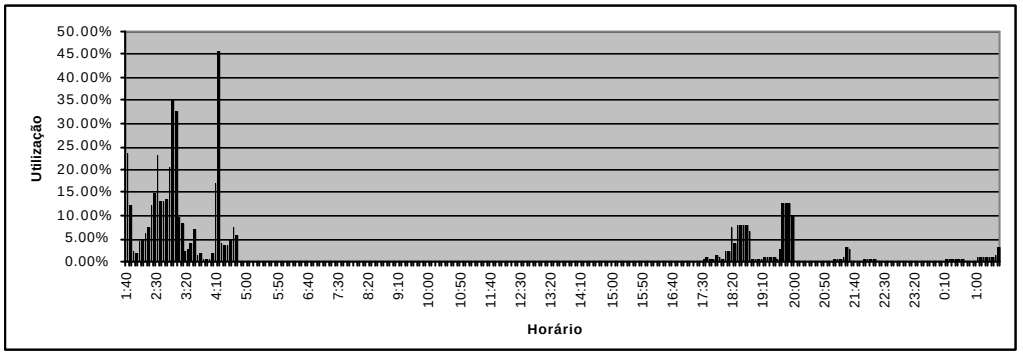


Figura 5.6 *– Utilização por um Período de 24 Horas de Observação*

Da mesma maneira que foram tratados estes dados coletados pelo *MRTG*[â], é possível prosseguir e formar os demais indicadores de desempenho desejados. Para isto, torna-se necessário que no *script* fornecido pelo *MRTG*[â] seja indicado quais os objetos desejam ser coletados (*ifInErrors*, *ifOutErrors*, etc). O mesmo tratamento estatístico aplicado à taxa de bytes da coluna B pode ser realizado na coluna C apresentada na Figura 5.3 referente aos bits que saem da interface do *AP*.

Em se tratando da coleta realizada pelo *MRTG*[â], existe em seu *script* a definição da taxa de transmissão da interface em análise, como se pode observar no Anexo A. Contudo, partindo do princípio de que não se conhece a taxa de transmissão do equipamento, será necessário um objeto encontrado na *MIB* proprietária para obtenção do indicador Utilização. Poderia se pensar no objeto *ifSpeed* citado na proposta para especificar a taxa nominal do equipamento. Porém, os equipamentos para redes IEEE 802.11 geralmente dispõem de mais de uma taxa de transmissão, como o equipamento *SA-40 Pro.11* da *BreezeCom* [41], com 1, 2 ou

3 Mbps, dependendo das condições do meio de transmissão, sendo assim, torna-se necessário a busca de um objeto na *MIB* proprietária do equipamento que traga a informação exata da taxa em que este estará transmitindo. Este objeto para o equipamento da *BreezeCom* será o *stCurTxRate*, que indica a taxa atual utilizada pelo *AP* para transmitir seus pacotes para a estação.

5.3 - A Fase Três (Interpretação do Administrador da Rede)

Agora, de posse das medidas estatísticas, juntamente com o gráfico, o administrador da rede dispõe de uma interface mais amigável. No entanto, não se pode desconsiderar a importância do grau de experiência do administrador da rede na análise dos resultados. Este fato será importante para que sejam tomadas as decisões mais corretas baseadas no menor tempo possível e com informações coletadas de forma mais otimizada. Por exemplo, o administrador da rede deverá saber que o coeficiente de variação representa o quociente entre o desvio padrão e a média e que esta medida estatística indica a proximidade dos valores coletados da média, quando o desvio padrão é pequeno. Desta forma, em medidas de tráfego, o administrador da rede deverá interpretar um valor baixo do coeficiente de variação como uma utilização constante. Para um valor alto, esta medida estatística estará indicando um tráfego em rajadas.

Na Figura 5.5 mostrada anteriormente, foram verificados valores relativamente pequenos para Utilização Média. Isto é explicado facilmente, já que o tráfego que entra no *AP* é muito pequeno durante grande parte do período de observação. Para o Desvio Padrão, que é uma medida do grau de dispersão dos valores em relação à Utilização Média, tem-se um valor relativamente alto, originando um elevado Coeficiente de Variação. Este valor elevado do Coeficiente de Variação pode estar indicando neste caso, que mais estações móveis gerando tráfego externo chegaram ao *BSS*, saíram, ou mesmo, as que já estavam registradas iniciaram requisições à rede externa.

Para este estudo de caso, o administrador da rede não encontrou nenhum problema na utilização da interface. Sendo assim, ele deve reiniciar o processo quantas vezes julgar necessário, coletando os dados essenciais ao bom funcionamento da rede e se em algum momento verificar alguma anomalia no indicador de desempenho Utilização, poderá entrar na Fase Quatro. Caso o

administrador da rede queira avaliar a ampliação do alcance do *backbone* da sua rede ou qualquer outra alteração, ele também entrará na Fase Quatro.

5.4 - A Fase Quatro (Processo de Simulação)

Como dito anteriormente, a utilização da interface do *AP* analisada pelo administrador da rede possui um valor admissível. No entanto, para ilustrar o processo de simulação, será considerado um tráfego fictício. Desta forma, o administrador da rede estará utilizando a fase de simulação para a solução do problema. Além disso, também será considerada a necessidade de ampliação do *backbone* da rede existente.

Não será necessário o tratamento dos dados coletados para a realização do processo de simulação, eliminando-se as Etapas Um e Dois desta fase, já que será utilizada a ferramenta de simulação *OPNET® Modeler* que permite a importação direta dos dados de tráfego coletados pelo *MRTG®*. Esta funcionalidade do *OPNET® Modeler* só é possível com a utilização de um módulo de importação de tráfego chamado *MVI* (*Multi-Vendor Import*) [35], o qual possibilita a entrada exata do tráfego coletado, sem nenhum tipo de tratamento externo. O *OPNET® Modeler* permite também a importação de arquivos (*.TXT*) do *Microsoft® Excel*, o que facilita muito o manuseio dos dados para simulação.

5.4.1 – Proposta de um Estudo de Caso para Análise de Desempenho da Expansão de uma Rede Existente Utilizando Redes IEEE 802.11 (Etapa Três)

O objetivo desta simulação é possibilitar o entendimento de como se pode analisar as conseqüências da ampliação do alcance do *backbone* de uma rede tradicional utilizando redes sem fio. Para isto, torna-se fundamental o levantamento das estatísticas suficientes para compreensão do que está acontecendo e poderá acontecer com a rede. A Figura 5.7 ilustra o diagrama em blocos utilizado para a análise da expansão de redes empregando a simulação digital.

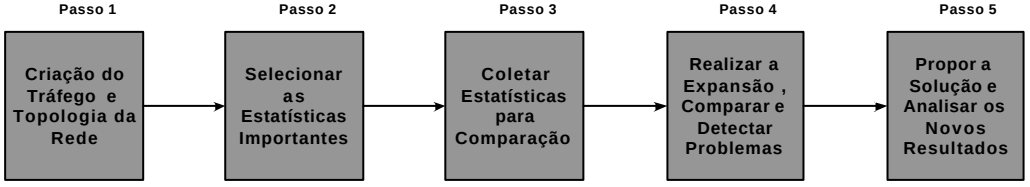


Figura 5.7 – *Diagrama em Blocos para Análise da Expansão de Redes Empregando Simulação*

5.4.1.1 – O Primeiro Passo

Inicialmente, deve-se ter em mãos os dados referentes ao tráfego gerado pelos usuários e a topologia da rede que se quer simular. Como não existe uma rede real, supõe-se que os clientes da rede estejam utilizando as aplicações *FTP* (*heavy*) e *HTTP* (*heavy*). A idéia da utilização do tráfego pesado é possibilitar a apresentação de estatísticas mais exageradas (fáceis) de serem analisadas visualmente.

A topologia inicial da rede é ilustrada nas figuras 5.8 e 5.9.

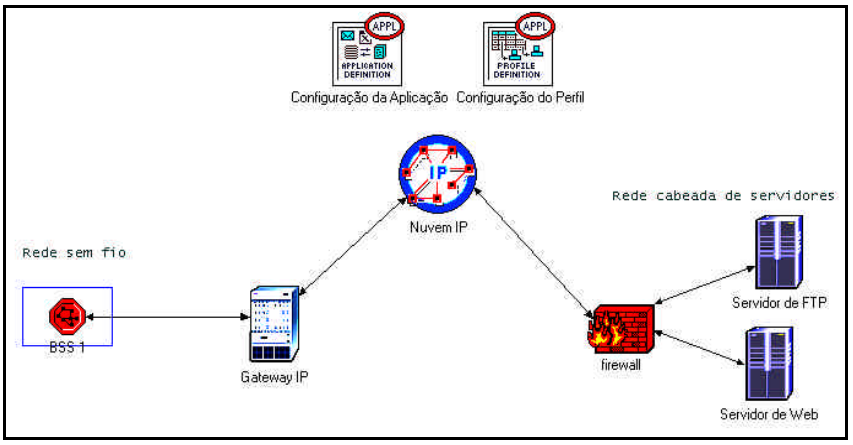


Figura 5.8 - *Topologia da Rede Inicial*

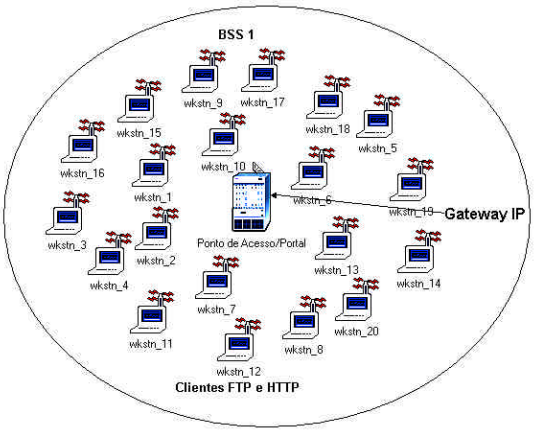


Figura 5.9 - *O Conjunto de Estações da Rede IEEE 802.11 – BSS 1*

Como se observa na Figura 5.8, a rede proposta é composta de uma parte cabeada, formada pelos servidores e pela *Nuvem IP* e por uma parte sem fio, formada pelo *BSS* 1 (20 *workstations*). O *Gateway IP* é responsável pelo roteamento dos pacotes baseado no endereço *IP* de destino. Já o *AP* (*Access Point*) está atuando como um portal para a rede cabeada. A função do *Firewall* (barreira de proteção) é rotear os pacotes *IP* endereçados a cada servidor de aplicação e bloquear o acesso

indesejado. A *Nuvem IP* é um nó responsável por emular o funcionamento da Internet. Neste caso em especial será considerado um atraso insignificante do pacote ao percorrer a Nuvem *IP*.

Os enlaces utilizados são os seguintes:

- *BSS* 1 ao *Gateway IP – 100BaseTduplex*
- *Gateway IP* à *Nuvem IP – PPP* (*Point-to-Point Protocol*) na taxa de 33 Kbps.
- *Nuvem IP* ao *Firewall – PPP DS1* (1,544 Mbps)
- *Firewall* aos servidores – *100BaseTduplex*

Vale ressaltar que no Brasil é empregada a padronização Européia (*E1* = 2,048 Mbps) e não a empregada na América do Norte e no Japão (*T1* = 1,544 Mbps), que é tecnicamente denominada *DS1* [5].

Uma observação importante é que o tráfego coletado, por exemplo pelo *MRTG*[â], poderia estar sendo utilizado para a representação do tráfego do enlace entre o *AP* e o *Gateway IP*, já que neste caso não será importante o tráfego gerado por cada estação da rede sem fio, mas sim, o que passa pelo *AP* e irá ocupar os enlaces até o destino (Grupo Facilidades de Comunicação).

5.4.1.2 – O Segundo Passo

Embora já tenha sido construído o modelo de simulação, ainda não é possível iniciar o processo. Antes disso, torna-se necessário verificar a possibilidade de coleta de diversas estatísticas sobre a rede e realizar uma escolha criteriosa dessas estatísticas de modo que a simulação seja eficiente, não ocupando muitos recursos computacionais. No caso desta simulação é importante conhecer o tempo de resposta da aplicação *FTP* e *HTTP*, a ocupação no enlace entre o *AP* e o *Gateway IP*, entre o *Gateway IP* e a *Nuvem IP*, entre a *Nuvem IP* e o *Firewall* e entre o *Firewall* e os servidores. Com estas análises, será possível a obtenção de uma base de dados gráficos que possibilite a verificação do impacto da adição de novas estações de trabalho e também determinar a melhor solução para possíveis problemas.

5.4.1.3 – O Terceiro Passo

Como foram definidas as estatísticas que interessam, agora deverá ser feita a verificação do desempenho da rede inicial.

Para determinar o impacto da expansão do número de computadores na rede é necessário comparar os desempenhos antes e após a expansão. Assim, torna-se

possível verificar os pontos críticos que podem estar gerando atrasos significativos. Através da Figura 5.10 percebe-se que o tempo médio de resposta *FTP* é de aproximadamente 28 segundos. O tempo médio de resposta *HTTP* mostrado na Figura 5.11 é de 8 segundos.

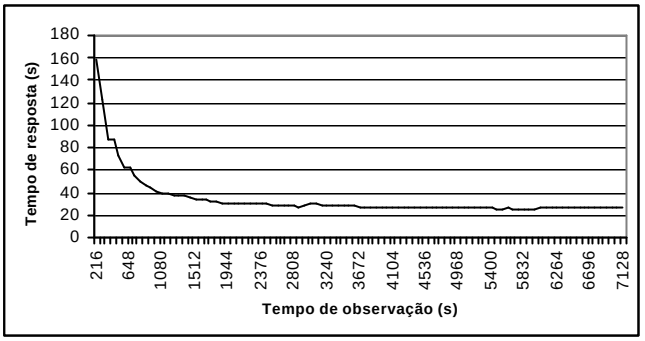


Figura 5.10 - *Tempo Médio de Resposta da Aplicação FTP*

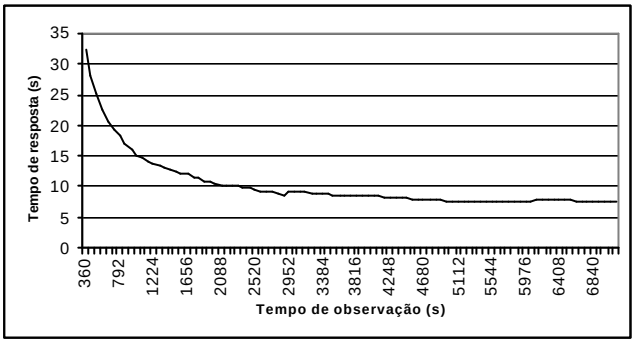


Figura 5.11 - *Tempo Médio de Resposta da Aplicação HTTP*

As figuras 5.12, 5.13, 5.14, 5.15 e 5.16 ilustram a utilização dos enlaces *BSS* 1<-->*Gateway IP*, *Gateway IP*<-->*Nuvem IP*, *Nuvem IP*<-->*Firewall*, *Firewall*<-->Servidor *FTP* e *Firewall*<-->Servidor *HTTP* respectivamente.

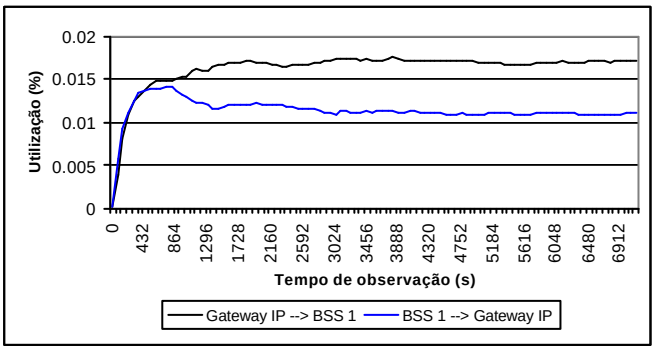


Figura 5.12 - *Utilização do Enlace BSS 1 <-->Gateway IP*

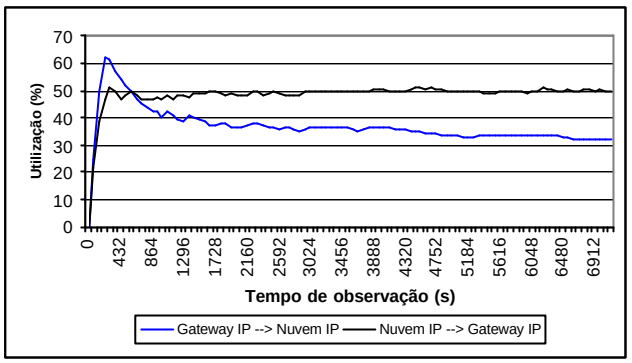


Figura 5.13 - *Utilização do Enlace Gateway IP<-->Nuvem IP*

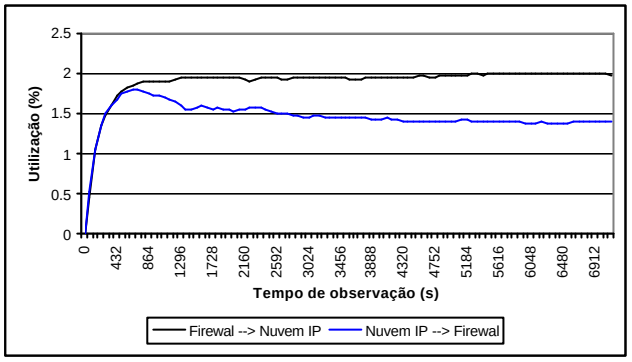


Figura 5.14 - *Utilização do Enlace Nuvem IP<-->Firewall*

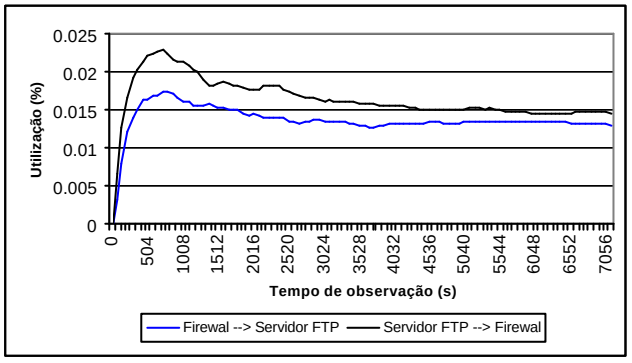


Figura 5.15 - *Utilização do Enlace Firewall<-->Servidor FTP*

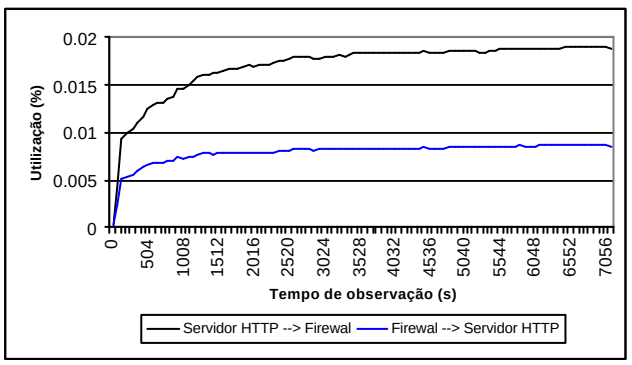


Figura 5.16 - *Utilização do Enlace Firewall<-->Servidor HTTP*

Observa-se nas figuras anteriores que o enlace que possui maior utilização é o *Gateway IP*<-->*Nuvem IP*, com uma ocupação média de 50 % no sentido do *Gateway IP* e de 32 % no sentido da *Nuvem IP*. Embora a ocupação do enlace nos dois sentidos seja bem diferente, não será preciso realizar a análise em ambos os sentidos. Isto é possível, pois a característica do tráfego gerado não muda, como poderá ser visto no Quarto Passo. Agora, de posse destes dados, definiu-se um padrão para determinar a influência no desempenho da rede expandida.

5.4.1.4 – O Quarto Passo

Neste passo é proposto o aumento do número de estações da rede sem fio através da inserção de um novo *BSS*. A Figura 5.17 ilustra a proposta para expansão da rede. Como se pode observar, foi adicionado mais um *BSS* ao *Gateway IP*. Esta necessidade pode ser imaginada como uma expansão da abrangência da rede cabeada devido à necessidade, por exemplo, de atingir salas de um prédio tombado como patrimônio histórico e que está abrigando um cartório de registros *on-line*. O *BSS* 2 é idêntico (aplicação e número de estações) ao *BSS* 1.

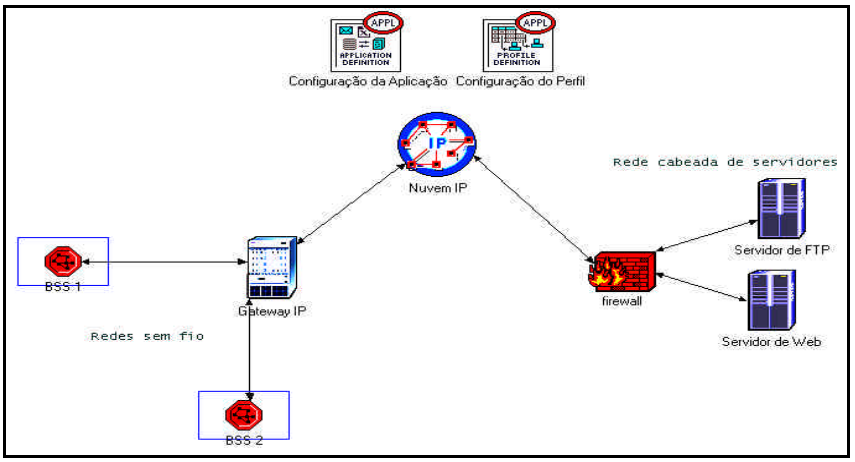


Figura 5.17 - *Rede Expandida*

Sabe-se que o *Gateway IP* suporta mais uma interface Ethernet, agora é necessário verificar a possibilidade da qualidade de serviço já existente não ser abalada. Para determinar o crescimento do tráfego gerado neste novo cenário, foram coletadas as mesmas estatísticas do tempo de resposta *FTP* e *HTTP* e da utilização do enlace *Gateway IP*<-->*Nuvem IP* apresentadas para rede inicial. A Figura 5.18 mostra o tempo de resposta *FTP* da rede inicial (*BSS* = 1) e da rede expandida (*BSS* = 2). Já a Figura 5.19 ilustra o tempo de resposta *HTTP*.

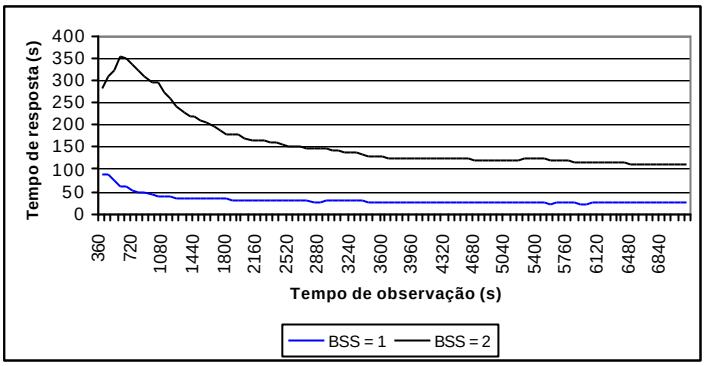


Figura 5.18 - *Tempo Médio de Resposta da Aplicação FTP para Rede Expandida*

Na Figura 5.18 observa-se que o tempo médio de resposta *FTP* é aumentado de 28 para cerca de 100 segundos.

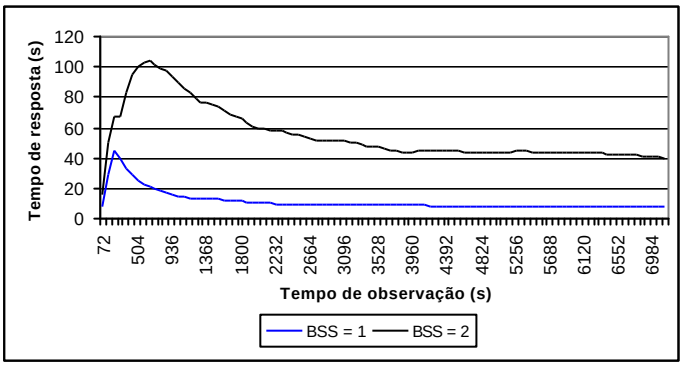


Figura 5.19 - *Tempo Médio de Resposta da Aplicação HTTP para Rede Expandida*

Na Figura 5.19 pode-se observar que o tempo médio de resposta *HTTP* é aumentado de 8 para cerca de 40 segundos.

Através das figuras 5.18 e 5.19 conclui-se que houve um aumento significativo do tempo de resposta das aplicações *FTP* e *HTTP*. Isso pode gerar reclamações por parte dos usuários devido ao tempo excessivo de espera na obtenção de arquivos e acesso às páginas da Internet.

A Figura 5.20 ilustra a utilização no sentido *Gateway IP-->BSS* 1 e *Gateway IP-->BSS* 2, já que este sentido representa o pior caso.

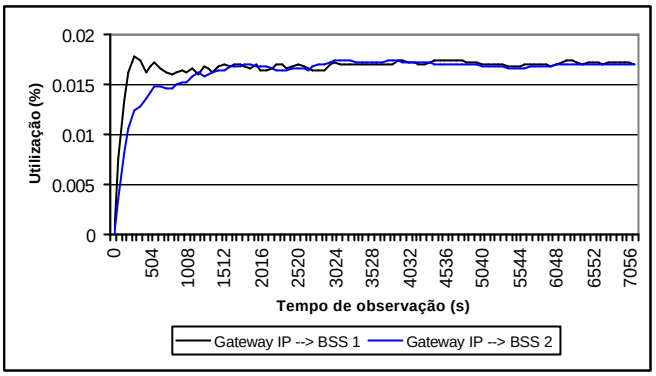


Figura 5.20 - *Comparação da Utilização do Enlace Gateway IP-->BSS*

As figuras 5.21 e 5.22 ilustram a utilização do enlace *Gateway IP<-->Nuvem IP* considerando a expansão da rede (*BSS* = 2) e a rede inicial (*BSS* = 1).

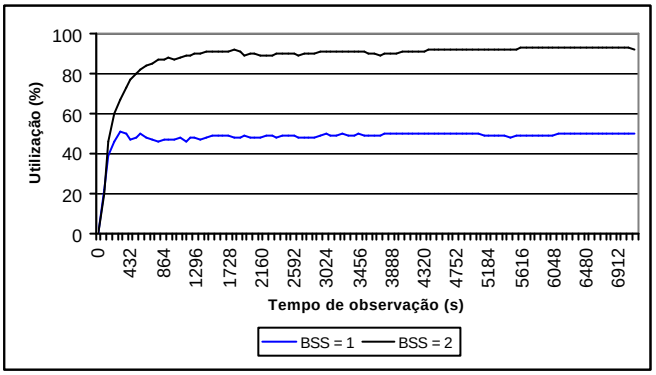


Figura 5.21 - *Comparação da Utilização do Enlace Nuvem IP-->Gateway IP*

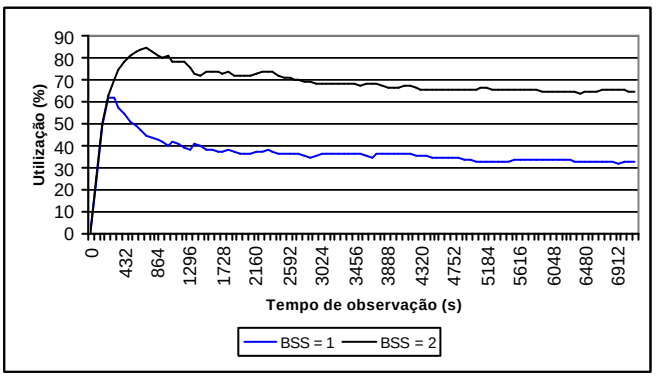


Figura 5.22 - *Comparação da Utilização do Enlace Gateway IP-->Nuvem IP*

Como conclusão das figuras 5.21 e 5.22, verifica-se que a utilização do enlace *Gateway IP<-->Nuvem IP* teve um aumento significativo, uma vez que existe um maior número de estações acessando a aplicação sustentada pelos servidores. Como a utilização no sentido *Nuvem IP-->Gateway IP* teve o aumento para próximo de 100%, a análise será focada neste sentido do enlace, já que no sentido

Gateway IP-->Nuvem IP a utilização ainda é admissível. Além disso, confirma-se que a adição de mais um *BSS* não alterou a característica do tráfego, ou seja, maior tráfego de *downlink* do que de *uplink*.

Pode-se observar nas figuras 5.23, 5.24 e 5.25 a utilização do enlace entre a *Nuvem IP* e o *Firewall*, entre o *Firewall* e o servidor de *FTP* e entre o *Firewall* e o servidor de *HTTP* para o tráfego de *downlink* nas redes expandida e inicial.

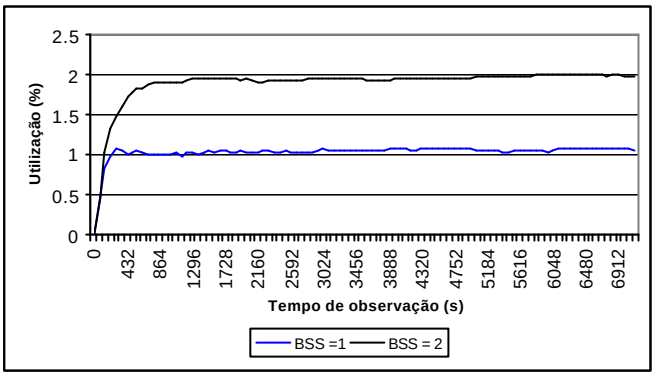


Figura 5.23 - *Comparação da Utilização do Enlace Firewall-->Nuvem IP*

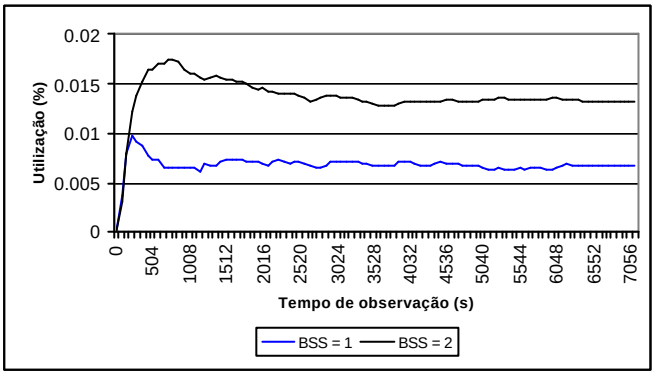


Figura 5.24 - *Comparação da Utilização do Enlace Servidor FTP-->Firewall*

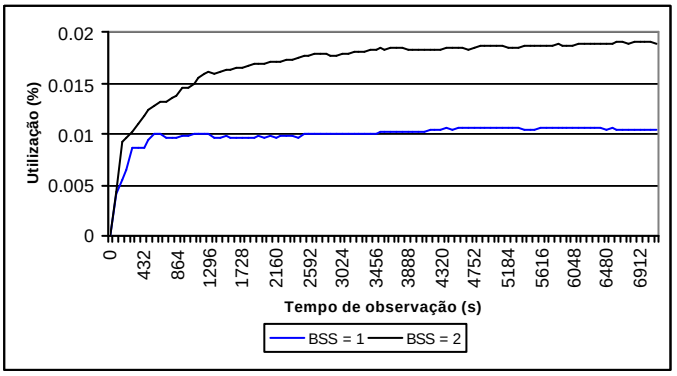


Figura 5.25 - *Comparação da Utilização do Enlace Servidor HTTP-->Firewall*

Como conclusão sobre os três enlaces anteriores, verifica-se que houve um aumento insignificante na utilização.

Analisando o indicador de desempenho Utilização para a rede inicial e para rede expandida fica claro que a capacidade do enlace entre o *Gateway IP* e a *Nuvem IP* não é adequada à nova situação, indicando a necessidade de melhoria desse enlace. Embora essa conclusão esteja clara a partir desta análise, nem sempre a mesma é óbvia quando não se têm os resultados da simulação e a situação simulada possui uma complexidade elevada. Em muitos casos, ao verificar que o enlace entre o *Gateway IP* e a *Nuvem IP* é de apenas 33 Kbps, a providência tomada é a de aumentar a sua capacidade. Isto pode solucionar o problema, mas é preciso analisar a relação entre o custo do novo enlace e os benefícios alcançados.

5.4.1.5 – O Quinto Passo

Agora, como solução para diminuir o tempo de resposta para a rede expandida, será aumentada a capacidade do enlace entre o *Gateway IP* e a *Nuvem IP*, verificando as melhorias no tempo de resposta *FTP* e *HTTP*. É claro que através do aumento da capacidade do enlace haverá uma diminuição de sua utilização, restando saber se o tempo de resposta alcançado é suficiente ou não.

Na Figura 5.26 mostra-se as cinco situações para o tempo de resposta *FTP* no enlace entre o *Gateway IP* e a *Nuvem IP*. Para uma melhor visualização, ilustra-se na Figura 5.27 somente os tempos de resposta para possíveis soluções, comparados à rede inicial.

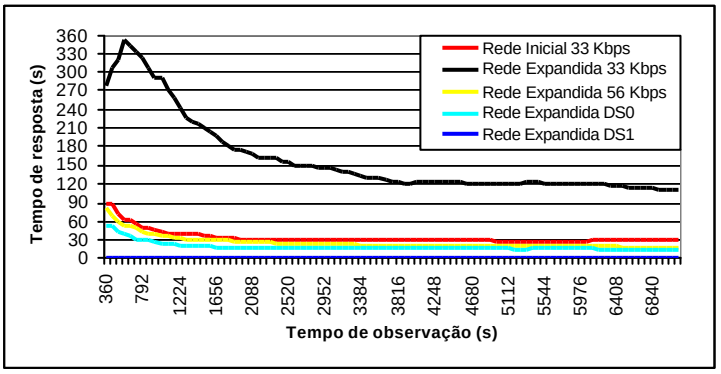


Figura 5.26 - *Tempo de Resposta para Aplicação FTP*

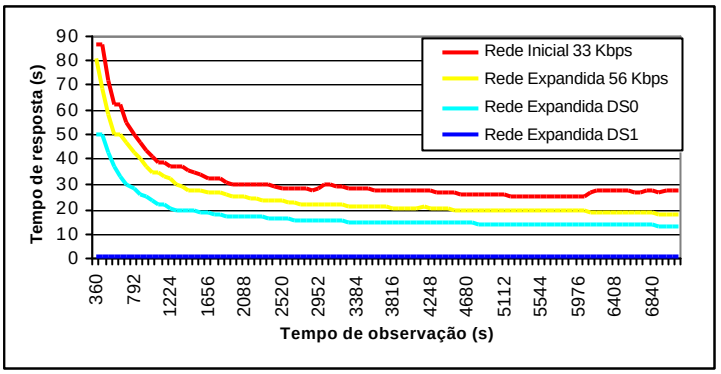


Figura 5.27 - *Melhores Tempos de Resposta para Aplicação FTP*

Na Figura 5.28 são apresentadas as cinco situações para o tempo de resposta *HTTP* no enlace entre o *Gateway IP* e a *Nuvem IP*. Observa-se na Figura 5.29 os melhores tempos de resposta para esta aplicação, comparados à rede inicial.

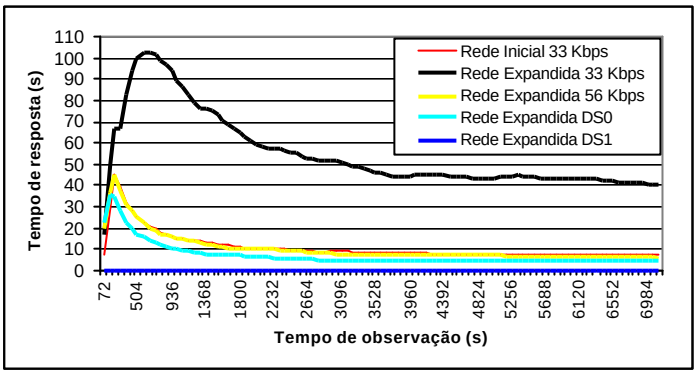


Figura 5.28 - *Tempo de Resposta para Aplicação HTTP*

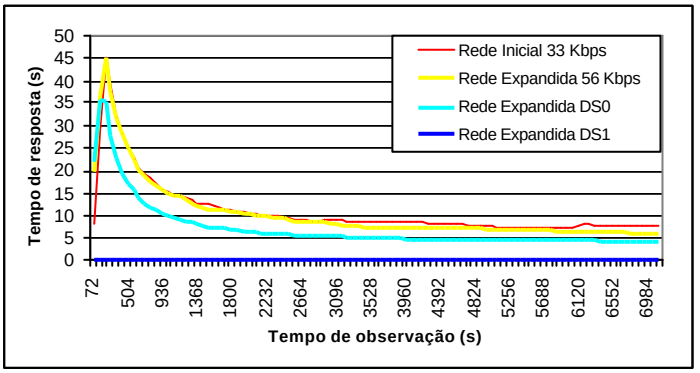


Figura 5.29 – *Melhores Tempos de Resposta para Aplicação HTTP*

Para o tempo de resposta da aplicação *FTP*, tem-se uma diminuição mais sensível do que para a aplicação *HTTP*. Isto é explicado pelo fato da utilização do enlace afetar a queda do tempo de resposta de forma exponencial. Verifica-se ainda nas figuras 5.27 e 5.29 que os tempos de resposta ficaram próximos do encontrado

para a rede inicial, exceto para a solução que utiliza o enlace *DS1*, na qual o tempo de resposta tendeu a 0 (zero). Desta forma, caso se deseje melhorar o desempenho da rede expandida com relação ao da rede inicial pode-se utilizar o enlace *DS1*. Esta solução, embora no momento seja super dimensionada, permitirá um novo aumento de tráfego com um tempo de resposta admissível.

Com a melhoria na capacidade do enlace, tem-se a garantia da diminuição da utilização do enlace entre o *Gateway IP* e a *Nuvem IP*, o qual representava um ponto de gargalo para a ampliação da rede. As figuras 5.30 e 5.31 ilustram essa melhoria nos dois sentidos do tráfego. Pode-se observar que esta utilização para o enlace *DS1* fica em torno de 0%.

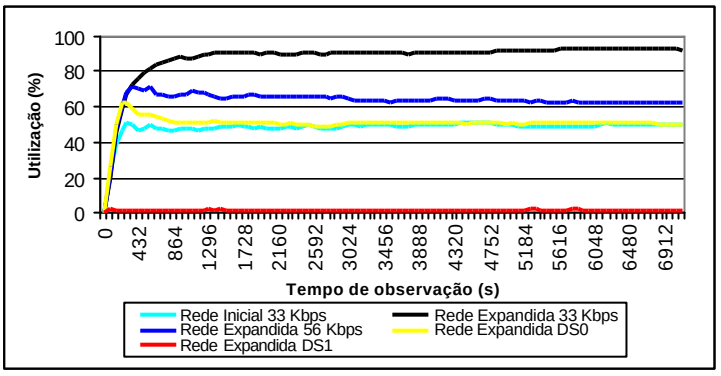


Figura 5.30 - *Utilização do Enlace Nuvem IP-->Gateway IP para Várias Situações da Rede*

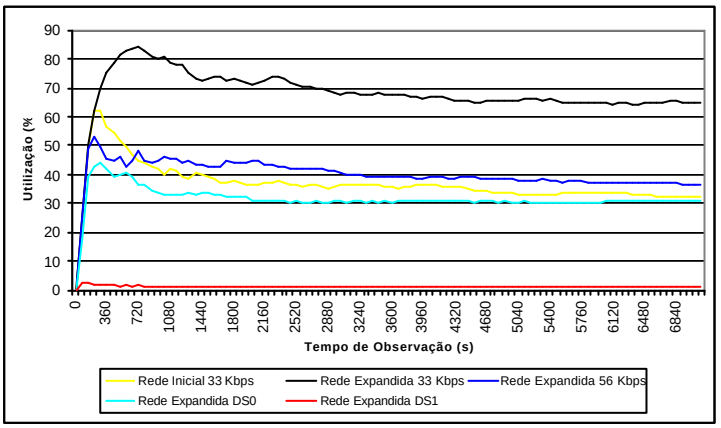


Figura 5.31 - *Utilização do Enlace Gateway IP-->Nuvem IP para Várias Situações da Rede*

Como conclusão, verifica-se que a análise de expansão de redes de computadores baseada nos resultados de simulações computacionais pode estimar o impacto do crescimento das redes sem fio na qualidade de serviço da rede como um todo. A realização de estimativas dos problemas que podem vir a acontecer com a

expansão e a busca de melhores soluções pode representar uma considerável economia nos recursos a serem investidos.

Uma outra conclusão importante que pode ser tirada sobre a análise do desempenho da rede empregando simulações é que, independentemente do meio de transmissão utilizado pela rede, o que interessa é o monitoramento do tráfego que passa pelos possíveis pontos de gargalo da rede.

É importante observar que o simulador *OPNET^â Modeler* traz facilidades muito maiores do que os softwares utilizados para a coleta de dados. Por exemplo, o tempo de resposta, que é facilmente obtido no simulador para cada aplicação, não pode ser obtido na rede real através dos objetos (variáveis) *SNMP*. Para a rede real, o problema deverá então ser identificado através da utilização dos enlaces para as situações da rede inicial e expandida. Sendo assim, o administrador da rede não terá como identificar o problema baseado no tempo de resposta da aplicação, a não ser que o usuário final faça uma reclamação, já que este tempo será perceptível. Como foi citado no Capítulo 3 desta dissertação, o tempo de resposta aumenta de forma exponencial com o aumento da utilização dos recursos da rede. Assim, os pontos de congestionamento podem fugir do controle do administrador da rede rapidamente. Desta forma, torna-se necessário que o administrador da rede tenha um bom conhecimento sobre a possibilidade do aumento no tempo de resposta causado pela ocupação do enlace, a fim de evitar reclamações e o congestionamento da rede.

Capítulo VI

6 – A Influência das Alterações dos Parâmetros da Camada *MAC* no Desempenho das Redes IEEE 802.11

De acordo com a metodologia proposta existe a possibilidade de gerenciar o desempenho de vários grupos. Entre estes grupos, o "Clientes" representa, por exemplo, as estações sem fio. Como não foi possível a coleta dos dados em uma rede real, resolveu-se através das características apresentadas sobre as redes IEEE 802.11, simular vários parâmetros que podem influenciar no desempenho das redes sem fio.

6.1 - Simulações com Duas Estações

Como neste momento o interesse está voltado somente à análise dos parâmetros básicos característicos do padrão IEEE 802.11, montou-se um cenário simples com duas estações gerando o mesmo tráfego estatístico. Ressalta-se que, embora na prática o tráfego seja gerado de forma bastante aleatória, utilizar-se-á nas simulações a seguir a mesma "semente" para os diferentes cenários simulados, tornando possível a comparação dos resultados obtidos. A Figura 6.1 ilustra as duas estações em uma comunicação direta.

Figura 6.1 – *Duas Estações no Modo DCF Opcional*

Na Figura 6.2 são apresentados os parâmetros que foram configurados no *OPNET® Modeler*. Observa-se que o tráfego gerado foi o padrão (*default*) do simulador, não correspondendo a nenhum tráfego específico (*HTTP*, *FTP*, *E-mail*), já que o interesse está voltado para a avaliação de aspectos relacionados à camada *MAC*. O tamanho do pacote gerado segue uma distribuição exponencial com média de 1024 bytes. Mais informações sobre os parâmetros configurados, assim como as estatísticas coletadas podem ser encontradas no Anexo B.

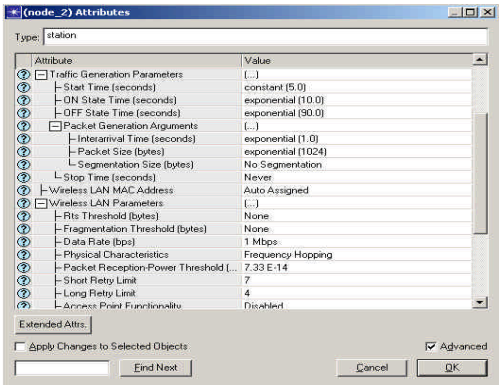


Figura 6.2 – *Configuração dos Parâmetros*

Para minimizar e evitar repetições dos valores de cada parâmetro dos cenários simulados, de agora em diante, só serão apresentados os valores dos parâmetros que forem alterados do padrão já configurado pelo *OPNET*$^{\hat{a}}$ *Modeler*.

6.1.1 - A Influência do Parâmetro *RTSthreshold*

O parâmetro *RTSthreshold* é o valor do limiar que indica se haverá a reserva do meio (canal de comunicação) para a transmissão ou não. Este parâmetro faz parte do modo de operação *DCF* opcional, onde as estações se comunicam diretamente sem o auxílio do *AP*.

Como resultado desta simulação coletou-se as informações sobre a influência do *RTSthreshold* no tempo utilizado para a reserva do canal para taxas de transmissão de 2 Mbps e 11 Mbps.

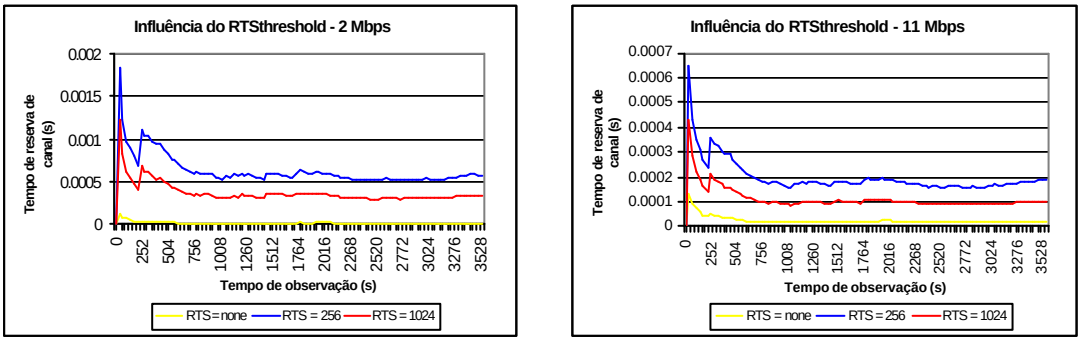


Figura 6.3 – *A Influência do Limiar de RTS no Tempo de Reserva de Canal*

Com base na Figura 6.3, conclui-se que para o valor do *RTSthreshold* mais próximo do tamanho médio do pacote transmitido (1024 bytes), consegue-se um tempo gasto com quadros utilizados para a reserva de canal menor. Isto ocorre devido a reserva de canal ser feita somente quando se deseja transmitir pacotes maiores do que o limiar de *RTS*. Assim, com o limiar menor mais pacotes

transmitidos utilizarão quadros *RTS* e *CTS* para alocação de banda, gastando mais tempo com a reserva de canal ao longo do período de observação. Ainda na Figura 6.3, os dois gráficos para as taxas de transmissão de 2 e 11 Mbps podem ser comparados entre si. Com isto, verifica-se que para a taxa de transmissão menor existe um tempo de alocação do canal maior. Isto se deve principalmente ao fato de que os pacotes transmitidos com maior velocidade, ocupam o canal por um tempo menor. Vale ressaltar que nesta simulação foi utilizado um tráfego gerado na rede relativamente pequeno. Para um tráfego maior, provavelmente serão apresentados valores mais distantes para os diferentes limiares de *RTS*, já que a reserva do meio pode não ser alcançada sempre. Embora o limiar de *RTS* igual a *none* indique que não haverá a reserva do meio para qualquer tamanho de pacote a ser transmitido, o padrão IEEE 802.11 determina que todas as estações devam ser capazes de receber o quadro *RTS* para atualizar o seu vetor de alocação da rede (*NAV*).

6.1.2 - A Influência do Parâmetro *FRAGMENTATIONthreshold*

De acordo com a Figura 6.4 é possível verificar que quando ocorre a fragmentação existe um tempo gasto com a reserva de canal sempre maior. Isto é explicado facilmente, já que o limiar de *RTS* considerado foi de 256 bytes e os pacotes são gerados com tamanho médio de 1024 bytes. Com isto, a maioria dos pacotes será fragmentada para um valor maior do que o limiar de *RTS*, originando um tempo gasto com alocação do meio de transmissão maior. Vale ressaltar que o limiar de fragmentação também determina o tamanho máximo dos fragmentos e dependendo do tamanho dos pacotes recebidos das camadas mais altas, poderá ocorrer a divisão em mais do que dois fragmentos.

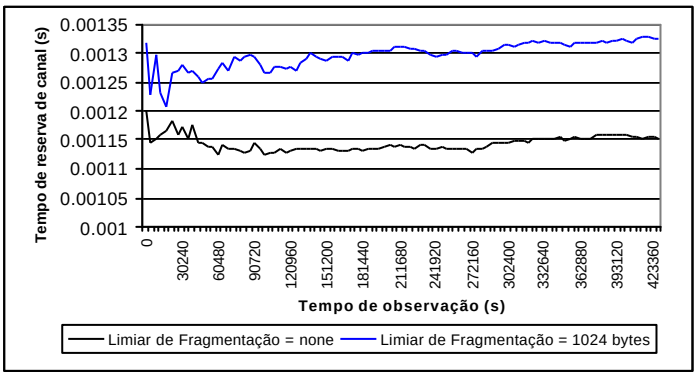


Figura 6.4 – *A Influência da Fragmentação no Tempo de Reserva de Canal*

Assim como o limiar de *RTS* influencia diretamente no tráfego de controle gerado na rede, podendo alterar o *throughput*, o limiar de fragmentação também pode afetá-lo. Isto se deve ao fato de que para cada pacote fragmentado, haverá um quadro de reconhecimento (*ACK*) por parte da estação de destino, aumentando o tráfego de controle. Como a influência no tráfego de controle é intuitiva, na Figura 6.5 é ilustrada a influência no *throughput*.

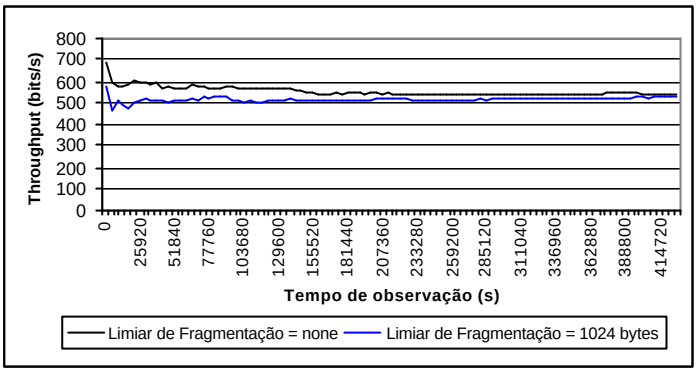


Figura 6.5 – *A Influência da Fragmentação no Throughput*

6.1.3 - A Influência da Taxa de Transmissão no Tempo de Acesso ao Meio

Na Figura 6.6 é possível mostrar que o atraso de acesso ao meio varia com a taxa de transmissão utilizada. Como já citado, isto acontece devido ao fato que o pacote, ao chegar da camada de enlace para ser transmitido, espera um tempo menor para a taxa de transmissão maior, considerando a mesma carga para as duas situações.

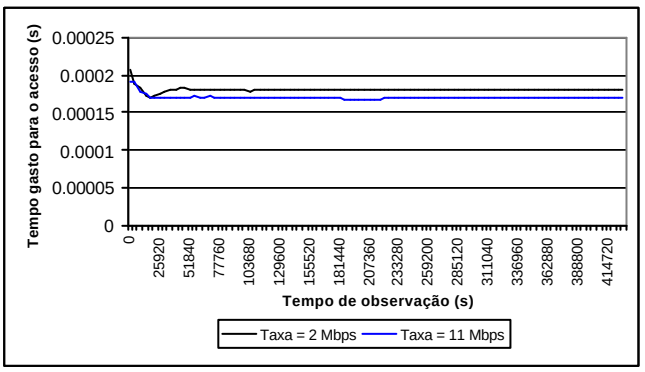


Figura 6.6 – *A Influência da Taxa de Transmissão no Tempo de Acesso ao Meio*

6.1.4 - Fatores que Influenciam no *Throughput*

Além da influência do limiar de fragmentação no *throughput*, já descrita, o limiar de *RTS* também pode influenciar neste indicador de desempenho. Na

Figura 6.7 verifica-se com a utilização de um limiar de *RTS* menor que haverá mais bits de controle (quadros *ACK*, *RTS* e *CTS*) sendo recebidos. Uma conclusão imediata seria a queda do *throughput*, no entanto, na Figura 6.8 observa-se que o *throughput* permanece o mesmo.

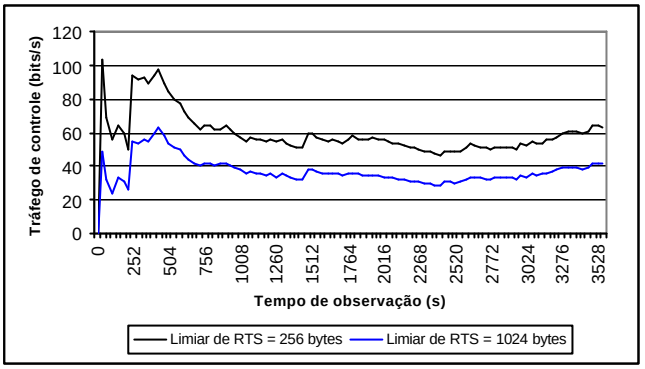


Figura 6.7 – *A Influência do Limiar de RTS no Tráfego de Controle*

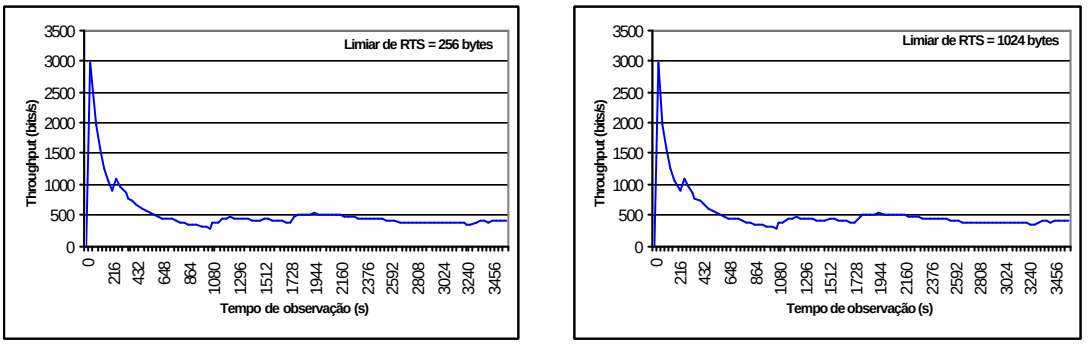


Figura 6.8 – *A Influência do Limiar de RTS no Throughput*

Este fato é explicado principalmente por estar sendo considerada a disputa pelo meio por apenas duas estações, que geram o mesmo tráfego. Pode-se concluir então que, apesar do limiar de *RTS* influenciar diretamente no tráfego de controle gerado na rede, dependendo da disputa pelo meio, não haverá influência no *throughput*. O fator que indica a igualdade do *throughput* é a perda de pacotes que permanece a mesma para as duas situações simuladas, como se observa na Figura 6.9.

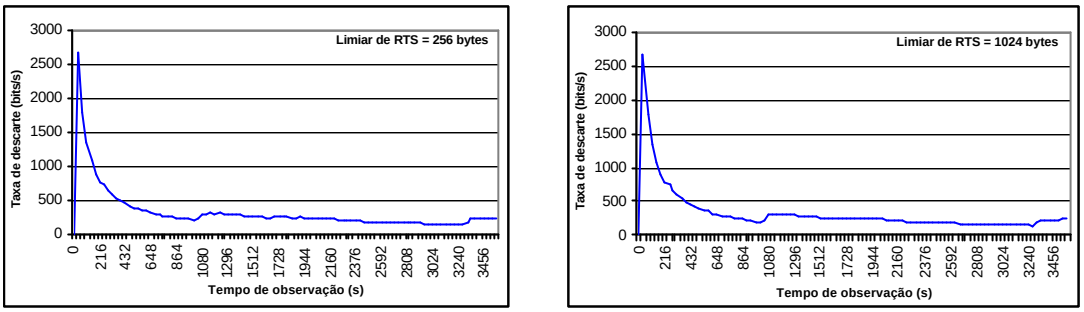


Figura 6.9 – *A Influência do Limiar de RTS na Taxa de Descarte*

6.1.5 - A Influência da Taxa de Transmissão na Perda de Pacotes

Na Figura 6.10 é possível observar que a perda de pacotes é menor quando se utiliza uma taxa de transmissão maior.

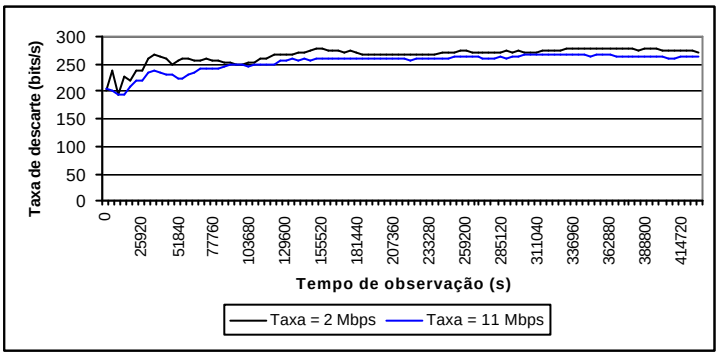


Figura 6.10 – *A Influência da Taxa de Transmissão no Descarte de Pacotes*

Deve ficar claro que só a taxa de transmissão maior não garante que uma estação terá um descarte menor de pacotes (bits/s), já que a perda de pacotes irá ocorrer quando o *buffer* estiver lotado. Sendo assim, a carga gerada na rede pelos demais usuários será o fator de grande influência na ocupação do *buffer*, ou seja, a taxa de transmissão maior poderá implicar na ocorrência da taxa de descarte também maior.

6.1.6 - Os Fatores que Influenciam na Tentativa de Retransmissão de Pacotes

Até então, nenhuma simulação apresentou os fatores que poderiam influenciar na retransmissão de pacotes. De acordo com o padrão IEEE 802.11, a retransmissão irá ocorrer quando houver uma falha do reconhecimento (*ACK*) por parte da estação de destino. Esta falha pode ocorrer devido a fatores como colisões, interferências no meio físico ou mesmo diferenças nos modos de operação das estações. Através das simulações feitas no *OPNET® Modeler* não existe a possibilidade da criação de interferências no meio físico, assim, só resta verificar as

retransmissões devido a colisões e também ao modo de operação da rede, o qual será apresentado na seção 6.2.2.

Na Figura 6.11 são ilustradas várias situações, onde são observadas as tentativas de retransmissão de pacotes. Para que fosse possível esta observação, o tráfego gerado pelas duas estações foi aumentado, criando, deste modo, um aumento do número de colisões. Isto favoreceu a visualização das tentativas de retransmissão, já que para as situações simuladas anteriormente este valor foi sempre 0 (zero). A característica do tráfego gerado continua seguindo uma distribuição exponencial, mas agora, com média 100 para o tempo de geração de pacotes, média 1 para o tempo onde não são gerados pacotes e média 0,01 para o tempo entre a geração de pacotes. Além disso, todos os cenários tiveram suas estações configuradas para a taxa de transmissão de 11 Mbps, com exceção de um, onde suas estações utilizam 2 Mbps.

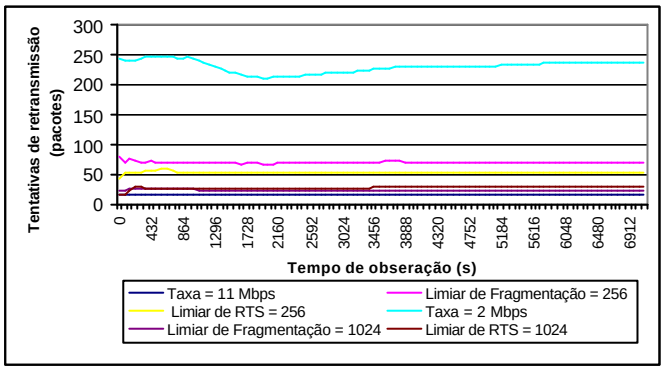


Figura 6.11 – *A Influência de Diversos Parâmetros na Tentativa de Retransmissão*

De posse dos resultados apresentados na Figura 6.11, conclui-se que os valores dos parâmetros configurados: taxa de transmissão, limiares de *RTS* e de fragmentação irão influenciar no número de tentativas de retransmissão de pacotes nas diversas situações simuladas. Além disso, a taxa de transmissão terá maior influência nas tentativas de retransmissão do que os limiares de *RTS* e de fragmentação. A explicação para este fato é que as estações com uma taxa de transmissão maior tratam o problema com as colisões de uma maneira mais rápida, ou seja, o processo de *backoff* [2] se torna mais rápido, já que as estações ocupam o meio de transmissão por um tempo menor. Com isto, torna-se interessante uma análise do *throughput* em cada uma destas situações. A Figura 6.12 apresenta o resultado obtido para o *throughput* nas diversas situações simuladas.

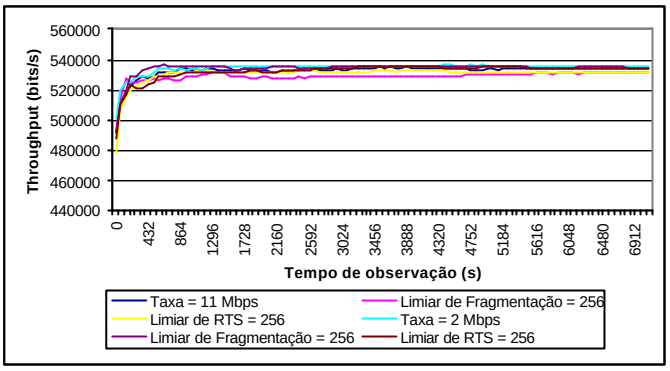


Figura 6.12 – *A Influência de Diversos Parâmetros no Throughput*

Como se observa na Figura 6.12, o valor para o *throughput* nas diversas situações é bastante próximo, embora o número de retransmissões seja bem diferente para cada uma das situações. Outros resultados como o tráfego de controle e o tempo de acesso ao meio com valores diferentes e a perda de pacotes com valores próximos para as várias situações simuladas, podem ser extraídos de forma indireta dos dois gráficos anteriores. Por serem resultados intuitivos, não foram apresentados no texto. Cabe observar que esta é uma situação particular e não se pode afirmar que independente do número de tentativas de retransmissão haverá o mesmo *throughput*, já que se houver, por exemplo, mais do que sete tentativas para a transmissão de um pacote, este será descartado.

6.2 - Simulações com Quatro Estações

Agora serão adicionados ao mesmo *IBSS* (*BSS* independente) mais duas estações com o mesmo perfil dos usuários das estações já existentes. A Figura 6.13 ilustra esta possibilidade.

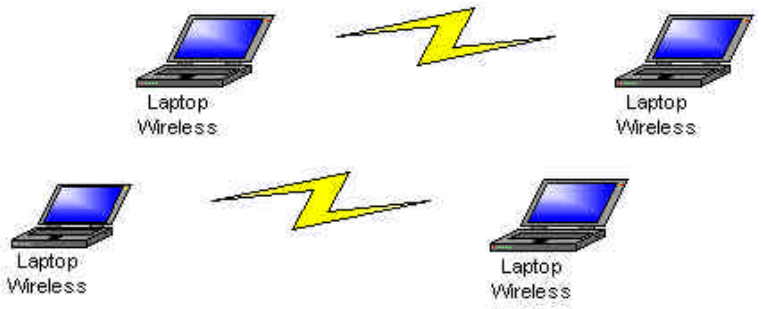


Figura 6.13 – *Quatro Estações Operando no Modo DCF*

6.2.1 - A Influência do Parâmetro *RTSthreshold*

A Figura 6.14 vem ilustrar melhor o que foi mencionado sobre a influência do limiar de *RTS* no *throughput*, já que com duas estações isto não ocorre. Verifica-se

que o *throughput* é bem menor para o menor valor do limiar de *RTS*. Isto é explicado pela reserva freqüente do canal de transmissão, a qual gera um grande tráfego de controle (*ACK*, *RTS* e *CTS*) comparado ao tráfego de dados. Vale lembrar que os pacotes transmitidos têm um tamanho médio de 1024 bytes. Para os maiores limiares de *RTS*, o valor do *throughput* será praticamente igual, indicando que a maioria dos pacotes gerados estão com o tamanho acima de 512 bytes.

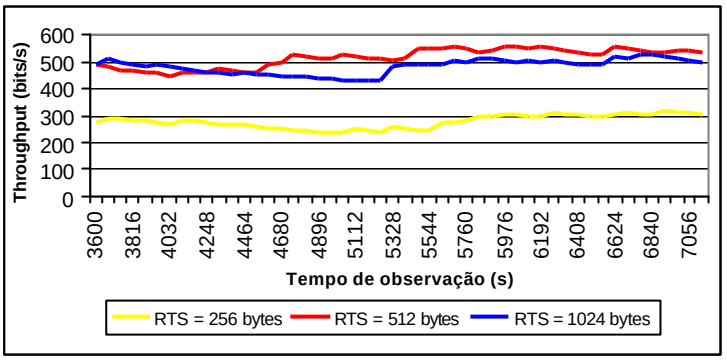


Figura 6.14 - *A Influência do Limiar de RTS no Throughput*

Resumidamente, o que ocorre são muito mais bits de dados sendo trocados num mesmo tempo do que bits de controle para maiores limiares de *RTS*. Isto é confirmado pela Figura 6.15, que mostra uma taxa de tráfego de controle recebido menor para limiares maiores de *RTS*.

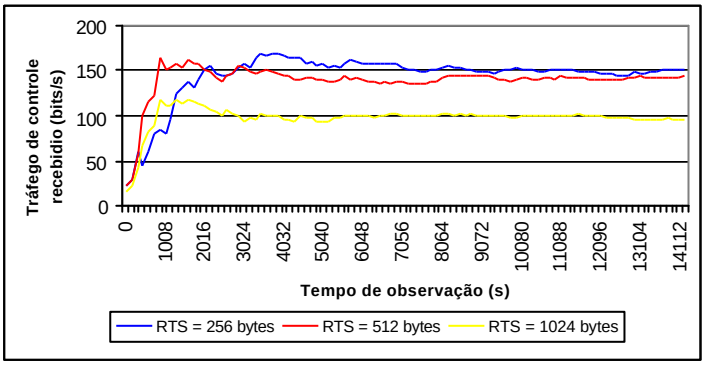


Figura 6.15 - *A Influência do Limiar de RTS no Tráfego de Controle*

Um fato importante que ocorre nos resultados desta simulação é a possibilidade da troca entre os valores apresentados tanto para o *throughput*, como para o tráfego de controle recebido para os diferentes limiares de *RTS*. Isto significa que não se pode tomar como resultado os valores encontrados para uma estação, já que existe uma aleatoriedade maior no acesso ao meio devido a disputa pelo mesmo estar ocorrendo entre quatro estações.

Vale ressaltar que a alocação do meio de transmissão para pacotes com tamanho bem maior do que o limiar de *RTS* é válido, pois dá maior confiabilidade à transmissão e gera um tráfego de controle na rede desprezível.

6.2.2 – A Influência dos Modos de Operação no *Throughput*

Para avaliar a influência dos modos de operação *DCF* e *PCF* no *throughput*, foi criado o cenário da Figura 6.16.

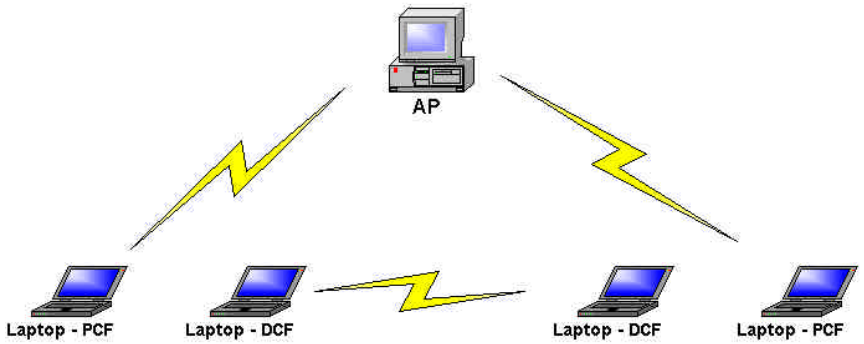


Figura 6.16 – *Estações Operando nos Modos DCF e PCF*

Como foi apresentado no Capítulo 2, as estações que desejam se comunicar no modo *PCF* devem se registrar junto ao Ponto de Acesso (*AP*) de forma a ganharem permissão para sua transmissão. Já as estações operando no modo *DCF* não necessitam da intervenção do *AP* para transmitirem os seus pacotes.

Nesta situação, a característica do tráfego gerado continua seguindo uma distribuição exponencial, entretanto, com média 0,1 para o tempo entre a geração de pacotes. Além da alteração neste parâmetro, foi atribuído ao limiar de fragmentação 1024 bytes e à taxa de transmissão 11 Mbps. Com estes parâmetros configurados foi simulado o cenário anterior, no entanto, as estações apresentaram o mesmo *throughput*, taxa de descarte e tentativas de retransmissão. Sendo assim, tornou-se interessante explorar o parâmetro *CFPmaxduration*, definido no Capítulo 2 para as estações operando no modo *PCF*. Este parâmetro corresponde ao tempo máximo de duração do período livre de contenção e pode ser alterado através dos parâmetros *CFP Interval* (s) e *Beacon Interval* (s) do *OPNET*$^{\hat{a}}$ *Modeler*, por exemplo, ambos para 0,1.

Na Figura 6.17 é possível verificar que o *throughput* para estações que operam no modo *PCF* é maior do que para aquelas que operam no modo *DCF*. Este fato é explicado devido à possibilidade da estação que opera no modo *PCF* poder

transmitir seus pacotes tanto no período livre de contenção (*CFP*), como no período com contenção (*CP*).

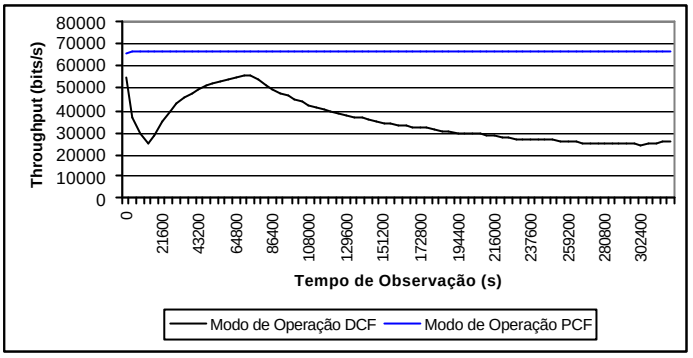


Figura 6.17 – *A Influência do Modo de Operação no Throughput*

Na Figura 6.18 verifica-se que o *throughput* maior alcançado pela estação operando no modo *PCF* justifica-se pela menor perda de pacotes ocorrida. Outro fato de destaque nesta figura é a alta taxa de descarte. Isto ocorre pelo fato do tráfego gerado ser bem elevado e o *buffer* não conseguir armazená-lo.

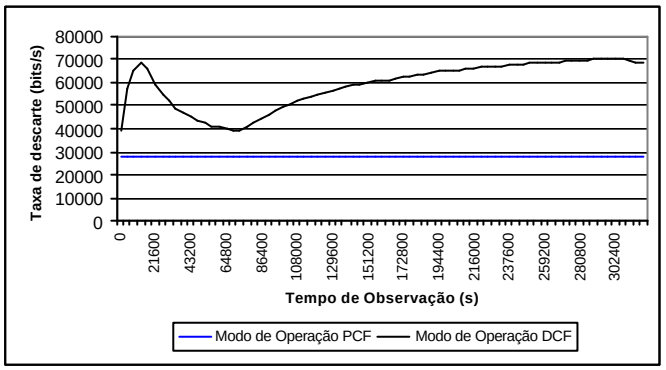


Figura 6.18 – *A Influência do Modo de Operação no Descarte de Pacotes*

Ainda, verifica-se na Figura 6.19 que a estação operando no modo *DCF* possui um número de tentativas de retransmissão maior. A explicação é que neste caso a retransmissão só ocorrerá no modo *DCF*, já que não existe interferências no meio físico. Desta forma, a estação operando no modo *PCF* irá sofrer menos com colisões, originando assim um número menor de tentativas de retransmissão.

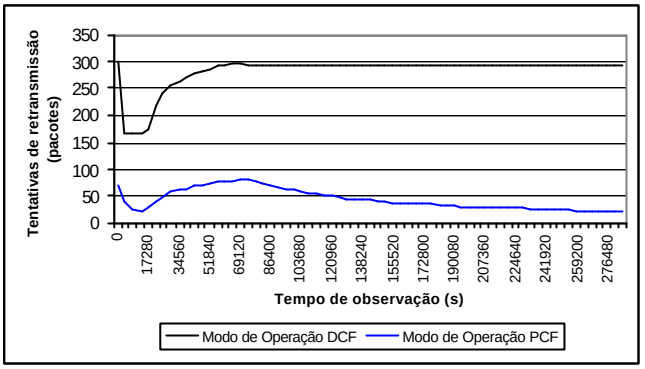


Figura 6.19 – *A Influência do Modo de Operação na Retransmissão*

É importante salientar que o desempenho para o modo de operação *DCF* é superior ao modo de operação *PCF* para a transmissão de pacotes pequenos e sujeitos a baixos valores da taxa de erro de bits. Por outro lado, se há o aumento do tamanho dos pacotes, o desempenho do modo *PCF* fica superior [47].

Parâmetros como o tempo *PIFS*, *SIFS* e *DIFS*, e o tamanho mínimo e máximo da janela de contenção não são possíveis de serem ajustados através do *OPNET*$^{\hat{a}}$ *Modeler*, já que seguem valores fixos estabelecidos pelo padrão IEEE 802.11.

6.3 - A Influência das Alterações dos Parâmetros da Camada *MAC* com o Aumento da Carga na Rede

Nesta simulação, propõe-se vários cenários onde o número de estações que buscam o acesso ao meio é aumentado na intenção de gerar uma carga maior na rede. O tráfego gerado por cada estação segue uma distribuição exponencial com média 1 para o tempo onde são gerados os pacotes, média 0 para o tempo onde não são gerados pacotes e 0,164 para o tempo entre a geração de pacotes. Além disso, todas as estações possuem o seu endereço de destino aleatório, ou seja, todas as estações possuem a mesma probabilidade de trocar pacotes entre si.

A Figura 6.20 ilustra o *throughput* agregado para vários limiares de *RTS* em função do número de estações. Essa medida estatística corresponde ao número médio de bits de dados recebidos corretamente por todas as estações durante o tempo de uma hora de observação da rede. Nas simulações anteriores os valores apresentados se distanciaram pouco entre si e a intenção era mostrar que a alteração de parâmetros como o limiar de *RTS* e de fragmentação afetavam os indicadores de desempenho da rede como o *throughput* de forma diferente. No entanto, os resultados das simulações apresentados a seguir não visam a interpretação desses valores para cada número de

estações disputando o meio, mas sim a influência que o aumento da carga na rede juntamente com os limiares de *RTS* e de fragmentação causam no *throughput* agregado da rede.

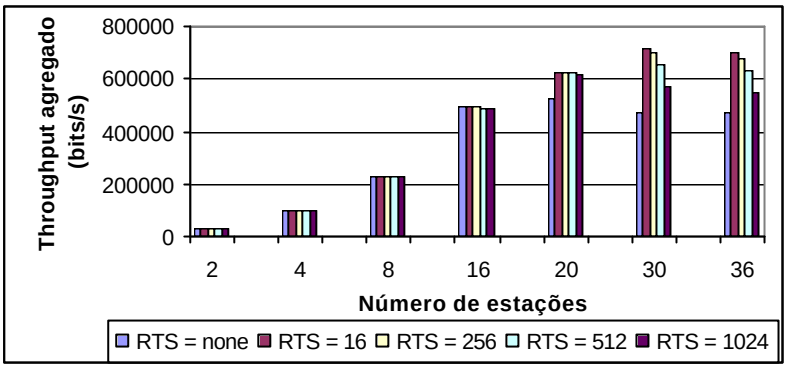


Figura 6.20 – *A Influência da Carga na Rede e do Limiar de RTS no Throughput Agregado*

Com base na Figura 6.20 observa-se que o *throughput* agregado aumenta com o número de estações gerando tráfego, no entanto, ao atingir o número de 30 estações disputando o meio, o *throughput* para a situação onde não está sendo utilizado quadros de controle para a reserva do meio começa a cair. Esse fato é explicado devido ao aumento da taxa de descarte de pacotes, já que as estações terão que esperar cada vez mais para acessar o meio com o aumento da carga na rede. Além disso, com a utilização da alocação do meio para a transmissão, consegue-se um aumento no *throughput* agregado mesmo com 30 estações disputando esse meio. Desta forma, conclui-se que a rede onde suas estações estão utilizando quadros para a reserva do meio estará suportando um tráfego maior antes de entrar em situação de saturação, ou seja, apresentar uma queda no *throughput* agregado. Uma situação similar ocorre para o limiar de *RTS* igual a 1024 bytes, onde poucos pacotes estarão utilizando a reserva do meio, fazendo com que o *throughput* agregado caia ao atingir o número de 30 estações.

Observa-se ainda na Figura 6.20 que o *throughput* agregado possui praticamente o mesmo valor para os vários limiares de *RTS* com 2, 4, 8 e 16 estações, assim, conclui-se que a utilização de quadros de controle apresentarão maior eficiência em redes sob carga maior. Isto mostra a vantagem de se empregar quadros de controle com a carga elevada na rede, além da transmissão de mensagens com tamanho bem maior do que os quadros *RTS* e *CTS* já mencionada. Para a situação com a maior carga na rede (36 estações), o limiar de *RTS* igual a 16 bytes apresentou

o maior *throughput* agregado, já que nesta situação todos os pacotes irão utilizar quadros de controle para a reserva do meio enquanto transmitem. A Figura 6.21 ilustra a taxa de descarte para os diversos limiares de *RTS* com o aumento da carga na rede.

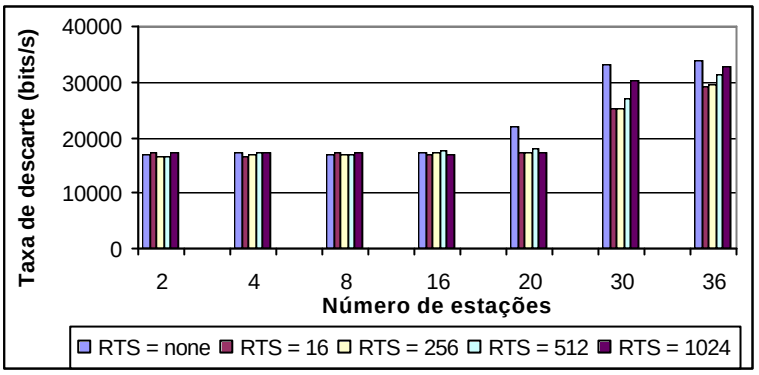


Figura 6.21 - *A Influência da Carga na Rede e do Limiar de RTS na Taxa de Descarte*

Na Figura 6.21 verifica-se com o aumento do número de estações na rede que a taxa de descarte permanece praticamente a mesma para até 16 estações. Observa-se ainda que acima de 16 estações esse valor começa a aumentar principalmente para a situação onde não se está empregando a reserva de canal. A explicação para esse fato é apresentada na Figura 6.22, onde se observa o aumento do número de tentativas de retransmissão com o aumento do número de estações para a situação onde está sendo utilizado quadros de controle para alocação do meio.

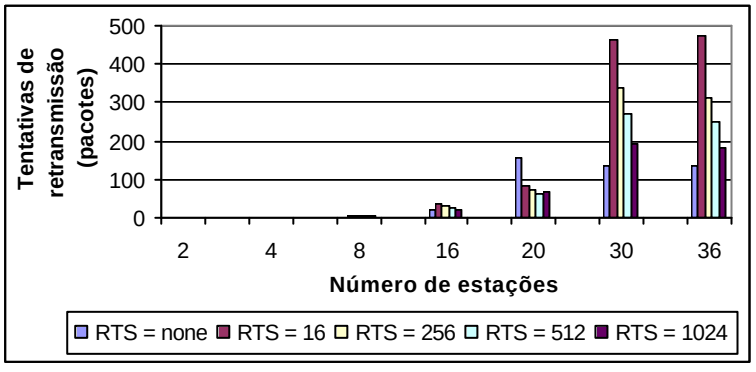


Figura 6.22 - *A Influência da Carga na Rede e do Limiar de RTS nas Tentativas de Retransmissão*

Ainda com relação às figuras 6.21 e 6.22 é interessante observar que quando a perda de pacotes é maior, as tentativas de retransmissão diminuem. Isto ocorre devido ao fato das estações estarem descartando os seus pacotes não por alcançarem sete tentativas de retransmissão, mas sim pela ocupação do *buffer*.

Outro fato que justifica a queda do *throughput* agregado é o aumento do tempo gasto para o acesso ao meio com o maior número de estações disputando o mesmo canal de comunicação, como mostra a Figura 6.23. Nesta figura o tempo gasto para o acesso ao meio para até 20 estações apresenta-se como 0 (zero), embora o seu valor real tenha sido aumentado até ficar em torno de 0,025 segundos.

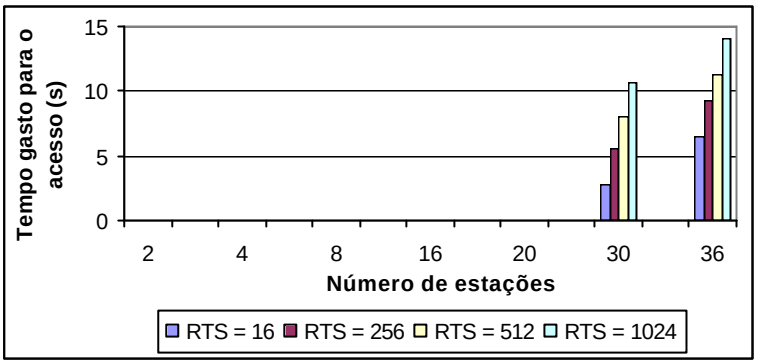


Figura 6.23 – *A Influência da Carga na Rede e do Limiar de RTS no Tempo de Acesso ao Meio*

Além do limiar de *RTS* influenciar no *throughput* agregado de forma diferente com o aumento da carga na rede, o limiar de fragmentação também irá influenciar. A Figura 6.24 ilustra o *throughput* agregado para os vários limiares de *RTS* e de fragmentação com o aumento da carga na rede.

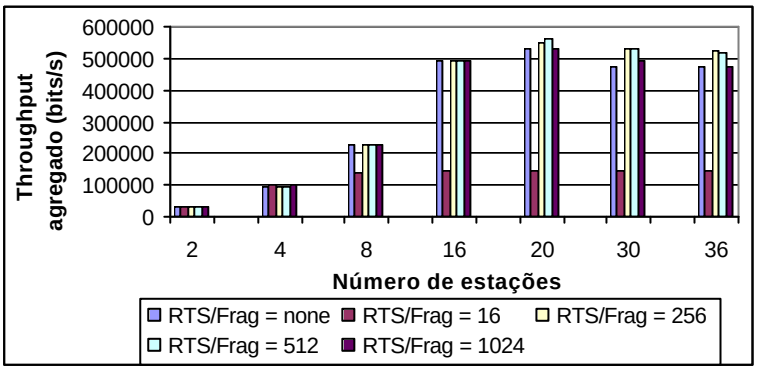


Figura 6.24 - *A Influência da Carga na Rede e do Limiar de RTS e de Fragmentação no Throughput Agregado*

Verifica-se na Figura 6.24 a mesma situação da Figura 6.20, onde o *throughput* agregado cresce com o aumento da carga na rede até um determinado número de estações gerando tráfego e depois tende a cair. Um fato interessante acontece com o *throughput* agregado para o limiar de *RTS* e de fragmentação igual a 16 bytes, que permanece praticamente o mesmo para mais do que 4 estações. Isto ocorre porque todos os pacotes utilizarão quadros de controle e fragmentação ao

serem transmitidos, ocasionando a saturação da rede com apenas 8 estações. Neste cenário onde é utilizado tanto o envio de quadros *RTS* e *CTS* para a reserva do meio como a fragmentação dos pacotes, a rede apresentou um *throughput* agregado menor do que a situação apresentada na Figura 6.20, onde os pacotes não são fragmentados.

Com os resultados destas simulações conclui-se que a carga na rede terá uma influência grande juntamente com os limiares de *RTS* e de fragmentação no desempenho das redes IEEE 802.11. É importante observar que a situação simulada é um caso particular, onde com cerca de 20 estações gerando o tráfego estatístico configurado, já apresentou uma queda no *throughput* agregado.

Utilizando os recursos de simulação do *OPNET*$^{\hat{a}}$ *Modeler* existe a possibilidade da coleta de outras medidas estatísticas, assim como a criação de diversas topologias de rede, no entanto, apenas algumas foram escolhidas como forma de analisar as características principais sobre as redes IEEE 802.11 apresentadas no Capítulo 2.

Capítulo VII

7 - Conclusões

Inicialmente, não havia o conhecimento de como realmente o meio sem fio poderia afetar os softwares de gerência convencionais e o desempenho da rede. Ao longo desta dissertação, constatou-se que a grande diferença no desempenho entre as redes IEEE 802.11 e a IEEE 802.3 se encontra no nível da camada *MAC* com parâmetros como limiar de *RTS* e de fragmentação, tráfego de controle, tempos entre quadros e de *backoff*, já que o meio utilizado para transmissão dos dados fica transparente para as camadas mais altas. Embora não seja parte do escopo desta dissertação a influência no desempenho das redes sem fio devido as características físicas da transmissão, deve-se estar ciente que transmissões em meio não confinado apresentam uma susceptibilidade maior a interferências.

Através da elaboração da metodologia proposta, verificou-se que existem diversas ferramentas no mercado que podem ser utilizadas para a gerência de redes sem fio. Algumas destas ferramentas podem realizar a coleta, o tratamento e a apresentação de alguns dos indicadores de desempenho. No entanto, para a obtenção de medidas estatísticas específicas para o auxílio à gerência de redes, torna-se necessário o tratamento destes dados utilizando a possibilidade de programação de macros empregando ferramentas como o *Microsoft® Excel*. Tanto as ferramentas de gerência comerciais, como as encontradas de forma gratuita podem receber o tratamento de seus dados coletados e a manipulação conforme as necessidades. Com o estudo sobre estes softwares de coleta, constatou-se que não há problemas em sua utilização para redes sem fio, já que eles utilizam o protocolo *SNMP* que atua sobre o protocolo de transporte *UDP*, independentemente das camadas mais baixas. Sendo assim, desde que o agente *SNMP* esteja ativado no dispositivo a ser gerenciado e o administrador da rede conheça a sua *MIB*, ele poderá coletar quaisquer dados que fizerem parte da *MIB*. Além disso, existem alguns softwares que facilitam a vida do administrador da rede, apresentando a estrutura em árvore da *MIB*, chamados

navegadores de *MIB* (*MIB Browsers*), ver Anexo A. Com relação às *MIBs* utilizadas pelos dispositivos de redes IEEE 802.11, verificou-se que a maioria dá suporte à *MIB-II*, onde se consegue obter boa parte dos objetos referentes aos indicadores de desempenho. No entanto, alguns dispositivos ainda apresentam a sua *MIB* proprietária, a *MIB Bridge* e também a *MIB* IEEE 802.11.

A integração entre a ferramenta de coleta *MRTG*â e o simulador *OPNET*â *Modeler* não apresentou problemas, já que existe a facilidade da importação fiel dos dados coletados. Contudo, caso não haja esta facilidade para a ferramenta de coleta específica, deverá existir a construção de módulos de adaptação dos dados gerados pela ferramenta de coleta para a ferramenta de simulação, além da necessidade da caracterização estatística do tráfego da rede.

O mesmo processo de planejamento de capacidade para expansão de redes proposto no Capítulo 4 pode ser realizado independente do tipo de rede utilizado, já que o importante será a carga gerada pelos novos usuários e/ou aplicações na rede como um todo.

Como conclusão mais importante, verifica-se que tanto as redes IEEE 802.11 como as IEEE 802.3 podem ser analisadas com a mesma metodologia, inclusive sendo utilizado o mesmo software de coleta, os mesmos objetos da *MIB-II* e o mesmo tratamento dos dados. É importante observar que os softwares específicos para redes sem fio devem ser empregados quando se deseja configurar a rede, coletar informações específicas de seus dispositivos, tais como o nível de sinal, taxa de transmissão atual, número de estações associadas com o *AP*, etc. Desta forma, o administrador de uma rede cabeada e que deseje ampliar esta rede com o padrão IEEE 802.11 deverá dispor de um software tradicional e do software específico para redes IEEE 802.11, de forma a complementar o processo gerencial.

Outra conclusão que pode ser tirada se refere ao fato das redes sem fio normalmente serem utilizadas para agregar funcionalidades às redes tradicionais e não para substituí-las. Sendo responsável por manter a conectividade entre o *backbone* tradicional e o usuário móvel.

Para trabalhos futuros, sugere-se a possibilidade do estudo mais aprofundado das características dos softwares de coleta *free* baseados no protocolo *SNMP*, preferencialmente sendo executados em uma rede sem fio instalada. Além das

características sobre os softwares de coleta de dados, com a rede IEEE 802.11 instalada, haverá a possibilidade de confirmar a relação entre os parâmetros configurados e o desempenho da rede e, ainda, realizar interferências no sinal transmitido para verificar se o nível de desempenho continua aceitável.

A metodologia proposta pode ser ampliada com a análise dos objetos disponibilizados pelas *MIBs* dos equipamentos e que são voltados para as outras áreas de gerência: Segurança, Configuração, Contabilidade e Falhas. Embora existam diversos softwares que possam ser utilizados, normalmente não haverá apenas um que realize todas as tarefas requisitadas pelo administrador da rede. Desta forma, torna-se interessante a criação de uma ferramenta computacional que consolide a metodologia proposta, aliando a coleta de dados e a elaboração de relatórios específicos para a tomada de decisões necessárias a cada fase da metodologia. A capacidade de reconhecer e navegar pelas *MIBs* do agente e apresentá-las para o administrador da rede é uma característica que pode ser agregada a esta ferramenta.

Além destas propostas para trabalhos futuros, uma pesquisa visando a construção de um sistema autônomo de gerência de redes, assumindo a tomada de decisões pertinentes a cada uma das quatro fases propostas na metodologia é bastante interessante. Como sugestão, pode ser seguida a abordagem de aplicação de modelos baseados em Agentes Inteligentes.

Referências Bibliográficas

[1] *"Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the 2.4 GHz band"*. IEEE Standard 802.11b, 1999.

[2] *"Wireless LAN medium access control (MAC) and physical layer (PHY)"*. IEEE Standard 802.11, 1999.

[3] PRASAD, N.; PRASAD, A.; *"WLAN Systems and Wireless IP for Next Generation Communications"*. Artech House. Estados Unidos; 2001.

[4] ERGEN, M.; *"IEEE 802.11 Tutorial"*, http://esoumoy.free.fr/telecom/tutorial/ieee-tutorial.pdf, 10/02/2003; 2002.

[5] TANENBAUM, A. S.; *"Redes de Computadores"*. Editora Campus. Rio de Janeiro; 1997.

[6] STALLINGS, W.; *"SNMP, SNMPv2, SNMPv3, RMON1 e RMON2"*. Addison Wesley. Third Edition. Estados Unidos; 1999.

[7] BRENNER, P.;*" A Technical Tutorial on the IEEE 802.11 Protocol"*, http://www.sss-mag.com/pdf/802_11tut.pdf, 15/12/2002; 1997.

[8] GANZ, A., PHONPHOEM, A., GANZ, Z.; *"Robust SuperPoll Protocol for IEEE 802.11 Wireless LANs"*, http://www.argreenhouse.com/society/TacCom/papers98/17_03i.pdf, 10/11/2002; 1998.

[9] RUBINSTEIN, M.,G.; REZENDE, J.,F.; "Qualidade de Serviço em Redes 802.11", http://www.gta.ufrj.br/ftp/gta/TechReports/RuRe02.pdf, 05/06/2002.

[10] GREEN, J. H.; *"The Irwin Handbook of Telecommunications Management"*. McGraw-Hill. Second Edition. Estados Unidos; 1996.

[11] *"Wireless LAN Network Management"*, http://www.phillips-infotech.com/infosales4.htm, 15/12/2002.

[12] HEGERING, H.; ABECK, S.; NEUMAIR. B.; *"Integrated Management of Networked Systems: Concepts, Architectures, and Their Operational Application"*. Morgan Kaufmann Publishers, Inc. São Francisco, CA; 1998.

[13] RECOMMENDATION X.700, ITU-T; *"Management Framework for Open Systems Interconection (OSI) for CCITT Applications"*, http://www.ucb.br/prg/professores/maurot/GR/GR.htm, 07/02/2003; 1992.

[14] PAN, H.; *"SNMP-Based ATM Network Management"*. Artech House. Estados Unidos; 1998.

[15] SLOMAN, M.; *"Network and Distributed Systems Management"*. Addison Wesley. Grâ Bretanha; 1996.

[16] CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; Davin, J.; *"Simple Network Management Protocol"*; http://www.ietf.org/rfc/rfc1157.txt? number=1157, 10/11/2002; 1990.

[17] ROSE, M.; MCCLOGHRIE, K.; *"Structure and Identification of Management Information for TCP/IP-based internets"*, http://www.ietf.org/rfc/rfc1155.txt? number=1155, 02/10/2002; 1990.

[18] ROSE, M.; *"Management Information Base for Network Management of TCP/IP-based internets: MIB-II"*, http://www.ietf.org/rfc/rfc1213.txt?number=1213, 10/10/2002; 1991.

[19] ROSE, M.; *"SNMP over OSI"*, http://www.ietf.org/rfc/rfc1418.txt?number=1418, 21/03/2003; 1993.

[20] MINSHALL, G.; RITTER, M.; *"SNMP over AppleTalk"*, http://www.ietf.org/rfc/rfc1419.txt?number=1419, 21/03/2003; 1993.

[21] BOSTOCK, S.; *"SNMP over IPX"*, http://www.ietf.org/rfc/rfc1420.txt?number=1420, 21/03/2003; 1993.

[22] CASE, J.; et al.; *"Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv.2)"*, http://www.ietf.org/rfc/rfc1905.txt?number=1905, 05/02/2003; 1996.

[23] CASE, J; et al.; *"Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)"*, http://www.ietf.org/rfc/rfc1903.txt?number=1903, 15/03/2003; 1996.

[24] CASE, J.; et al.; *"Manager-to-Manager Management Information Base"*, http://www.ietf.org/rfc/rfc1451.txt?number=1451, 11/02/2003; 1993.

[25] CASE, J.; et al.; *"Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)"*, http://www.ietf.org/rfc/rfc1907.txt?number=1907, 12/03/2003; 1996.

[26] CASE, J.; et al.; *"Coexistence between Version 1 and Version 2 of the Internet- standard Network Management Framework"*, http://www.ietf.org/rfc/rfc1908txt?number= 1908, 20/02/2003; 1996.

[27] DRAGO, Á.,B.; *"Uma Ferramenta Computacional para Auxílio na Prática da Gerência de Desempenho de Redes de Computadores."*, Universidade Federal do Espírito Santo; 2001.

[28] SOARES, L., F., G.; *"Redes de Computadores: Das LANs, MANs e WANs às Redes ATM"*. Editora Campus. Rio de Janeiro; 1995.

[29] GARCIA, A.,S.; *"Avaliação de Desempenho"*. Universidade Federal do Espírito Santo. Vitória; 1997.

[30] MENASCÉ, D., A.; ALMEIDA, V., A., F.; *"Capacity Planning for Web Services: Metrics, Models and Methods"*. Prentice Hall. Estados Unidos; 2002.

[31] JAIN, R.; *"The Art of Computer Systems Performance Analysis"*. John Wiley. New York; 1991.

[32] SOARES, L., F., G.; *"Modelagem e Simulação Discreta de Sistemas"*. IME-USP; 1990.

[33] KELTON, W., D.; *"Simulation with Arena"*. WCB/McGraw-Hill. Estados Unidos; 1998.

[34] UCB/LBNL/VINT; *"Network Simulator – NS (version 2)"*, http://www.isi.edu/nsnam/ns/, 03/03/2003.

[35] OPNET® Modeler; *"Network Simulator"*, http://www.opnet.com/products/modeler/home.html, 10/05/2002.

[36] *"Network Management in a Wireless Environment"*, http://ecc400.com/symbol /wp_stwp0013.htm, 06/02/2003.

[37] Diversas *MIBs* proprietárias e públicas; *"SNMP Link"*, http://www.snmplink.org/, 15/11/2002.

[38] FERNANDEZ, M.; DELFINO, G.; PEDROZA, A.; *"Protocolo para Gerenciamento Hierárquico de Redes de Computadores e de*

Telecomunicações", http://www.gta.ufrj.br/~marcial/publicacoes/MarcialVol16-2.pdf, 05/05/2003; 2001.

[39] *"Network Management for Wireless Data Collection Applications"*, http://www.psionteklogix.com/assets/downloadable/Network_Mgmt_for_WLANs.pdf, 10/02/2003.

[40] LANGILLE, P.; RIJSINGHANI, A.; MCCLOGHRIE, K.; *"Definitions of Managed Objects for Bridges"*, http://www.ietf.org/rfc/rfc1493.txt?number=1493, 07/04/2003; 1993.

[41] *"BreezeCom private MIB version 1.0";* http://www.icg.ro/Resources/bnpro-ae.pdf, 10/04/2003.

[42] MONTEIRO M., E.; *"Metodologia para Gerência Pró-ativa de Desempenho em Redes de Comunicação de Dados"*. Universidade Federal do Espírito Santo; 2000.

[43] KANTOROVITCH, J.; et al.**;** *"Wireless SNMP"*, http://www.isoc.org/isoc/conferences/inet/01/CDproceedings/T96/_INET_Wireless_*SNMP*_paper.html, 15/08/2002.

[44] Gerenciamento de Redes; *"Apostila MIBs SNMP"*. http://redes.ucpel.tche.br/ensino/070020/html/apostila.html, 15/03/2003.

[45] *"Wireless Fleet Network Management"*, http://students.depaul.edu/~nmicek/WirelessNetworkManagement.html, .07/02/2003.

[46] MONTEIRO M., E., GARCIA, A., S. ;"Metodologia Computacional para Tratamento Estatístico de Dados em Gerencia de Redes", http://www.maxima-ti.com.br/White Paper/WhitePaper.htm, 15/04/2003; 1999.

[47] SANTAMARÍA, A., HERNÁNDEZ, F., J., L.; *"Wireless LAN Standards and Applications"*. Artech House. Estados Unidos; 2001.

[48] Symbol® Technologies; *"SpectrumSoft™ WNMS Wireless Network Management System"*, http://www.ecc400.com/symbol/std00068.htm - mgmt, 11/11/2002; 1998.

[49] Proxim Corporation; *"Wireless Network Manager – User Guide"*, http://www.orinocowireless.com/support/all/orinoco/manuals/pdf/WinmaUserManual.pdf, 12/05/2003.

[50] AZAMBUJA, N.,S.; et al.; *"Gerência de uma Rede Metropolitana Sem Fio"*, http://www.cbcomp.univali.br/pdf/2001/red008.pdf, 15/10/2002.

[51] RIBAS, J.,C.,C.; et al.; *"Perfil de Link Sem Fio em Ambiente Aberto: Avaliação Através de Medições"*, http://www.cefetsc.edu.br/usuarios/julio/download /PLW.pdf, 15/02/2003.

Glossário

100BaseTduplex – Refere-se ao cabo de par trançado sem blindagem que transporta dados sem modulação nos dois sentidos de comunicação simultaneamente a uma taxa de 100 Mbps.

Abstract Sintax Notation – version one (ASN.1) - É uma linguagem formal desenvolvida pelos órgãos *International Telecommunication Union* (*ITU*) e pelo *International Organization for Standardization* (*ISO*) para a representação e identificação dos objetos na base de informações de gerência visando realizar transferência de informações entre aplicações de diferentes sistemas. É uma forma de descrição abstrata dos dados com o objetivo de não se levar em consideração a estrutura e restrições do equipamento no qual está sendo implementada.

Backup – Cópia de dados com o objetivo de restaurá-los em caso de problemas ou de perda de dados.

Bps – Bits por segundo. Unidade utilizada para medir velocidade de transmissão e recepção de dados. Pode aparecer como múltiplo de mil com Kbps (kilobits por segundo), Mbps (megabits por segundo) e Gbps (gigabits por segundo).

Bridge – É um dispositivo que interconecta duas *LANs* ou dois segmentos de uma mesma *LAN*. Podendo interconectar por exemplo, uma rede Ethernet com uma *Token Ring*. Ao contrário dos roteadores que atuam na camada de rede, as *bridges* atuam na camada *MAC*.

Buffer – Espaço de memória em dispositivos destinado a armazenar pacotes de dados que esperam processamento.

Byte – Representa normalmente um grupo de 8 bits.

Community – Uma senha que limita o acesso a uma determinada entidade da *MIB* de um elemento de rede.

Cyclic Redundancy Checking (CRC) – É um código para a detecção de erros.

Datagrama – Unidade de transporte utilizada pelo *IP*.

E-mail – Trata-se do correio eletrônico onde, através da Internet, consegue-se acessá-lo.

Endereço MAC – Endereço físico da interface de rede.

Ethernet - É uma das tecnologias de rede local (*LAN*) mais amplamente utilizada hoje em dia. Especificada pelo padrão IEEE 802.3, foi desenvolvida originalmente pela *Xerox*®, para então continuar sendo desenvolvida por *Xerox*®, *DEC*® e *Intel*® em conjunto.

Event Report – Conjunto de estatísticas enviado ao gerente pelos respectivos agentes presentes na rede.

Frames – É um grupo de bits que inclui os dados, além de um ou mais endereços e outras informações para o controle do protocolo. Geralmente este nome se refere a unidade de dados da camada 2 do modelo *OSI*.

Gateway – Dispositivos utilizados para conectar redes. Os tipos mais comuns de *gateways* são repetidores, *bridges*, roteadores ou mesmo um computador pessoal.

Hub – Dispositivo que funciona como um barramento único para conectar diferentes estações em um ambiente de rede.

Interface – Software e hardware que habilitam a camada de rede de um protocolo para transmitir uma *PDU* através do meio.

International Organization for Standardization (ISO) – Órgão internacional fundado para promover uma cooperação internacional para o progresso da ciência e tecnologia.

International Telecommunication Union (ITU) – Organização formada para coordenar a junção entre o mundo das telecomunicações e o mundo de comunicação de dados.

Internet Protocol (IP) – Protocolo da camada de rede do modelo *OSI*. Utilizado para o transporte de datagramas através da Internet.

Industrial, Science and Medical (ISM) – Banda de freqüência alocada para o desenvolvimento de aplicações de rádio freqüência licenciadas automaticamente.

Jitter – É a variação de atraso da entrega de datagramas.

Link – Elo de conexão entre dois ou mais pontos.

Local Area Network (LAN) – Conjunto de dispositivos interconectados entre si de modo a formar uma rede local.

Management Information Base (MIB) – Base de dados lógica que contém informações de configuração, *status* e estatísticas de um dispositivo.

Media Access Control (MAC) – Protocolo que determina o acesso de uma estação ao meio de transmissão.

On-line – Na linha, ou seja, um serviço que se encontra *on-line* pode ser acessado pela Internet.

Overhead – Informação de controle que trafega na rede gerando uma carga adicional à mesma. Quanto menor o *overhead*, maior será a possibilidade de utilização de um enlace.

Polling – Operação de comunicação onde uma estação fica, periodicamente, enviando mensagens do tipo *request-response* para outra estação.

Point-to-Point Protocol (PPP) – É um dos protocolos mais conhecidos para acesso via interface serial. Estabelece um método em que um computador, através da linha telefônica e um modem de alta velocidade, consegue acessar a Internet.

Proxy – Agente que responde a solicitações de um ou mais gerentes, realizando um *polling* em dispositivos remotos.

Request-response – Combinação das mensagens de solicitação (*request*) e de sua resposta (*response*).

Roteador – *Gateway* de camada de rede utilizado para conectar redes locais entre si, ou estas a redes de longa distância. Possui uma tabela de roteamento para encaminhar os pacotes.

Switch – É um equipamento utilizado para segmentar uma rede em partes menores, com o intuito de melhorar o desempenho. Uma boa aplicação do *switch* é definir níveis de prioridade nas portas de acesso à rede. Exceto por este aspecto, o *switch* é muito parecido com o *hub*.

Tokens – São quadros especiais utilizados para o controle de permissão para a transmissão em algumas tecnologias de redes locais, como por exemplo, a *Token Bus*.

X.25 – É um padrão criado para oferecer uma interface entre as redes públicas de comutação de pacotes e seus clientes.

Wired Equivalent Privacy (WEP) - É um algoritmo de criptografia definido pelo IEEE 802.11 para prevenir intrusos na rede e captura de tráfego por pessoas não autorizadas. Trata-se de um algoritmo que dá a confidencialidade de uma *LAN* com fio que não emprega técnica de criptografia à rede sem fio.

Anexo A – Um Estudo sobre Softwares de Gerência Utilizados em Redes IEEE 802.11

A.1 – Introdução

As ferramentas de gerência utilizadas em redes cabeadas não são adequadas aos aspectos dinâmicos encontrados nas redes sem fio, tais como: associação a uma célula (*BSS*), *roaming*, conexões aleatórias e o gerenciamento de potência. Já os softwares especialmente construídos para redes sem fio consideram todas essas características. Estas ferramentas foram chamadas de patéticas ao chegarem ao mercado [11], no entanto, com as melhorias anunciadas nestes produtos, a confiança passou a ser conquistada e novos produtos chegaram ao mercado.

O ideal para a realização deste estudo seria a instalação de alguns softwares de gerência, a fim de possibilitar a análise do desempenho de uma rede sem fio. No entanto, como não se dispõe de uma rede sem fio instalada, serão apresentados alguns softwares utilizados na gerência de redes sem fio, verificando os seus requisitos de instalação, funcionamento e características básicas. Com este estudo sobre as possíveis ferramentas de coleta de dados, análise e configuração, o administrador da rede consegue adquirir um conhecimento que irá facilitar na sua escolha pela ferramenta de coleta dos dados proposta no Capítulo 4 desta dissertação.

A.2 - O Software *SpectrumSoft*^{ä} *WNMS*

O software *SpectrumSoft*^{ä} *WNMS* é facilmente integrado a plataformas de gerência de redes em ambientes corporativos. É construído utilizando os padrões comprovados de gerência, *SNMP* e *MIB-II*. Possui uma interface gráfica bastante amigável, fornecendo uma ferramenta intuitiva para investigar, examinar e gerenciar uma rede sem fio. Com a utilização deste software o administrador da rede tem ferramentas para instalar, configurar, monitorar centralmente e gerenciar toda a sua rede [48].

Obtenção do Produto

Trata-se de um software de gerência pago, produzido pela *Symbol Technologies*. Maiores informações podem ser obtidas no endereço eletrônico http://www.symbol.com/products/wireless/mobility11.html.

Requisitos de Instalação e Funcionamento

Pode ser instalado tanto na versão *standalone* para o *Microsoft Windows NT* ou 2000, ou como um produto integrado as plataformas *HP OpenView*, *NetView* ou *Unicenter*.

Características Básicas

A utilização deste software é voltada para a gerência dos dispositivos que formam a rede *Spectrum24*, tornando assim, um produto altamente proprietário. A única exceção é no que se refere ao protocolo *SNMP*, já que no caso do emprego de outro protocolo de gerência, o *SpectrumSoft WNMS* dispõe de um agente *proxy*. Este software possibilita a gerência da parte sem fio da rede e o mapeamento dos dispositivos da parte cabeada.

Do amplo conjunto de características fornecidas pelo *SpectrumSoft WNMS*, existe também as funcionalidades definidas pela *ISO* através das cinco áreas de gerência: Falhas, Configuração, Contabilidade, Desempenho e Segurança. A Tabela A.1 ilustra as características do *SpectrumSoft WNMS* relacionadas com as suas respectivas áreas de gerência.

Tabela A.1 – *Características x Áreas de Gerência OSI para o SpectrumSoft WNMS*

Características	Áreas de Gerência	Benefícios
Notificação de eventos	Falhas	Atualização em tempo real baseado nos eventos importantes da rede.
Configuração do AP ⇒ Gerenciamento do grupo ⇒ Configuração da base de dados ⇒ Suporte ao *SNMP*	Configuração	Economia de tempo, aumento da precisão. Mantém uma configuração consistente.
Monitoramento ⇒ Representação gráfica da rede ⇒ Monitoramento do grupo	Contabilidade Desempenho	Dá um foco tanto na topologia, como no grupo. Monitorando grupos, diminui a complexidade da rede.
Acesso configurável Lista de controle para o acesso	Configuração Segurança	Controla os dispositivos que podem se associar à rede.
Mapeamento da rede	Configuração	Permite a associação à parte cabeada da rede.
Visualização sobre a hierarquia da rede ou especificamente de um dispositivo	Falhas	Amplia as informações requeridas.
Descoberta dos dispositivos	Configuração Contabilidade	Os novos dispositivos são automaticamente reconhecidos. Não é necessária configuração adicional.
Agente Proxy	Falhas	Suporta dispositivos móveis que não utilizam o *SNMP*.
Diagnósticos	Falhas	Análise potencial dos problemas nas áreas de gerência.
Relatório de estatísticas	Contabilidade Desempenho	Revela as tendências do tráfego da rede, permitindo uma análise pró-ativa da rede.
Controle de revisão do software e do firmware.	Configuração	Gerência remota de dispositivos através de uma posição central. Não necessita de serviços para atualizar o software.

O software *SpectrumSoft*ä *WNMS* oferece duas configurações, sendo:

WNMS Integrated – controla toda a rede com uma simples integração dentro de plataformas de gerência, tais como: *OpenView-Solaris, HP-UX*, entre outras.

WNMS Enterprise – não precisa de outra plataforma de gerência. Suporta tanto a instalação como a configuração de uma *WLAN*, assim como a gerência de toda a rede sem fio empregando um ou vários pontos de gerência.

O monitoramento da rede se dá através das *MIBs* ativas nos *APs*, mantendo um modelo em tempo real dos nós ativos da rede. Ainda é possível mensagens de alerta nos terminais de gerência através do suporte às *traps SNMP*.

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.3 – *WNM* (*Wireless Network Manager*) da *Proxim Corporation*

Este software é uma ferramenta de gerência de redes sem fio que permite ao administrador da rede um controle de milhares de pontos de acesso facilmente e remotamente de qualquer lugar do mundo. Entre as suas possibilidades estão: controle, atualização e configuração das redes sem fio utilizando uma simples interface gráfica. É facilmente integrado dentro dos sistemas de gerenciamento *SNMP* existentes.

Obtenção do Produto

Trata-se de um software de gerência pago, produzido pela *Proxim Corporation*. Informações para a instalação de uma versão para experiência por um mês, além de seu manual, podem ser obtidas no endereço eletrônico http://www.orinocowireless.com/products/all/orinoco/winma/winma/index .html.

Requisitos de Instalação e Funcionamento

O mínimo de hardware necessário para o ambiente *Windows*â é: 128 MB de memória e 700 MB (mínimo) / 5 GB (recomendado) de disco. Ainda é indicada a utilização do processador *Pentium*â ou versão mais atual (compatível com *IBM*â) para melhor desempenho.

A sua instalação requer o *Microsoft*â *Windows*â 2000 ou *NT*. Para o caso da utilização da função de descoberta dos dispositivos (*Discovery*) torna-se necessário o

uso da plataforma *HP OpenView*â *Network Node Manager* (*HP OV NNM*) versão 6.1 ou mais avançada.

Características Básicas

Através do *WNM* são obtidas informações detalhadas sobre pacotes: *TCP*, *UDP*, *IP*, *SNMP* e da rede sem fio, como pacotes enviados, recebidos, descartados entre outras utilizando uma janela de monitoramento. Ainda é possível configurar os pontos de acesso e verificar o *status* de seus parâmetros.

Os dispositivos *WNM* enviam notificações (*traps*) assincronamente para a estação de gerência *WNM* através da porta *UDP* 162 e suportam *traps* específicas do padrão *MIB-II* e da *MIB* IEEE 802.11 [49].

Da mesma forma que o *SpectrumSoft*ä *WNMS*, o emprego do *WNM* é restrito aos equipamentos de alguns fabricantes [49].

A Figura A.1 ilustra a possibilidade da gerência remota de qualquer lugar do mundo utilizando a Internet. Esta facilidade permite a verificação de todos os dispositivos da rede sem fio através da função *Auto Discovery* ou através do endereço *IP*.

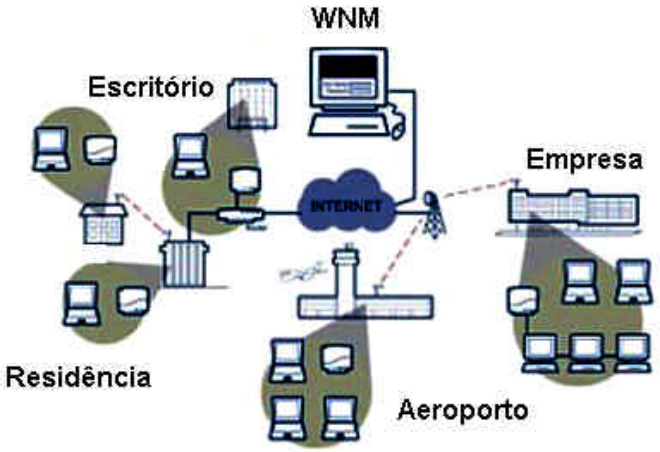


Figura A.1 - *Redes IEEE 802.11 Gerenciadas através da Internet*

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.4 - Gerenciamento *Corinex® Wireless – Powerline*

Trata-se de um software de gerência que permite ao administrador da rede a sua configuração remota, monitoramento e teste. Qualquer dispositivo da rede *Corinex®* tanto da parte sem fio como da cabeada é controlado e monitorado através do protocolo *SNMP*. O gerenciamento completo dos dispositivos sem fio *Corinex®* é alcançado com a integração da plataforma *Corinex® View SNMP*. No entanto, existe a possibilidade da utilização de módulos de gerência *Corinex®* como parte de qualquer sistema de gerenciamento baseado no *SNMP*. Além disso, o gerenciamento *Corinex®* pode coletar estatísticas de utilização da rede para serem utilizadas pela área de gerência de contabilidade.

Obtenção do Produto

Trata-se de um software de gerência pago, produzido pela *Corinex® Global*. Informações sobre a aquisição deste software, assim como o seu manual podem ser encontrados no endereço eletrônico http://www.corinex.com/web/doccx.nsf/ a7b17e752fd2a7fac1256aed004214e0/2e93984f9407c1cac1256c60003e80b8.

Requisitos de Instalação e Funcionamento

Deve ser utilizado um processador *Pentium®* 266 MHz ou melhor, 64 MB de memória e 1 MB de espaço em disco.

Pode ser instalado em qualquer máquina que possua o sistema operacional *Windows®* 98, 2000, *NT*, *ME*, *XP* ou *Linux*.

Características Básicas

Este software é construído com base na linguagem *Java* o que traz como benefícios a independência do sistema operacional e da plataforma utilizados. Dispõe de um agente *proxy SNMP* que atua como um tradutor dos comandos *SNMP* utilizados pelo *Corinex®* dentro de um protocolo proprietário empregado pelos dispositivos sem fio. Possui a capacidade de monitorar e configurar dispositivos remotamente, além de monitorar a utilização da banda em tempo real. Realiza um reconhecimento automático da topologia da rede e tem a possibilidade do envio de notificações pelo *e-mail.*

A Figura A.2 ilustra a possibilidade da interface gráfica como ferramenta para o administrador da rede. Como se observa nesta figura, no instante selecionado a transferência de dados está com uma taxa de 3,18 Mbps.

Figura A.2 - *Gráfico da Transferência de Dados - Corinex*[ª]

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.5 - *MRTG*[â] (*Multi Router Traffic Grapher*) 2.9.27

Obtenção do Produto

O *MRTG*[â] é um software *free* para monitorar indicadores de desempenho de uma rede, podendo ser encontrado para *download* na página http://people.ee.ethz.ch/~oetiker/webtools/*mrtg*/pub. Para o seu funcionamento também é necessária a instalação do compilador *ActivePerl*, disponível para *download* na página http://www.activestate.com.

Requisitos de Instalação e Funcionamento

O sistema operacional utilizado pode ser *Unix*[â], *Windows*[â] 95, 98, *ME*, *NT*, 2000, *Linux* ou *Mac OS X 10.1*. A ocupação em disco para o *MRTG*[â] 2.9.27 é de 3,86 MB e para o *ActivePerl* 5.8.0 é de 46,9 MB. A carga do programa consome aproximadamente 100 KB de memória.

O software *MRTG*[â] não necessita ser instalado. O arquivo adquirido na página informada é de auto - extração, bastando executá-lo e em seguida informar o local onde o mesmo será descomprimido.

Apenas será necessária a criação de uma pasta para publicação das páginas com os gráficos gerados pelo programa. Para a instalação do *ActivePerl* basta executar o arquivo *ActivePerl-5.8.0.805-MSWin32-x86* encontrado na página informada anteriormente. O tempo total de instalação é de aproximadamente 2 minutos.

Após a instalação, deve-se relacionar os dispositivos a serem monitorados através da criação de um ou mais arquivos de configuração. Isto pode ser feito manualmente ou através da ferramenta *cfgmaker* pertencente ao pacote do *MRTG*â. O tempo de configuração pode variar de acordo com a complexidade do monitoramento a ser realizado. A seguir é mostrado, como exemplo, uma parte de um arquivo de configuração responsável pelo monitoramento de tráfego do enlace INATEL - IMPSAT.

```
---------------------------------------------------------------------
Target[impsat]: 2:SNMP3197I@200.186.136.129:
Options[impsat]: growright,bits
SetEnv[impsat]: MRTG_INT_IP="200.186.136.129" MRTG_INT_DESCR="Serial0"
MaxBytes[impsat]: 128000
Title[impsat]: Análise de tráfego Inatel <-> Impsat
PageTop[impsat]: <H1>Análise de tráfego Inatel <-> Impsat</H1>
<TABLE>
<TR><TD>System:</TD> <TD>Link Inatel <-> Impsat</TD></TR>
<TR><TD>Maintainer:</TD><TD>SeçãodeRedeseInternet</TD></TR>
<TR><TD>Description:</TD><TD>Serial0  </TD></TR>
<TR><TD>Max Speed:</TD>  <TD>1 Mbps</TD></TR>
<TR><TD>Ip:</TD><TD>200.186.136.129</TD></TR></TABLE>
#---------------------------------------------------------------------
```

Com a chave *"Target"*, é indicado ao *MRTG*â qual dispositivo ele deverá monitorar. Esta chave possui o seguinte formato "porta:comunidade@dispositivo", isto vai gerar um gráfico de tráfego que passa por uma determinada interface de um dispositivo (referenciado geralmente pelo número *IP*), usando a comunidade a que este dispositivo pertence. Já o *MaxBytes* especifica quantos bytes por segundo esta interface pode suportar. Para os enlaces (*links*) mencionados em bits por segundo é necessário dividir por oito e dar o valor em bytes por segundo.

Contudo, não foi possível monitorar uma pequena parte da rede do INATEL que não é cabeada, já que o *AP* que está disponível não é gerenciável através do protocolo *SNMP*, ou seja, não dispõe de um agente *SNMP*. A fim de ilustrar a possibilidade do *MRTG*â estar coletando dados sobre uma rede sem fio, resolveu-se

exemplificar a coleta dos pacotes que entram e saem pela interface que liga o *AP* da *Cisco Aironet*â à rede IEEE 802.11b, como se verifica na parte do *script* de configuração e do gráfico a seguir.

Traffic Analysis for 10.224.40.23 -- aa_aironet01

System: aa_aironet01 in 1229_Albany_Ave

Maintainer: Stephen_Shipman

Description: Aironet DS-SS Radio

ifType: Other (1)

ifName:

Max Speed: 1000.0 kbits/s

IP: 10.224.40.23 (aa_aironet01)

É interessante observar que o *ifType*, que indica o tipo de interface é *other* (1), como foi analisado na seção 4.2.3 do Capítulo 4 desta dissertação. Na Figura A.3 é apresentado, como exemplo, um gráfico diário do tráfego que passa pela interface sem fio do *AP* da *Cisco Aironet*â.

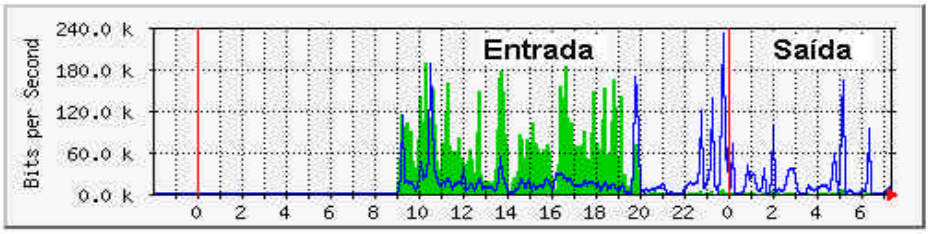


Figura A.3 - *Gráfico "Diário" (5 minutos - média)*

Máx Ent: 190.3 kb/s (19.0%) Média Ent: 24.4 kb/s (2.4%) Atual Ent: 2776.0 b/s (0.3%).

Máx Saí: 231.4 kb/s (23.1%) Média Saí: 14.3 kb/s (1.4%) Atual Saí: 29.7 kb/s (3.0%).

A maior desvantagem observada em comparação às ferramentas com interface gráfica, é que o processo de configuração e operação deste software é feito com linhas de comando, dificultando o manuseio para usuários com pouca experiência no *MRTG*â.

Características Básicas

O *MRTG*â é um software baseado na arquitetura *SNMP* (*Simple Network Management Protocol*) que permite a construção de páginas *Web* para a monitoração

de sistemas. Acionado em intervalos regulares o software consulta as *MIBs* (*Management Information Base*) dos dispositivos monitorados para buscar os valores das variáveis de interesse conforme especificados nos arquivos de configuração. De posse desses valores, ele gera gráficos contendo as curvas de evolução das variáveis monitoradas. Quatro tipos de gráficos podem ser gerados para a mesma medida: diário, semanal, mensal e anual.

Esta ferramenta tem um uso bastante difundido para a análise de tráfego principalmente no meio acadêmico, por ser *free* e possuir funcionalidades importantes ao processo de monitoramento do ambiente.

O *MRTG*â possui as seguintes características:

- Geração de resultados gráficos no formato *html*;
- Permite o monitoramento da utilização da *CPU* e do disco, estado do enlace físico de uma interface, utilização de memória, quantidade de pacotes e bits que entram e saem de uma interface;
- Gerenciamento baseado em método de *polling* e utilizando o protocolo *SNMP*.

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.6 – *LoriotProâ*

É um software capaz de monitorar os recursos computacionais que garantem disponibilidade e desempenho da rede para o seu usuário. Todos esses recursos são monitorados através do protocolo *SNMP*. O controle da rede ainda é realizado com o auxílio dos protocolos *ICMP* e *HTTP* para o monitoramento via *Web*.

Obtenção do Produto

Trata-se de um software pago, que possui uma versão *free* por um período de 30 dias, podendo ser encontrado no endereço eletrônico http://www.loriotpro.com/Download/DownLoad_EN.htm.

Requisitos de Instalação e Funcionamento

Deve ser utilizado um processador *Pentium*â III ou mais avançado, 256 MB de memória e 4 GB de disco. O sistema operacional pode ser o *Microsoft*â *Windows*â 98, *NT* ou 2000.

Características Básicas

- Consegue mostrar os ícones representativos dos dispositivos e o seu *status* atual em tempo real;
- Registro dos dados em forma de inventário e disponibilizado em *html*;
- Coleta, armazena e apresenta informações de alarmes em relatórios;
- Permite a configuração remota de qualquer dispositivo *IP* através dos objetos da *MIB* e comandos (*set*) do *SNMP*;
- Descobre os nós da rede e desenha um mapa com os dispositivos *IP*;
- Disponibiliza o acesso via *Web* de forma que a rede possa ser monitorada de qualquer localização;
- Detecta as *MIBs* que são suportadas por cada dispositivo;
- Fornece um *script* que facilita a geração do relatório em *html*;

A Figura A.4 ilustra a possibilidade de navegar em qualquer *MIB* proprietária ou pública, de forma a coletar informações sobre seus objetos. Vale lembrar que para utilização desta facilidade é preciso ter o arquivo da *MIB* compilado.

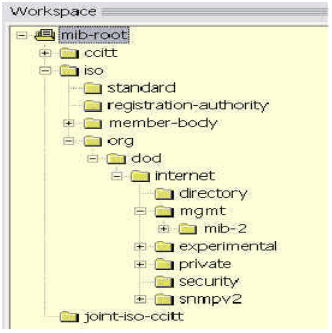


Figura A.4 - *Navegando nas MIBs SNMP através do LoriotPro â*

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.7 – *Net – SNMP*

É um pacote de ferramentas e bibliotecas relacionadas com o protocolo *SNMP*, incluindo um agente extensível, uma biblioteca *SNMP*, ferramentas para pedir ou alterar informações dos agentes *SNMP*, gerar e tratar notificações (*traps*) *SNMP*, entre outras.

Obtenção do Produto

É um software construído em linguagem C sendo encontrado para *download free* na página http://net-snmp.sourceforge.net/. Em versões anteriores recebe o nome *UCD-SNMP*.

Requisitos de Instalação e Funcionamento

Para conseguir o sucesso na instalação deste software é necessário um bom conhecimento do ambiente onde se deseja instalar, já que as bibliotecas utilizadas e todos os recursos deste pacote devem ter seus caminhos indicados corretamente.

Tanto as aplicações, como os agentes são executados (pelo menos em parte) sobre os seguintes sistemas operacionais:

- *HP-UX* (9.10, 10.20 e 11.0 -- ver *README.hpux11*)
- *Ultrix* (4.2 a 4.5)
- *Solaris* (2.3 a 2.8) and *SunOS* (4.1.2 a 4.1.4)
- *OSF* (3.2 e 4.0)
- *NetBSD* (1.0 a 1.5*alpha*)
- *FreeBSD* (2.2 a 4.1)
- *BSDi* (2.1 a 4.1)
- *Linux* (*kernels* 1.3 a 2.4)
- *AIX* (3.2.5 e 4.1.5)
- *OpenBSD* (2.6 e 2.8)
- *Irix* (5.1 a 6.5)
- *OS X* (10.1.1 e 10.1.2)
- *Dynix*/*PTX* 4.4

Este conjunto de aplicações ainda pode ser instalado em ambiente *Windows*^{â} de acordo com o *README.win32,* no entanto, alguns módulos de *MIBs* não são executados neste ambiente.

Características Básicas

Este pacote atualmente suporta o *SNMPv.1* original, *SNMPv.2c* (*RFCs* 1901 a 1908) e *SNMPv.3* (*RFCs* 2571 a 2575). Sendo assim, o agente irá responder aos pedidos utilizando qualquer um destes protocolos e todas as ferramentas utilizadas deverão possuir em sua linha de comando a versão do protocolo.

Possui suporte às estatísticas gerais da rede através da *MIB-II* (*RFC* 1213), extensões do agente *UCD* para obtenção dos consumos de memória e disco, linhas de comando, tratamento de erros e também os recursos das máquinas coletados nos objetos da *RFC* 1514 que está em implementação inicial. Além destas *MIBs* utilizadas, as *MIBs* do *SNMPv.3* também podem ser empregadas. Existe ainda a possibilidade de acrescentar novas *MIBs* aos agentes de forma simples.

É um software que não é voltado a coletas específicas, podendo coletar os dados a respeito dos objetos que o usuário achar necessário na *MIB* disponibilizada pelo agente. Com a utilização do navegador de *MIB Tk/Perl* existe a facilidade de navegar na *MIB* do agente e apresentá-la ao administrador da rede.

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.8 – *MG - SOFT MIB Browser*

É um software produzido pela *MG–SOFT Corporation*. Possibilita o monitoramento e a gerência de qualquer dispositivo *SNMP* na rede, como servidores de banco de dados ou arquivos, modens, impressoras, roteadores, *switches*, *APs*, entre outros. Suporta os protocolos padrões *SNMPv.1*, *SNMPv.2c* e *SNMPv.3*.

Obtenção do Produto

O *MG-SOFT MIB Browser* fornece uma versão limitada para avaliação *free* durante 30 dias. A aquisição deste software pode ser feita no endereço eletrônico: http://www.mg-soft.com/mgMibBrowserPE-evaluate.html.

Requisitos de Instalação e Funcionamento

O sistema operacional utilizado é o *Microsoft® Windows®* (*Windows®* 95, 98, *ME*, *NT*, 2000 ou *XP*). Também é disponível uma versão para o sistema operacional *Linux*.

Características Básicas

O *MG-SOFT MIB Browser* com o compilador de *MIB* é extremamente flexível, muito bom tecnicamente e apresenta uma interface bastante amigável. Todas essas características tornam o *MG-SOFT MIB Browser* uma ferramenta

interessante para a coleta de dados e análise. A seguir são apresentadas algumas de suas características:

- Permite a realização das operações *SNMP*: *get*, *get-Next*, *get-Bulk* e *set*. Além destas operações, existe a possibilidade de captura das mensagens de notificação (*traps*) e *inform*;
- Tem a possibilidade de configurar o tempo de *polling*;
- Pode carregar qualquer arquivo de *MIB* privada, desde que sejam compiladas com o compilador de *MIB MG-SOFT*;
- Apresenta gráficos de desempenho para o monitoramento de agentes *SNMP* através do seu endereço *IP*;
- Habilita e desabilita interfaces com o uso do comando *set*.

A Figura A.5 ilustra algumas características citadas anteriormente, como a possibilidade de seleção do tempo de *polling*, os objetos referentes a *MIB-II* e o protocolo *SNMPv.3* para três tipos de interface.

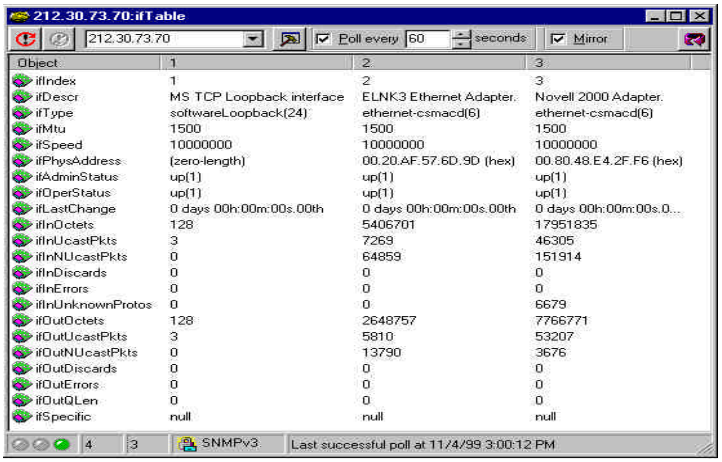


Figura A.5 – *Visão de uma Tabela SNMP na Forma de Colunas – MG-SOFT*

Utilização da Rede

A utilização da rede será baseada na carga gerada pelo software na rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

A.9 – Softwares Utilizados na Coleta de dados, embora não sejam baseados no *SNMP*

A.9.1 - *Nagios*[â]

Obtenção do Produto

O *Nagios*â (antigo *Netsaint*) é um sistema de monitoramento de redes e serviços criado para o ambiente *Linux*. É disponibilizado de forma gratuita, podendo ser encontrado para *download* na página http://www.nagios.org/.

Requisitos de Instalação e Funcionamento

Por se tratar de um software construído para o ambiente *Linux*, torna-se necessário a sua instalação em máquinas que estejam executando *Linux* ou alguma variante do *Unix*â. Um compilador C também é necessário, além de ter o *TCP/IP* configurado, já que a maioria das verificações será feita sobre a rede.

Para o sucesso em sua instalação é necessário um bom conhecimento das variáveis do ambiente *Linux* e não se deve assustar com uma demora inicial para o entendimento de seu funcionamento.

Características Básicas

Algumas características principais são apresentadas a seguir:

- Realiza o monitoramento dos serviços da rede (*SMTP*, *POP3*, *HTTP*, *NNTP*, *PING*, etc.) e dos recursos das máquinas (carga no processador, utilização do disco, etc.).
- Possibilita ao usuário desenvolver serviços de verificação e também checar os serviços paralisados.
- Capacidade de definir a hierarquia da rede baseado nas máquinas, permitindo a detecção e distinção entre máquinas que estão desligadas e que não são alcançáveis.
- Tem a identificação das notificações (*traps*) geradas de acordo com problemas ocorridos nas máquinas ou serviços (via *e-mail*, *pager* ou algum método definido pelo usuário).
- Capacidade de definir o tratamento dos eventos em tempo real para soluções pró-ativas.
- Tem uma interface *Web* opcional para observação do *status* atual da rede, notificação, arquivo do histórico de problemas, arquivo de registros, etc.

A Figura A.6 ilustra uma interface amigável ao administrador da rede, mostrando o *status* de uma determinada estação. Também há um arquivo de registro destes dados e outras informações apresentadas na tela do administrador da rede,

como o gráfico de alerta, que mostra, por exemplo, o número de eventos no período de um dia, comparando-o com limiares de advertência e crítico.

State	Time	% Total Time	% Known Time
UP	7d 23h 26m 29s	53.18%	100.00%
DOWN	0d 0h 0m 0s	0.00%	0.00%
UNREACHABLE	0d 0h 0m 0s	0.00%	0.00%
Undetermined	7d 0h 33m 31s	46.82%	
All	15d 0h 0m 0s	100.0%	100.0%

Figura A.6 - *O Status e a Disponibilidade de uma Estação - Nagios*â

Utilização da Rede

Como este software só captura os dados, não há geração de carga na rede.

A.9.2 – *Sniffer*â *Wireless*

O *Sniffer*â *Wireless* fornece uma solução que engloba o controle de aplicações e a implantação das redes locais sem fio 802.11a e 802.11b. Este software inclui o monitoramento da rede, captura, decodificação e filtragem dos quadros transmitidos e recebidos por dispositivos. É uma ferramenta de gerenciamento capaz de reconhecer zonas de riscos para segurança em tempo real, identificar eficientemente problemas da rede e reduzir os custos operacionais da rede.

Obtenção do Produto

Trata-se de uma ferramenta paga produzida pela *Sniffer*â *Technologies*. Maiores informações sobre a aquisição deste produto podem ser obtidas no endereço eletrônico https://secure.nai.com/us/forms/registration/survey.asp?code=nw404.

Requisitos de Instalação e Funcionamento

A sua instalação requer uma estação com *Microsoft*â *Windows*â 98 *SE*, *NT* 4.0, 2000, ou *XP* e um *slot PCMCIA* disponível para redes sem fio.

Características Básicas

Atualmente o *Sniffer*â *Wireless* atua com o fabricante *Proxim Harmony Cardbus* para o suporte ao IEEE 802.11a e para o suporte ao IEEE 802.11b inclui os seguintes fabricantes:

- *Symbol*â *Technologies Spectrum24*â *Model* 4121
- *Cisco Systems Aironet*â 340/350
- *Agere Systems ORiNOCO*â
- *Enterasys RoamAbout*â

O *Sniffer® Wireless* é uma ferramenta de gerência que possui as seguintes características básicas:

- Fornece uma visão geral do tráfego e das máquinas em qualquer um dos possíveis canais;
- Pode descriptografar e decodificar pacotes *WEP*;
- Mostra estatística de todos os dados monitorados 802.11a e 802.11b, além do número de pacotes enviados e em qual velocidade (1, 2, 5,5 ou 11 Mbps) permitindo um monitoramento do desempenho da rede;
- Realiza uma análise automática de problemas e localização, verificando a sua causa;
- Identifica pontos de acesso e estações que não estão autorizadas.

A Figura A.7 ilustra uma arquitetura possível de rede sem fio utilizando o *Sniffer® Wireless* com tecnologias compatíveis de outros fabricantes.

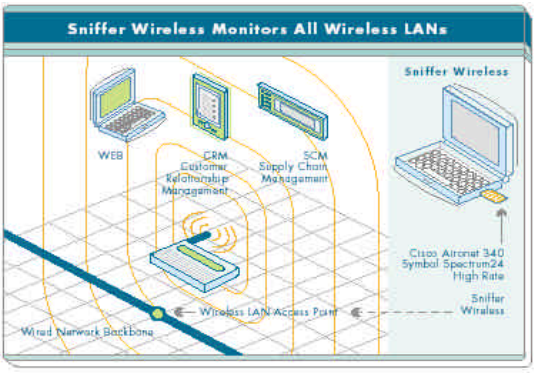


Figura A.7 – *Uma Possível Atuação para o Sniffer® Wireless*

Utilização da Rede

Em se tratando de um *Sniffer* não existe a utilização de recursos da rede monitorada.

A.10 – Considerações sobre os Softwares Analisados

Os sete primeiros softwares estudados anteriormente utilizam o protocolo *SNMP*, sendo assim, a utilização da rede será baseada na carga gerada com a utilização destes softwares. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *polling* (requisições do gerente).

Vale ressaltar que o elemento de maior importância em uma rede sem fio que dispõe de uma infra-estrutura é o Ponto de Acesso (*AP*), pois é por onde passam todas as informações de acesso à rede cabeada e à Internet. Sendo assim, torna-se o dispositivo de maior importância para o gerenciamento e configuração de uma rede sem fio.

Como conclusão sobre a análise realizada sobre os softwares de gerência de redes sem fio (*SpectrumSoft® WNMS*, *WNM* e da *Corinex® Global*), tem-se que as fases de coleta, análise e o tratamento dos dados são realizadas internamente de forma a gerar gráficos ou alarmes para o administrador da rede. Isto possibilita a intervenção na rede através da configuração que mais se adapte a sua nova situação. Um exemplo seria a limitação do número de estações associadas simultaneamente ao *AP*. Além disso, estes três softwares são voltados para a configuração dos pontos de acesso e o monitoramento das estatísticas específicas para as redes sem fio, inclusive da qualidade do sinal que está sendo transmitido e recebido.

Entretanto, foram estudados também os softwares *MRTG©* e *Net - SNMP* que são encontrados de forma gratuita, ao contrário dos outros três citados anteriormente. Estes dois softwares na verdade são bastante diferentes dos anteriores, já que não são específicos para redes sem fio. Além disso, a utilização destes softwares não é proprietária, ou seja, podem ser empregados no monitoramento do tráfego em redes sem fio independentemente dos fabricantes dos dispositivos envolvidos.

O *MRTG©* e o *LoriotPro©* se assemelham por utilizarem o protocolo *SNMP*, geração de relatórios em *html* e possibilitar o acesso via *Web* de forma que a rede possa ser monitorada de qualquer localização. No entanto, os recursos disponíveis pelo *LoriotPro©* são mais completos e possui uma interface mais amigável para o usuário.

Os softwares *Net – SNMP* e o *MG-SOFT MIB Browser* já foram utilizados para a coleta de dados em redes sem fio em alguns artigos [43] [50] [51]. São softwares que possibilitam a coleta utilizando várias versões do protocolo *SNMP*. O *MG-SOFT MIB Browser* oferece uma interface bastante amigável para efetuar tanto a investigação nas *MIBs* do agente, coleta dos dados e ajustes do tempo de *polling*.

Tanto o *Nagios©*, como o *Sniffer© Wireless* são capazes de monitorar o tráfego da rede sem a utilização do protocolo *SNMP*. Mostram-se interessantes por

conseguirem coletar os dados sem a geração de carga adicional ao sistema. São softwares que podem auxiliar na gerência de redes que emprega por exemplo, o software *SpectrumSoft*ä *WNMS, WNM* ou o da *Corinex*ä *Global* que são voltados às redes sem fio.

Entre todos os softwares apresentados, diversas outras possibilidades podem ser analisadas e empregadas em redes sem fio. Algumas outras opções de ferramentas comerciais podem ser encontradas na Internet, tais como:

O *MIB Explorer*â, que é da mesma linha do *MG-SOFT MIB Browser*.

O *NetworkView*â, que pode realizar a descoberta dos dispositivos, monitorar o *status* dos dispositivos, navegar na *MIB-II* ou qualquer outra *MIB* proprietária, etc.

Outras ferramentas *free* também podem ser encontradas na Internet, tais como:

GxSNMP utilizado para a coleta de dados *SNMP*, navegar na *MIB*, descobrir automaticamente a rede, etc.

JFFNMS (*Just For Fun Network Management System*) traz informações como a utilização da interface (%), taxa de pacotes por segundo, erros por segundo, perdas de pacotes, utilização de memória e disco, etc. Dá suporte em especial as *MIBs* da Cisco.

Como o objetivo é buscar uma ferramenta que possibilite a realização da coleta dos dados proposta no Capítulo 4 desta dissertação e se possível apresente medidas estatísticas sobre esses dados de forma amigável ao administrador da rede, tornou-se interessante as possíveis coletas realizadas pelo *MRTG*â e *MG - SOFT MIB Browser*. No entanto, nada impede a utilização de outras ferramentas, ou mesmo a elaboração de uma nova ferramenta capaz de facilitar a realização das quatro fases propostas pela metodologia. Com a utilização do *MRTG*â para o planejamento de capacidade da rede já existe um arquivo texto da coleta dos dados que pode ser importado pelo simulador *OPNET*â *Modeler*. Desta forma, consegue-se obter uma precisão maior na simulação a respeito do tráfego e realizar o planejamento de capacidade mais preciso. Além desta vantagem, as coletas feitas sobre o tráfego da rede não necessitariam do tratamento estatístico a fim de encontrar distribuições de probabilidade conhecidas para a simulação, pois seriam importadas como se estivessem sendo coletadas pelo próprio *OPNET*â *Modeler*.

Vale ressaltar que a ferramenta utilizada para a coleta dos dados independe tanto da tecnologia utilizada pelo meio de transmissão, como do próprio meio. Será importante que tanto as *MIBs* disponíveis, como os agentes ativos estejam adequados ao protocolo *SNMP* nos dispositivos em análise. Por exemplo, para o caso do software *MRTG*[â], deve-se saber se o agente suporta o protocolo *SNMP* e conhecer entre outros detalhes, o endereço *IP* do dispositivo para configurar adequadamente a coleta.

Deve ficar claro que para os pacotes capturados por softwares não específicos às redes IEEE 802.11 não se consegue entender o seu conteúdo, já que normalmente são criptografados. No entanto, não é importante o conteúdo dos pacotes na análise de desempenho, mas sim o número de pacotes que passam por uma interface, pacotes descartados, pacotes com erro, o *status* do dispositivo, a taxa de transmissão utilizada, etc.

Não existe a intenção de esgotar a possibilidade de utilização de softwares baseados na coleta *SNMP*, já que isto seria impossível. Todas estas ferramentas foram pesquisadas na Internet e não pode ser descartada a hipótese de haver diversas outras ferramentas *free* ou mesmo pagas que possam estar sendo utilizadas para a coleta de dados através do protocolo *SNMP* em redes sem fio de forma até mais eficiente. Sendo assim, caberá ao administrador da rede utilizar uma ferramenta que colete os dados de seu interesse e de preferência realize o tratamento matemático adequado, fornecendo uma interface amigável. Nem sempre o administrador da rede poderá utilizar a melhor ferramenta, já que muitas são comerciais. Contudo, torna-se necessário que as ferramentas disponíveis sejam bem analisadas, pois grande parte das ferramentas *free* realizam as mesmas funções das comerciais, possuindo algumas limitações, mas atendendo perfeitamente as necessidades de gerência de tal rede. É importante ressaltar que nada impede a estação gerente de utilizar um software *free* que colete e gere relatórios via *Web* e outro comercial mais específico aos equipamentos utilizados, assim, haverá a possibilidade da tomada de decisão por parte do administrador da rede baseada em um número maior de informações.

Anexo B – Alguns Parâmetros e Estatísticas Coletadas para Rede IEEE 802.11 na Simulação

B.1 - Introdução

A finalidade deste anexo é explicar quais os parâmetros foram utilizados na simulação, esclarecer o significado das estatísticas coletadas e mostrar as janelas de configuração utilizadas. Vale ressaltar que para a obtenção da confiabilidade estatística dos gráficos gerados pelo *OPNET$^{\hat{a}}$ Modeler* deve ser obtido um tempo de observação suficiente para a realização da simulação. Por exemplo, verifica-se que em alguns gráficos gerados nas simulações com apenas duas estações, que a convergência em torno de um valor médio era alcançada com o tempo de uma hora de observação. Já com o aumento da complexidade da simulação, torna-se necessário utilizar um tempo maior para a simulação. Além disso, para que a simulação ocorra normalmente, é necessário que o usuário esteja atento a configuração da sua estação de trabalho para opção Inglês (Estados Unidos).

O pico inicial apresentado em alguns gráficos é explicado pelo fato das estações terem um início da geração de pacotes segundo um valor constante em 5 segundos de simulação e principalmente ao tempo de observação utilizado (tempo de simulação). Para estas simulações isto não foi importante, já que o interesse está na comparação entre os resultados de situações distintas. Vale ressaltar que o *OPNET$^{\hat{a}}$ Modeler* fornece vários tipos de filtros para visualização de seus gráficos, no entanto, foi utilizado o *time_average*, que apresenta para uma janela de amostragem de tamanho fixado pelo simulador, os valores médio ao longo do tempo de observação.

B.2 - Alguns Valores Utilizados nas Simulações

Agora serão apresentados alguns valores de parâmetros que foram utilizados nas simulações. As figuras B.1 e B.2 ilustram a forma como o simulador apresenta estes valores para uma estação sem fio.

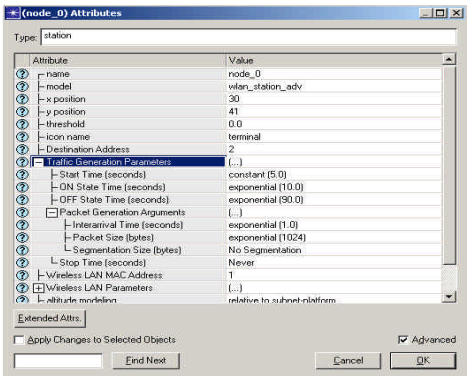


Figura B.1 - *Configurando os Atributos da Estação da Rede IEEE 802.11*

Através da Figura B.1 observa-se os seguintes parâmetros utilizados para a geração de tráfego:

- ***Start Time* (s)** - indica que o início da geração de pacotes irá seguir uma distribuição constante em 5.
- ***ON State Time* (s)** – indica que o tempo no qual os pacotes serão gerados seguem uma distribuição exponencial de média 10.
- ***OFF State Time* (s)** – indica que o tempo no qual os pacotes não serão gerados seguem uma distribuição exponencial de média 90.

Ainda com relação a geração de tráfego, existem três argumentos:

- ***Interarrival Time* (s)** – indica que o tempo entre os sucessivos pacotes gerados no *ON State Time* segue uma distribuição exponencial de média 1.
- ***Packet Size* (bytes)** – indica que o tamanho dos pacotes gerados segue uma distribuição exponencial de média 1024.
- ***Segmentation Size* (bytes)** – indica o tamanho do pacote transmitido, caso seja necessário segmentar o pacote gerado.

Agora são apresentados na Figura B.2 os parâmetros padrões do *OPNET*$^{\hat{a}}$ *Modeler* específicos para estações de redes sem fio IEEE 802.11.

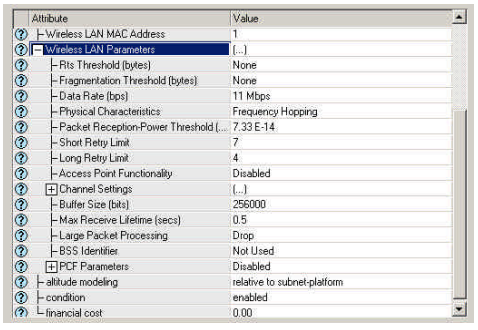


Figura B.2 - *Configurando os Atributos da Estação da Rede IEEE 802.11*

Um endereço de origem e um de destino pode ser atribuído para a estação (1 e 2) ou ainda deixar que o simulador o atribua aleatoriamente.

Os parâmetros apresentados anteriormente nas Figuras B.1 e B.2 foram os padrões do *OPNET^{â} Modeler*, neste momento, serão apresentados o significado dos parâmetros que foram configurados nas várias simulações realizadas.

- ***RTS Threshold* (bytes)** – indica o limiar para se utilizar o envio de quadros *RTS* e *CTS* para a reserva do meio de transmissão. Se atribuído *none*, não haverá reserva do meio.
- ***Fragmentation Threshold* (bytes)** – indica o limiar para a fragmentação de pacotes. Se atribuído *none*, não haverá fragmentação.
- ***Date Rate* (bps)** – indica a taxa de transmissão utilizada pela estação.
- ***Physical Characterístics*** – determina a tecnologia de camada física utilizada.
- ***Access Point Funcionality*** – permite a estação atuar como um coordenador de ponto (*AP*).
- ***PCF Parameters*** – quando ativado, indica que a estação está no modo de operação *PCF*, em caso contrário, a estação se encontra no modo de operação *DCF*.

A descrição das estatísticas disponibilizadas pelo *OPNET^{â} Modeler* para as estações de uma rede sem fio são apresentadas a seguir:

- ***Delay*** – atraso fim-a-fim de todos os pacotes recebidos por um nó da rede sem fio e enviado para as camadas acima.
- ***Load*** – é o número total de bits recebidos das camadas mais altas. Estes pacotes que chegam das camadas mais altas são armazenados em *buffer*, formando uma fila.
- ***Media Access Delay*** – é o tempo total gasto pelo pacote para ter acesso ao meio de transmissão.
- ***Throughput*** – é o número total de bits enviado para camada acima da *MAC*. Isto significa que só os bits endereçados a esta estação e contendo dados serão registrados.
- ***Channel Reservation*** – indica o tempo gasto com a reserva de meio utilizando o contador *NAV* (*Network Allocation Vector*) pela estação, é claro que se torna necessário que o limiar de *RTS* esteja ativado.

- ***Control Traffic Sent*** – indica quantos bits de quadros de controle (*ACK*, *RTS* e *CTS*) foram enviados em um segundo.
- ***Dropped Data Packets*** – indica o descarte de pacotes (bits/s) devido a sobrecarga (*overflow*) do *buffer* da camada mais alta, ou seja, a impossibilidade de transmissão após aguardar um certo tempo e o meio ainda continuar ocupado.

B.3 - Alguns Valores Utilizados no Estudo de Caso

Para a realização do estudo de caso, não foi utilizada uma aplicação genérica de tráfego para o usuário. Escolheram-se as aplicações *FTP* e *HTTP*, como apresentado na Figura B.3, que ilustra os atributos de uma estação utilizando a aplicação *FTP*.

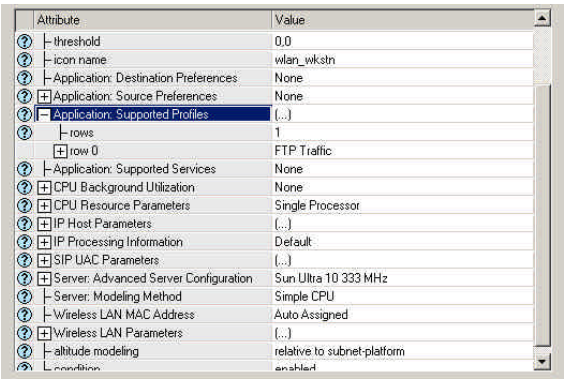


Figura B.3 – *Atributos de uma Estação Suportando FTP*

Na Figura B.4 são ilustradas as duas caixas de diálogo responsáveis pela configuração da aplicação e do perfil do usuário.

Figura B.4 – *Caixas de Diálogo de Configuração*

Com a definição da aplicação e do tipo de tráfego gerado pelas estações é criado um usuário. Ele pode usar estas aplicações com muita ou pouca freqüência, formando o seu perfil.

Uma aplicação como *FTP* do *OPNET^{â} Modeler* pode ser modelada estatisticamente com várias funções de distribuição fornecidas ou mesmo criadas.

A Figura B.5 traz várias linhas de aplicações que podem ser utilizadas para formar o perfil do usuário.

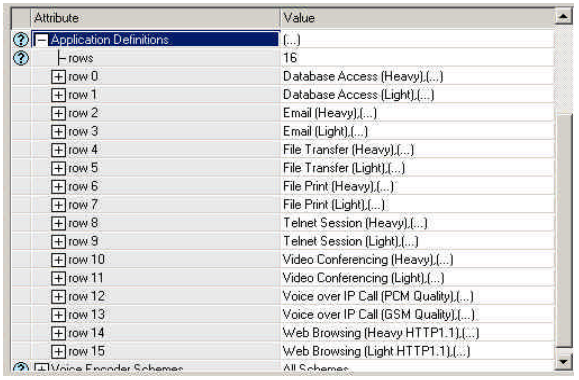


Figura B.5 - *Configuração da Aplicação*

A Figura B.6 ilustra os parâmetros de configuração para o perfil do usuário da rede sem fio, mostrando as aplicações que são suportadas de acordo com a definição feita na configuração da aplicação.

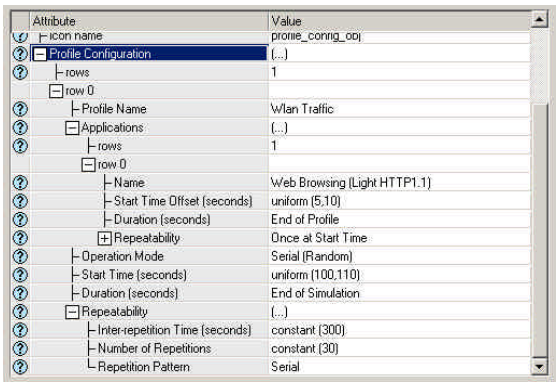


Figura B.6 - *Configuração do Perfil do Usuário*

A Figura B.7 mostra os atributos (*default*) que podem ser empregados para modelar um tráfego gerado, por exemplo, utilizando requisições a um banco de dados.

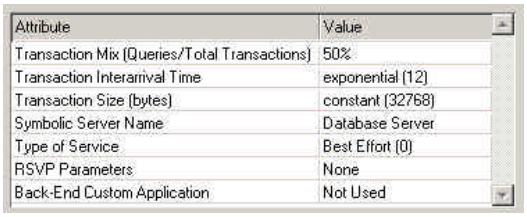


Figura B.7 - *Modelando uma Aplicação*

B.4 - Estações para Redes IEEE 802.11 mais Comuns

As figuras B.8 e B.9 mostram as duas arquiteturas normalmente utilizadas para as redes sem fio.

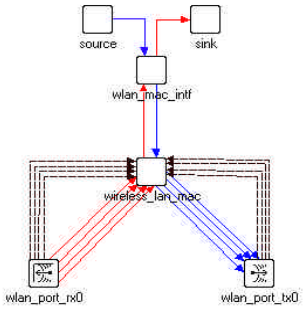


Figura B.8 - *Modelo de Estação para Redes IEEE 802.11 sem as Camadas Superiores*

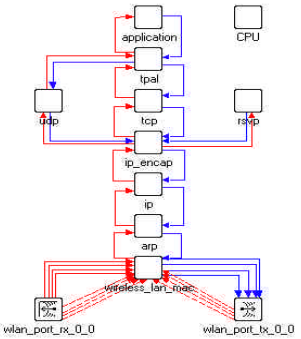


Figura B.9 - *Modelo de Estação para Redes IEEE 802.11 com as Camadas Superiores*

O emprego das estações sem as camadas mais altas (*TCP/IP* e aplicações) utiliza o modelo de nós sem fio com fonte (*source*) e sorvedouro (*sink*) para substituição das camadas mais altas. Alguns benefícios deste modelo são apresentados a seguir:

- Simular os efeitos dos parâmetros das redes sem fio de forma independente para as camadas mais altas;
- Obtém um tempo de simulação menor para redes complexas.

Ainda existe no *OPNET*$^{\hat{a}}$ *Modeler*, a possibilidade das estações sem fio serem configuradas como móveis, portáteis ou estacionárias.

Espera-se com a análise deste anexo que o leitor consiga adquirir um pouco de conhecimento sobre algumas possibilidades de configuração do *OPNET*$^{\hat{a}}$ *Modeler* para redes IEEE 802.11. Informações sobre cada campo da janela de configuração podem ser encontradas no ícone apresentado ao lado de cada atributo.

B.5 – Uma Breve Comparação entre o *OPNET*$^{\hat{a}}$ *Modeler* e o *NS-2*

Conforme mencionado no Capítulo 3 desta dissertação, o usuário do *Network Simulator* deve ter um bom conhecimento sobre a linguagem de programação *OTcl*,

além de conhecer bem o sistema de bibliotecas do ambiente *Linux*. Para ilustrar essa dificuldade, é apresentado a seguir um *script* para a simulação básica de duas estações sem fio com a explicação de cada etapa.

```
# ============================================================
#   Definição dos Parâmetros
# ============================================================
set val(chan)           Channel/WirelessChannel;    # Tipo de canal
set val(prop)           Propagation/TwoRayGround;   # Modelo de propagação
set val(netif)          Phy/WirelessPhy;            # Tipo de interface
set val(mac)            Mac/802_11;                 # Tipo de camada MAC
set val(ifq)            Queue/DropTail/PriQueue;    # Tipo de fila na interface
set val(ll)             LL;                         # Tipo de camada de enlace
set val(ant)            Antenna/OmniAntenna;        # Modelo da antena
set val(ifqlen)         50;                         # Tamanho do buffer
set val(nn)             2;                          # Número de estações
set val(rp)             DSDV;                       # Protocolo de roteamento
# ============================================================
#   Programa Principal
# ============================================================
# Inicializa as variáveis globais, criando os arquivos de registro (log)
set ns_         [new Simulator]
set tracefd     [open simple.tr w]
$ns_ trace-all $tracefd
set namtrace    [open simple.nam w]
$ns_ namtrace-all-wireless $namtrace 500 500
# Ajusta os limites da topologia da rede
set topo        [new Topography]
$topo load_flatgrid 500 500
# Cria as posições das estações
set god_ [create-god 2]
ns_ at 899.00 "$god_ setdist 2 3 1"
create-god $val(nn)
```

```
# Configuração das estações no nível de camada MAC
        $ns_ node-config -adhocRouting $val(rp) \
                                -llType $val(ll) \
                                -macType $val(mac) \
                                -ifqType $val(ifq) \
                                -ifqLen $val(ifqlen) \
                                -antType $val(ant) \
                                -propType $val(prop) \
                                -phyType $val(netif) \
                                -topoInstance $topo \
                                -channelType $val(chan) \
                                -agentTrace ON \
                                -routerTrace ON \
                                -macTrace OFF \
                                -movementTrace OFF
# Cria o número de estações
set node [$ns_ node]
          for {set i 0} {$i < $val(nn) } {incr i} {
                    set node_($i) [$ns_ node]
                    $node_($i) random-motion 0 ; # Estações sem mobilidade
          }
# Fornece as coordenadas iniciais (X,Y, para Z=0) para cada estação
$node_(0) set X_ 5.0
$node_(0) set Y_ 2.0
$node_(0) set Z_ 0.0
$node_(1) set X_ 390.0
$node_(1) set Y_ 385.0
$node_(1) set Z_ 0.0
# Produção de alguns movimentos simples
# Estação 1 inicia o movimento em direção a estação 2
$ns_ at 50.0 "$node_(1) setdest 25.0 20.0 15.0"
$ns_ at 10.0 "$node_(0) setdest 20.0 18.0 1.0"
```

```
# Estação 2 começa a afastar-se da Estação 1
$ns_ at 100.0 "$node_(1) setdest 490.0 480.0 15.0"
# Ajusta o fluxo de pacotes entre as estações
set tcp [new Agent/TCP]
$tcp set class_ 2
set sink [new Agent/TCPSink]
# Cria as conexões TCP entre as estações.
$ns_ attach-agent $node_(0) $tcp
$ns_ attach-agent $node_(1) $sink
$ns_ connect $tcp $sink
# Cria a aplicação que vai utilizar a conexão TCP
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns_ at 10.0 "$ftp start" # Tempo onde se inicia a geração de tráfego FTP
# Indica o tempo final da simulação.
for {set i 0} {$i < $val(nn) } {incr i} {
   $ns_ at 150.0 "$node_($i) reset";
}
$ns_ at 150.0 "stop"
$ns_ at 150.01 "puts \"Saindo do NS...\" ; $ns_ halt"
proc stop {} {
   global ns_ tracefd
   $ns_ flush-trace
   close $tracefd
}
puts "Iniciando a simulação..."
$ns_ run
```

Comparando com o *OPNET*^{â} *Modeler*, observa-se que utilizando um bloco (ícone) é possível configurar facilmente todos os parâmetros da rede IEEE 802.11 sem o conhecimento de nenhuma linguagem de programação, já no *NS-2* deverá existir uma amplo conhecimento desta linguagem. Outra grande dificuldade encontrada é a interpretação dos resultados fornecidos pelo *NS-2*.