

**Uma Estratégia Para Implementação de
Gerenciamento de Redes – Estudo de Caso
do Tribunal de Contas da União**

**Universidade Federal de Santa Catarina
Programa de Pós Graduação em Engenharia de Produção**

**Uma Estratégia Para Implementação de
Gerenciamento de Redes – Estudo de Caso do Tribunal
de Contas da União**

Geraldo Magela Lopes de Freitas

Dissertação apresentada ao
Programa de Pós-Graduação em
Engenharia de Produção da
Universidade Federal de Santa Catarina
como requisito parcial para obtenção
do título de Mestre em
Engenharia da Produção

**Florianópolis
2001**

Geraldo Magela Lopes de Freitas

**Uma Estratégia Para Implementação de
Gerenciamento de Redes – Estudo de Caso do Tribunal
de Contas da União**

**Esta dissertação foi julgada adequada e aprovada para
obtenção do título de Mestre em Engenharia de
Produção no Programa de Pós-Graduação em
Engenharia de Produção da Universidade Federal de
Santa Catarina**

Florianópolis, 29 de junho de 2001.



**Prof. Ricardo Miranda Barcia, Ph. D.
Coordenador do Curso**

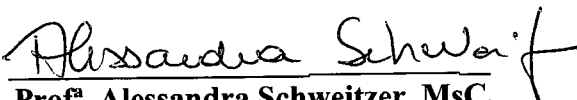
BANCA EXAMINADORA


Prof.ª Elizabeth Sueli Specialski, Dr.ª.

Orientadora


Prof. Alexandre Moraes Ramos, Dr.


Prof. Vitorio Bruno Mazzola, Dr.


Prof.ª Alessandra Schweitzer, MsC.

À minha família, especialmente a meus pais
que sempre me deram todo o apoio possível,
mesmo que isto significasse longos períodos longe deles.

À minha filha, que espero que possa acompanhar
mais de perto novas empreitadas
e que também sofreu bastante
com meu distanciamento.

Agradecimentos

À todas as pessoas que contribuíram para a realização deste trabalho. Principalmente, à prof^a. Elizabeth Sueli Specialski pela valiosa orientação dada. Um agradecimento também deve ser dado à prof^a. Alessandra Schweitzer pelas dicas de quem havia passado recentemente pelas mesmas experiências.

À Universidade Federal de Santa Catarina pela oportunidade dada aos estudantes remotos e ao excelente trabalho e busca de melhoria constante do pessoal do Laboratório de Ensino à Distância.

Aos colegas do Tribunal de Contas da União, especialmente ao apoio dado pela equipe do Serviço de Suporte Técnico e ao meu estagiário e amigo David Cordeiro Jr., que me auxiliou na instalação de monitores e no levantamento de variáveis.

Aos colegas de mestrado, por termos compartilhado muitas vitórias e muito aprendizado durante o curso, mas também muitas angústias e algum sofrimento.

SUMÁRIO

CAPÍTULO I – INTRODUÇÃO	1
1.1 Motivação.....	2
1.2 Organização do Trabalho	3
CAPÍTULO II – GERÊNCIA DE REDES	5
2.1 Introdução.....	5
2.2 Modelo OSI de Gerência de Redes	7
2.2.1 Gerenciamento de Configuração	8
2.2.2 Gerenciamento de Falhas	8
2.2.3 Gerenciamento de Desempenho.....	9
2.2.4 Gerenciamento de Contabilização.....	10
2.2.5 Gerenciamento de Segurança.....	10
2.3 A Gerência Internet	11
2.3.1 O SNMPv1	12
2.3.2 O RMON.....	19
2.3.3 O RMON2.....	25
2.3.4 O SNMPv2	28
2.3.5 O SNMPv3	34
2.3.6 O SMON	39
2.4 TMN – Telecommunications Management Network.....	40
CAPÍTULO III – SISTEMAS E INFORMAÇÕES DE GERENCIAMENTO	45
3.1 Ferramentas e Sistemas de Gerenciamento	45
3.2 Público Alvo das Informações de Gerenciamento	49
3.3 Estabelecimento de <i>Baseline</i>	51
3.4 Acordo de Nível de Serviço - SLA	53
3.5 Gerenciamento de Performance	55
3.6 Controle Operacional de Redes – NOC	60
CAPÍTULO IV – ESTRATÉGIA PROPOSTA PARA IMPLEMENTAÇÃO DO GERENCIAMENTO	63
4.1 Apresentação da Estratégia	63
4.2 Opções de implementação.....	67
4.3 Efetividade do Gerenciamento	69
4.4 Ambiente Para Validação da Estratégia Proposta	70
4.4.1 A Instituição TCU.....	70
4.4.2 O Histórico da Rede de Computadores do TCU	73
4.4.3 O Problema do Gerenciamento	78
CAPÍTULO V – IMPLEMENTAÇÃO DO GERENCIAMENTO	80
5.1 Fase 1 – Estudo da Rede Existente.....	80
5.1.1 Rede LAN do TCU	81
5.1.2 Rede WAN do TCU	82
5.1.3 Equipamentos de Rede.....	85
5.2 Fase 2 – Identificação dos Problemas e Requisitos de Gerenciamento	87
5.3 Fase 3 – Estabelecimento de Prioridades	88
5.4 Fase 4 – Análise das Informações de Gerenciamento Disponíveis.....	89

5.4.1	MIB Privada Cisco	92
5.4.2	MIB Privada Lannet	93
5.5	Fase 5 – Estabelecimento de Monitoração e Limiares	95
5.5.1	Taxa de Utilização	95
5.5.2	Taxa de Erros	99
5.5.3	Congestionamento	106
5.5.4	Responsividade dos <i>links</i>	108
5.5.5	Disponibilidade	109
5.5.6	Estabelecimento de <i>Baseline</i>	109
5.6	Fase 6 – Especificação Funcional das Ferramentas	111
5.7	Fase 7 – Implementação e Integração	112
5.7.1	Configuração do MRTG	113
5.7.2	Configuração de alarmes RMON nos equipamentos	115
5.7.3	Análise de tráfego	115
5.7.4	Análise da banda consumida no processo de gerenciamento	121
5.8	Fase 8 – Revisão dos Resultados	123
CAPÍTULO VI – CONCLUSÕES		126
6.1	Considerações e Contribuições	126
6.2	Trabalhos Futuros	128
7.	BIBLIOGRAFIA	129
8.	ANEXO I – Variáveis Passíveis de Monitoração	136
9.	ANEXO II – Tamanho de Pacotes por Aplicação	141
10.	ANEXO III – Arquivos de Configuração do MRTG	145
11.	ANEXO IV – Saída do SnmpWalk	152
12.	ANEXO V – Configuração SNMP e RMON nos Equipamentos	157
13.	ANEXO VI – RFC's Relevantes	159

LISTA DE FIGURAS

Figura 2.1 – Modelo de Gerenciamento de Rede OSI.....	8
Figura 2.2 – Arquitetura de Gerenciamento de Rede SNMPv1	14
Figura 2.3 – Formato de Mensagens SNMPv1	15
Figura 2.4 – MIB II	19
Figura 2.5 – Rede com agentes RMON	21
Figura 2.6 – Grupos RMON1	24
Figura 2.7 – Classificação dos grupos RMON.....	25
Figura 2.8 – Grupos RMON2.....	27
Figura 2.9 – Visibilidade RMON1 x RMON2	28
Figura 2.10 – Arquitetura de gerenciamento de rede SNMPv2.....	31
Figura 2.11 – Formato de PDUs do SNMPv2.....	32
Figura 2.12 – Árvore do SNMPv2	33
Figura 2.13 – Entidade SNMPv3 (RFC 2571)	37
Figura 2.14 – Formato de mensagens SNMPv3.....	38
Figura 2.15 – Recomendações TMN.....	41
Figura 2.16 – Metodologia de especificação de interface TMN	44
Figura 3.1 – Arquitetura de um Sistema de Gerenciamento de Redes	47
Figura 3.2 – Evolução dos sistemas de gerenciamento de redes	49
Figura 3.3 – Principais medidas no estabelecimento de baseline de redes.....	52
Figura 3.4 – Valores de pico e média de utilização de circuitos de comunicação.....	56
Figura 3.5– Levantamento de taxa de transferência efetiva (EFT)	58
Figura 3.6 – Mecanismo de histeresse RMON.....	59
Figura 3.7 – Mecanismos de geração de alertas	61
Figura 4.1 – Estratégia proposta para implementação do gerenciamento	65
Figura 4.2 – Fase 1 da Rede de Comunicação de Dados.....	74
Figura 4.3 – Fase 2 da Rede de Comunicação de Dados.....	75
Figura 4.4 – Fase 3 da Rede de Comunicação de Dados.....	76
Figura 4.5 – Situação atual da Rede de Computadores do TCU	77
Figura 5.1 – Esquema de ligações da rede TCU	82
Figura 5.2 – Tráfego em circuito Frame Relay	84
Figura 5.3 – MIB privada Cisco.....	93
Figura 5.4 – MIB privada Lannet.....	94
Figura 5.5 – Vazão média dos circuitos Frame Relay.....	116
Figura 5.6 – Distribuição do tráfego WAN por protocolo	117
Figura 5.7 – Distribuição do tráfego WAN por servidor.....	118

Figura 5.8 – RTT dos circuitos Frame Relay no mês de abril/2001	119
Figura 5.9 – Média diária de RTT do circuito de São Paulo no mês de abril/2001.....	119
Figura 5.10 – Distribuição dos pacotes por tamanho	120

LISTA DE QUADROS

Quadro 2.1 – Operações Suportadas no SNMPv1.....	14
Quadro 3.1 – Relatórios de Gerenciamento de Redes por Público Alvo.....	50
Quadro 4.1 – Competências Constitucionais do TCU.....	70
Quadro 4.2 – Competências Legais do TCU.....	71
Quadro 4.3 – Negócio, Missão, Visão e Objetivos Institucionais do TCU.....	71
Quadro 5.1 – Configuração dos roteadores.....	86
Quadro 5.2 – Quantidade de gráficos para monitoração.....	122

LISTA DE ABREVIATURAS

ASN.1	Abstract Syntax Notation One
BB	Banco do Brasil
BECN	Backward Explicit Congestion Notification
CA	Computer Associates
CEF	Caixa Econômica Federal
CIR	Committed Information Rate
CMIP	Common Management Information Protocol
CMOT	CMIP Over TCP/IP
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCN	Data Communication Network
DLCI	Data Link Connection Identifier
DTE	Data Terminal Equipment
EFT	Effective File Throughput
FECN	Forward Explicit Congestion Notification
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
ISC	Instituto Serzedello Corrêa
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LPCD	Linha Privada de Comunicação de Dados
MAN	Metropolitan Area Network
MIB	Management Information Base
MIS	Management Information Service
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair

NE	Network Element
NMS	Network Management System
NOC	Network Operational Control
OAM&P	Operação, Administração, Manutenção e Provisionamento
OID	Object Identifier
OSI/NM	Open System Interconnection / Network Management
OSI/RM	Open System Interconnection / Reference Model
OSF	Operations System Function
PDU	Protocol Data Unit
PRODASEN	Centro de Processamento de Dados do Senado Federal
QoS	Quality of Service
RENPAAC	Rede Nacional de Pacotes
RFC	Request For Comments
RMON	Remote Monitoring
RTT	Round Trip Time
SEGECEX	Secretaria Geral de Controle Externo
SECEX	Secretaria de Controle Externo
SERPRO	Serviço Federal de Processamento de Dados
SGMP	Simple Gateway Management Protocol
SIAFI	Sistema Integrado de Administração Financeira
SLA	Service Level Agreement
SMI	Structure of Management Information
SMON	Switched Network Monitoring
SMP	Simple Management Protocol
SNMP	Simple Network Management Protocol
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Contas da União
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
TMN	Telecommunications Management Network
TTS	Trouble Ticket System
UDP	User Datagram Protocol

VLAN Virtual Local Area Network

WAN Wide Area Network

RESUMO

Este trabalho descreve a problemática com relação ao controle de redes de computadores, que vem sendo enfrentada em ambientes corporativos. Mostra-se a necessidade de implantação de sistemas automatizados para o gerenciamento das redes e discute-se as dificuldades encontradas na implantação de tais sistemas. É proposta uma estratégia para implantação de sistemas de gerenciamento considerando-se a questão de determinação de quais as informações disponibilizadas pelos sistemas de gerenciamento devem ser consideradas. Um estudo de caso ilustra a aplicação da estratégia proposta e mostra os resultados concretos que foram obtidos com sua aplicação.

ABSTRACT

This work describes the problem related to computer networks management, that has been faced in corporative environments. It shows the necessity of automated network management systems and discusses the difficulties faced to implement these systems. It's proposed a strategy of network management systems implementation, considering the question of determining witch of de management system information must be monitored. A Case Study tests the application of the proposed strategy and shows the results of this implementation.

CAPÍTULO I – INTRODUÇÃO

À medida que as organizações vão se tornando mais informatizadas e ocorre o crescimento das redes de computadores, mais dependentes seus funcionários ficam dos recursos computacionais para realização de suas tarefas de maneira integrada e cooperativa. Desta forma, as organizações se tornaram extremamente dependentes de seus ambientes de redes de computadores, tornando imprescindível a função de gerência de redes, no sentido de mantê-las funcionando com a qualidade requerida.

Normalmente, as organizações em um primeiro momento instalam e colocam as redes operacionais para posteriormente se preocuparem com o problema do gerenciamento. Este fato ocorre muitas vezes devido à escassez de tempo, restrições financeiras ou devido ao crescimento desordenado e acelerado da rede. Isto faz com que os gerentes de rede fiquem a maior parte do seu tempo tentando solucionar problemas que são reportados pelos usuários, em vez de estarem trabalhando com planejamento e antevendo o surgimento de problemas.

Considerando ainda que o crescimento das redes em termos de quantidade de computadores conectados, aumento do fluxo de informações trafegadas, surgimento de novos equipamentos, tecnologias, protocolos e velocidades suportando um conjunto de novos serviços, tem-se um quadro de sistemas cada vez mais complexos que necessitam de monitoramento contínuo, o que só pode ser feito de forma automatizada.

A simples adoção de sistemas de gerenciamento de rede não resolve todos os problemas, é necessário um conhecimento detalhado da estrutura da rede, incluindo, além de equipamentos, cabeamento e protocolos, os objetivos a serem alcançados,

perspectiva de crescimento, serviços disponibilizados e nível de serviço requerido. Além disso, faz-se necessário providenciar a integração de diversas ferramentas, uma vez que, normalmente, somente uma ferramenta não vai resolver todos os problemas.

O gerenciamento pode ajudar na administração, planejamento e expansão da rede, pois além do envio de alertas efetua também outros controles, tais como: armazenamento de dados históricos, crescimento do uso da rede, identificação de problemas mais freqüentes, indicando a necessidade de solução imediata e geração de dados para as mais diversas análises possíveis, inclusive utilizando inteligência artificial. (Sousa 1999, p.491)

Dois padrões, OSI e IETF, se destacam no cenário de gerenciamento de redes. Em decorrência do caráter mais pragmático da abordagem IETF e de haver mais equipamentos de rede implementando este padrão (SNMP, RMON e SMON), ele vai ser utilizado para implementação dos conceitos desenvolvidos neste trabalho. Visando delimitar o escopo deste trabalho, optou-se pela implementação do gerenciamento dos principais equipamentos ativos da rede e dos *links* de comunicação, restringindo às áreas funcionais de gerenciamento de desempenho e falhas. Vale ressaltar ainda que a implementação de gerenciamento em uma rede corporativa é um processo cíclico e contínuo, devendo ser reavaliado periodicamente.

1.1 Motivação

Em 1998 o TCU decidiu pelo *downsizing*, migrando todos os sistemas do *mainframe* para a rede de computadores. Atualmente, seus funcionários não podem prescindir dos serviços de rede, sejam eles para execução dos trabalhos diários, consulta

aos bancos de dados corporativos e de outros órgãos, acesso de informações na internet e trabalho colaborativo. Como descrito no item anterior, a rede foi toda colocada operacional sem a possibilidade de implementação efetiva de gerenciamento.

Se por um lado, eventuais problemas em seu funcionamento podem implicar em degradação inaceitável de desempenho, ou mesmo parada total ou parcial, por outro lado a rede de computadores tem apresentado enorme crescimento em termos de número de usuários e de serviços sem que haja o crescimento proporcional no efetivo do pessoal de suporte à rede.

A motivação deste trabalho é definir uma estratégia para implementação de gerenciamento de redes, associado à meta pessoal de elaborar um trabalho abrangente e útil de efetiva aplicação prática que contribuísse também para disseminar a cultura de gerência de redes, especialmente dentro do TCU, buscando satisfazer as expectativas dos usuários da rede de computadores e permitindo uma racionalização dos investimentos, principalmente relativos a *links* de comunicação.

1.2 Organização do Trabalho

O estudo para implementação de uma solução de gerência deve partir do conhecimento do referencial teórico relativo ao Gerenciamento OSI e Internet. Este referencial é apresentado no capítulo 2.

O capítulo 3 discute a problemática existente na implantação de gerenciamento, incluindo estabelecimento de *baseline* e de SLA e de disponibilização destas informações para os diferentes tipos de usuários.

O capítulo 4 apresenta uma proposta para guiar a implantação de sistemas de gerenciamento em redes que já estão operacionais e descreve o ambiente do TCU, onde a estratégia proposta foi aplicada. Além da apresentação da instituição TCU, é mostrado o histórico da rede de computadores e os problemas de gerenciamento atuais.

O capítulo 5 descreve a experiência de implementação da estratégia proposta, englobando todas as fases previstas no capítulo 4. São analisadas as informações disponíveis, definidos valores a serem monitorados e limiares para os mesmos e são analisadas as informações coletadas.

No capítulo 6 são apresentadas as conclusões, incluindo considerações sobre o trabalho desenvolvido e sugestões para trabalhos futuros, a seguir é apresentada a bibliografia consultada. Finalmente, foram incluídos anexos com informações consideradas relevantes para o entendimento do trabalho, são eles: OIDs consideradas relevantes, distribuição tamanho de pacotes por aplicação, arquivos de configuração do MRTG, saída gerada pelo snmpwalk, comandos para configuração SNMP e RMON nos equipamentos e RFCs relevantes ao gerenciamento de redes.

CAPÍTULO II – GERÊNCIA DE REDES

2.1 Introdução

À medida que as redes crescem, incorporando novos serviços e melhorando a comunicação e produtividade dentro das empresas os usuários se tornam mais dependentes de seus ambientes de redes, transformando-nas em recursos críticos para as organizações. Por este motivo a gerência efetiva de redes tem se tornado um elemento chave no sucesso das mesmas.

Em virtude da importância de seus serviços, as redes têm sido usualmente controladas por técnicos especialistas que possuem a responsabilidade de instalar, configurar, monitorar e resolver os seus problemas. Nesse sentido, segundo Subramanian (2000, p.40), o gerenciamento de redes pode ser definido como operação, administração, manutenção e provisionamento (OAM&P) de serviços de rede. O objetivo maior do gerenciamento de redes é garantir que os usuários tenham acesso aos serviços de que necessitam com a qualidade esperada. Melchior (1999) cita outros objetivos que também são almejados com o gerenciamento de redes, entre eles: garantir sua disponibilidade, reduzir os custos operacionais, aumentar a flexibilidade de operação e integração das redes, permitir facilidades de uso e garantir características de segurança.

O crescimento da complexidade e quantidade de equipamentos, protocolos e tecnologias que são empregados nas redes torna o trabalho de gerenciamento bastante complexo, exigindo amplo conhecimento por parte dos administradores de rede. Teixeira Jr. (1999, p.349) agrupa as funções de gerenciamento em duas categorias: o monitoramento da rede e o controle da rede. O monitoramento da rede está relacionado com a observação e análise do estado e do comportamento dos elementos da rede enquanto o controle da rede está relacionado com a modificação de parâmetros e configuração dos componentes.

As informações que devem ser avaliadas para o monitoramento da rede podem ser classificadas como estáticas – relativas à configuração, dinâmicas – relativas a eventos da rede e estatísticas – obtidas através de sumarização das informações dinâmicas. (Stallings 1999, p.24).

As informações úteis para o monitoramento da rede são coletadas e armazenadas por sistemas agentes e disponibilizadas para um ou mais sistemas gerentes. Duas técnicas são utilizadas para disponibilizar as informações dos agentes para os gerentes:

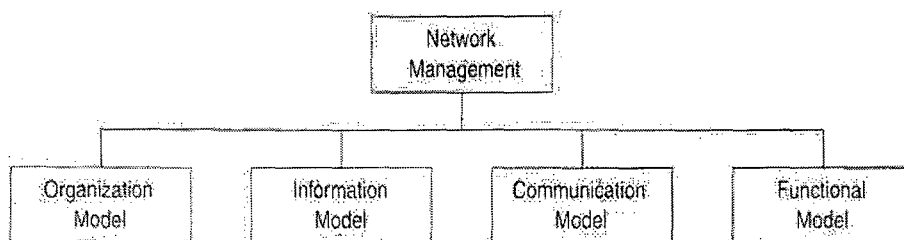
- ✓ *polling* – uma entidade gerente, desde que autorizada, solicita a uma entidade agente que ela envie alguma informação, também é conhecido como *request-response*;
- ✓ *event-reporting* – a iniciativa parte do agente e a entidade gerente age apenas como ouvinte, aguardando a chegada de informações. O agente pode gerar um event-report periodicamente para fornecer ao gerente o seu estado atual ou quando uma condição significativa ou anormal acontecer.

2.2 Modelo OSI de Gerência de Redes

A ISO (International Organization for Standardization) através do OSI/NM (Open Systems Interconnection / Network Management) propôs uma arquitetura de gerenciamento de redes composta de quatro modelos (Subramanian 2000, p.105):

- ✓ O Modelo Organizacional descreve os componentes de um sistema de gerenciamento, suas funções de infraestrutura. Ele foi definido na norma ISO 10040 – OSI Systems Management Overview, que define os termos objeto, agente e gerente.
- ✓ O Modelo Informacional trata da estrutura e organização da informação de gerenciamento. A norma ISO 10165 especifica a estrutura da informação de gerenciamento (SMI) a base de informações de gerenciamento (MIB).
- ✓ O Modelo de Comunicação que está associado à forma que as mensagens são trocadas entre sistemas.
- ✓ O Modelo Funcional que trata dos requisitos de gerência de rede voltados às aplicações e define funções do sistema de gerenciamento. A ISO define cinco áreas funcionais de aplicação: configuração, falhas, desempenho, contabilização e segurança. Esta classificação é adotada pela maioria dos fornecedores de sistemas de gerenciamento de redes.

Figura 2.1 – Modelo de Gerenciamento de Rede OSI



2.2.1 Gerenciamento de Configuração

Specialski (2000, p.4) diz que o gerenciamento de configuração está relacionado com a inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado com as tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e do estado dos componentes durante a operação da rede.

O gerenciamento de configuração normalmente é usado no contexto de descobrir a topologia da rede, mapear a rede, e definir parâmetros de configuração de agentes e gerentes. De uma forma mais geral, o provisionamento de recursos de rede, que inclui planejamento e projeto da rede estão englobados em gerenciamento de configuração. (Subramanian 2000, p.42-43)

2.2.2 Gerenciamento de Falhas

Um conceito central no gerenciamento de falhas é o conceito de falhas e a diferença entre falha e erro. Uma falha é uma condição anormal que requer uma ação para correção, enquanto erro é um evento simples. Uma falha usualmente indica problema de operação ou erros excessivos. (Stallings 1999, p.2)

Subramanian (2000, p.118) identifica cinco passos no processo de gerenciamento de falhas: detecção da falha, isolamento da falha, restauração do serviço, identificação das causas do problema e resolução do problema. Estes passos devem ser seguidos a fim de que a rede fique operacional o mais rápido possível, mesmo que a causa do problema ainda leve algum tempo para ser encontrada e solucionada.

Existem duas formas de efetuar gerenciamento de falhas: reativamente e proativamente. No gerenciamento reativo espera ocorrer o problema e então conserta-o. No gerenciamento pró-ativo tenta-se evitar que os problemas aconteçam ou que venham a afetar os usuários. O impacto e a duração do estado de falha pode ser minimizado pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um grau de “tolerância à falhas”.

2.2.3 Gerenciamento de Desempenho

Segundo Rocha (1996, p.31), a principal atividade da gerência de desempenho é auxiliar os técnicos e administradores de rede no planejamento da capacidade, de maneira a oferecer a seus usuários um nível satisfatório de serviços. Com o uso da gerência de desempenho, o gerente de rede pode monitorar a utilização dos dispositivos e enlaces, sendo possível isolar problemas de desempenho com a finalidade de resolvê-los antes que esses impliquem maior impacto.

A gerência de desempenho é composta pelos quatro seguintes passos: coleta de dados da utilização corrente dos dispositivos e enlaces, análise dos dados relevantes, estabelecimento de limiares e simulação da rede. O decremento do nível de serviços dos usuários é um indício significativo sobre a utilização dos dispositivos e enlaces da rede.

No que diz respeito à avaliação do nível de serviços, deve-se ter disponíveis os seguintes parâmetros: tempo de resposta; taxa de rejeição e disponibilidade.

2.2.4 Gerenciamento de Contabilização

O gerenciamento de contabilização permite a cobrança de utilização de recursos da rede, bem como determinar quem está usando o quê e acompanhar o crescimento da utilização dos recursos da rede, o que pode indicar a necessidade de aquisições de novos recursos ou rearranjo dos recursos existentes.

Segundo Stallings (1999, p.2), mesmo que não haja uma cobrança financeira, o gerenciamento de contabilização é importante, pois o gerente de rede precisa saber como estão sendo utilizados os recursos da rede por usuários ou classes de usuários, visando verificar se:

- ✓ um usuário ou grupo de usuários está abusando de seus privilégios de acesso;
- ✓ usuários estão usando a rede de forma ineficiente, neste caso o gerente pode tomar providências para alteração de procedimentos e melhoria da performance;
- ✓ planejar o crescimento da rede de acordo com a utilização e crescimento de utilização.

2.2.5 Gerenciamento de Segurança

O propósito do gerenciamento de segurança é permitir a aplicação de políticas de segurança por meio de funções que incluem a criação, deleção e controle de serviços e mecanismos de segurança, a distribuição de informações críticas (confidenciais) e a notificação de eventos relativos à segurança.

Segundo Specialski (2000, p.5) o gerenciamento de segurança trata de questões como:

- ✓ geração, distribuição e armazenamento de chaves de criptografia;
- ✓ manutenção e distribuição de senhas e informações de controle de acesso;
- ✓ monitoração e controle de acesso à rede ou parte da rede e às informações obtidas dos nodos da rede;
- ✓ coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.

2.3 A Gerência Internet

O início dos protocolos de gerência de rede foi com o SGMP (Simple Gateway Monitoring Protocol) em novembro 1987. Entretanto o SGMP era restrito a *gateways*. A necessidade crescente de uma ferramenta de gerenciamento de rede mais genérica fez emergirem três abordagens:

- ✓ High-Level Entity Management System – HEMS – generalização do HMP – Host Management Protocol;
- ✓ SNMP – Simple Network Management Protocol – um melhoramento do SGMP;
- ✓ CMOT – (CMIP over TCP/IP) uma tentativa de incorporar o máximo possível o protocolo (CMIP), serviços e estrutura de base de dados que estava sendo padronizada pela ISO para gerenciamento de redes.

No início de 1988 a IAB (Internet Architecture Board) revisou os protocolos e escolheu o SNMP como uma solução de curto prazo e o CMOT como solução de longo

prazo. O sentimento era que em um período de tempo razoável as instalações migrariam do TCP/IP para protocolos baseados em OSI.

Entretanto, como a padronização do gerenciamento baseado no modelo OSI demorou muito a ser divulgada e o padrão SNMP foi amplamente implementado nos produtos comerciais, devido à sua simplicidade, o SNMP tornou-se um padrão de fato. Posteriormente foram definidas novas versões do protocolo SNMP chamadas de SNMPv2 e SNMPv3, o SNMP original ficou conhecido como SNMPv1.

2.3.1 O SNMPv1

O RFC 1157 define que a arquitetura SNMP consiste de uma solução para o problema de gerenciamento de redes, em termos de: escopo da informação de gerenciamento, representação da informação de gerenciamento, operações suportadas pelo protocolo sobre as informações de gerenciamento, forma e significado das trocas entre entidades de gerenciamento, definição de relacionamentos administrativos entre entidades de gerenciamento e a forma e o significado das referências às informações de gerenciamento.

O RFC 1157 define ainda três objetivos a serem alcançados pelo SNMP: minimizar o número e complexidade das funções de gerenciamento, ser flexível o suficiente para permitir expansões futuras e ser independente da arquitetura e mecanismo dos dispositivos gerenciados.

O modelo de gerenciamento de rede usado pelo SNMP inclui os seguintes elementos: estação de gerenciamento, agente de gerenciamento, base de informações de gerenciamento e protocolo de gerenciamento de rede. (Stallings, 1999, p.75)

A estação de gerenciamento terá: um conjunto de aplicações de gerenciamento para análise de dados e recuperação de falhas, uma interface que permitirá o gerente da rede a monitorar e controlar a rede, capacidade de traduzir os comandos do gerente em comando de gerenciamento e uma base de dados extraída das MIBs (Management Information Base) de todas as entidades gerenciadas na rede.

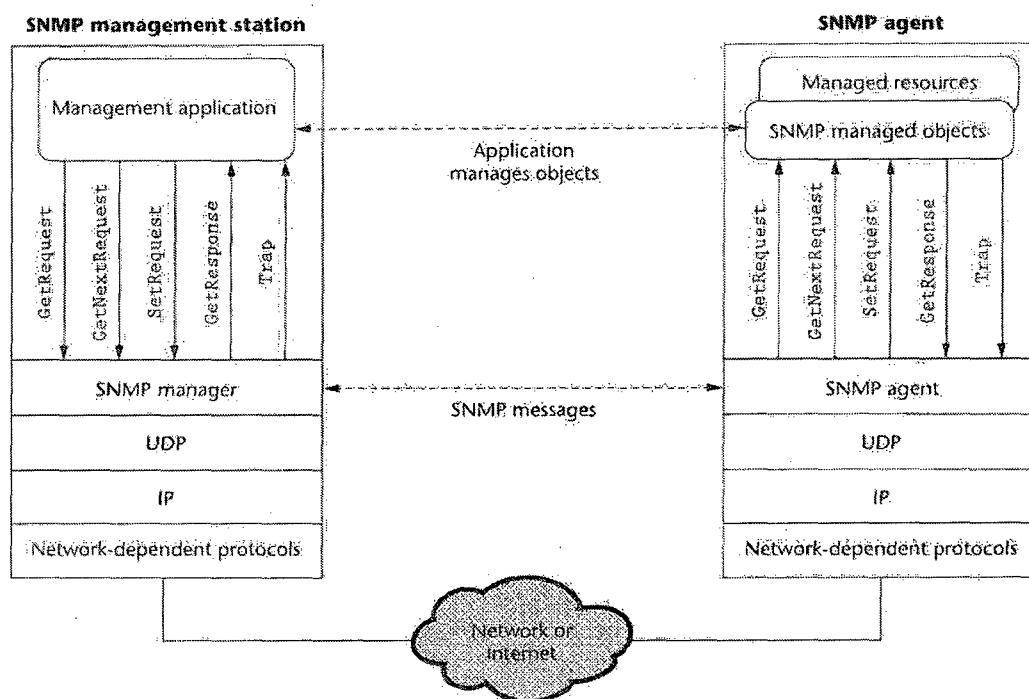
O agente de gerenciamento está localizado nos objetos gerenciados e responde a requerimentos de informação e ações do sistema de gerenciamento e pode prover a estação de gerenciamento de informações importantes mas não solicitadas. Os recursos da rede podem ser gerenciados através da representação destes recursos como objetos. Cada objeto é essencialmente uma variável de dados que representa um aspecto do agente gerenciado. A coleção de objetos é denominada MIB (base de informações de gerenciamento).

A estação de gerenciamento e os agentes se comunicam através do protocolo de gerenciamento, o protocolo utilizado no TCP/IP é o SNMP. O SNMP foi projetado para ser um protocolo de camada de aplicação da família TCP/IP e trabalhar sobre UDP, que é um protocolo não orientado à conexão. A simplicidade e a utilização de comunicação sem conexão resultou em um protocolo robusto. Nem o gerente nem o agente dependem um do outro para continuarem operacionais.

A comunicação de informações de gerenciamento é feita no SNMPv1 utilizando somente cinco mensagens de protocolo, conforme mostrado na figura 2.2, três delas (*get-request*, *get-next-request* e *set-request*) são iniciadas pelo processo de aplicação gerente, as outras duas (*get-response* e *trap*) são geradas pelo processo agente. A geração de mensagens é chamada de um evento. No esquema de gerenciamento SNMP

o gerente monitora a rede polando os agentes sobre seu estado e características. Entretanto a eficiência é aumentada quando agentes enviam mensagens não solicitadas chamadas de *traps*. Um *trap* ocorre quando o agente observa a ocorrência de um parâmetro pré-configurado no módulo agente.

Figura 2.2 – Arquitetura de Gerenciamento de Rede SNMPv1



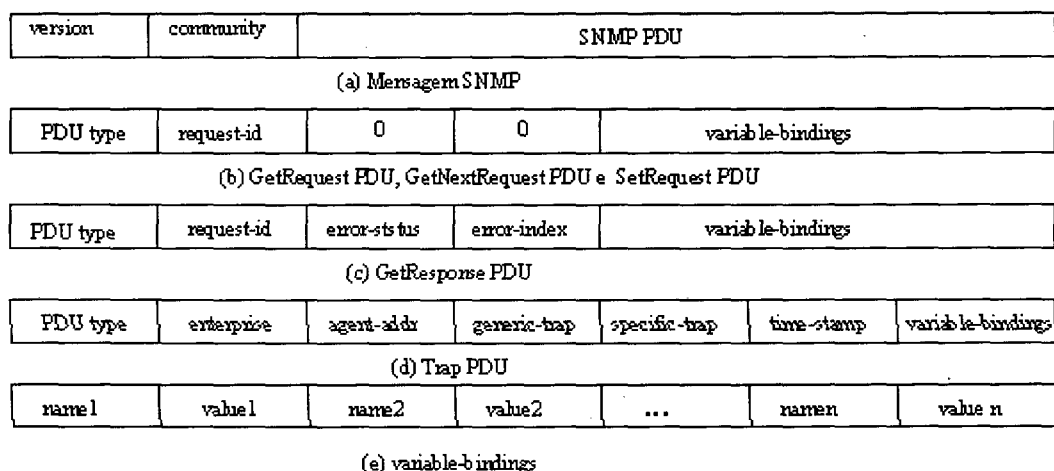
Fonte: Stallings (1999, p.81)

Quadro 2.1 – Operações Suportadas no SNMPv1

Operação	Função
get-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis informados na solicitação
get-next-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis que sucedem lexicograficamente àquelas informadas na solicitação
set-request	Solicitação para atribuição de valor a uma ou um conjunto de variáveis
get-response	Resposta às operações get-request, get-next-request e set-request
Trap	Envio de um evento não solicitado para uma ou várias estações de gerenciamento. Tipos de traps definidos no RFC 1215: cold start, warm start, link down, link up, authentication failure, egp neighbor loss e enterprise specific.

A mensagem SNMP é dividida em duas seções: uma identificação de versão e nome da comunidade e a PDU (protocol data unit). A versão e comunidade são às vezes chamadas de *header* de autenticação SNMP. Existem 5 tipos diferentes de PDU: *get-request*, *get-next-request*, *get-response*, *set-request* e *trap*. Todas as PDU's, exceto o *trap*, têm o mesmo formato. (Miller 1997, p.167)

Figura 2.3 – Formato de Mensagens SNMPv1



O SNMPv1 tem um processo de autenticação fraca. Ele se baseia em *string* de caracteres chamado *community* contido no *header* do pacote SNMP e que trafega em modo legível pela rede. São definidas duas *communities*, uma para acesso somente de leitura e outra para acesso de leitura e gravação.

O SNMP não provê mecanismos específicos para que um gerente dê comandos para que um agente execute uma ação. Entretanto, é possível utilizar a operação *set* para contornar esta deficiência. Um objeto pode ser utilizado para representar um comando, então uma ação específica é executada se o valor do objeto é alterado para um valor específico (ex: objeto *reboot*).

A representação de objetos e informações relevantes ao seu gerenciamento formam o modelo de informações de gerenciamento. O SMI define a sintaxe e semântica das informações armazenadas na MIB. A MIB é usada tanto no agente quanto no gerente para armazenar e trocar informações de gerenciamento. A MIB associada ao agente é denominada MIB agente e a associada ao gerente é denominada MIB gerente. Uma MIB gerente consiste de informações de todos os componentes que ela gerencia, enquanto a MIB agente necessita conhecer somente sua informação local. (Subramanian 2000, p.110)

A MIB usa uma arquitetura em árvore, definida na ISO ASN.1, para organizar todas as suas informações. Cada parte da informação da árvore é definido como um nó rotulado que contém um identificador de objetos (OID), que é uma seqüência de números separados por pontos, e uma pequena descrição textual do nó rotulado. As folhas são os objetos realmente gerenciados, que representam algum recurso, atividade ou informação a ser gerenciada.

A estrutura em árvore define agrupamentos de objetos logicamente relacionados. Os objetos gerenciados são organizados em grupos por dois motivos: fica mais inteligível em uma organização em árvore e também se um grupo é implementado implica na implementação de todos os objetos do grupo. Certamente é possível que um agente não suporte todos os objetos do grupo, neste caso o fabricante não pode dizer que suporta o grupo. Stallings (1999, p.198) alerta que alguns fornecedores tentaram contornar esta restrição devolvendo valor zero para os objetos do grupo que não conseguem gerenciar.

A MIB inicialmente definida no SNMP como padrão no RFC 1156, que ficou conhecida como MIB-I, foi posteriormente expandida e formalizada como padrão no RFC 1213, conhecida como MIB-II. A MIB-II, representada pela figura 2.4, está definida em iso.org.dod.internet.mgmt.mib2 (1.3.6.1.2.1). Abaixo da sub-árvore da MIB-II estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos são divididos em 11 grupos:

- ✓ **system (mib-2 1)** – grupo obrigatório que contém informações sobre o sistema no qual se encontra a entidade gerenciada;
- ✓ **interfaces (mib-2 2)** – grupo obrigatório que oferece dados sobre cada interface do dispositivo gerenciado.
- ✓ **address translation (mib-2 3)** – não constitui mais um grupo separado. Seus objetos foram incorporados aos grupos de protocolos;
- ✓ **ip (mib-2 4)** – grupo obrigatório que provê informações sobre o protocolo ip da entidade. As informações estão subdivididas em quatro grupos: objetos que informam erros e tipos de pacotes ip vistos, tabela de informação sobre endereços ip da entidade, tabela de roteamento ip da entidade e mapeamento de endereços ip para outros protocolos (substituindo o grupo Address Translation);
- ✓ **icmp (mib-2 5)** – grupo obrigatório que contém objetos que fornecem informações sobre o protocolo icmp da entidade;
- ✓ **tcp (mib-2 6)** – grupo obrigatório caso o dispositivo implemente o protocolo tcp e provê informações importantes para o gerenciamento do tcp. Este grupo é dividido em dois subgrupos: objetos gerais sobre o tcp no sistema e uma tabela de valores para cada conexão tcp corrente;

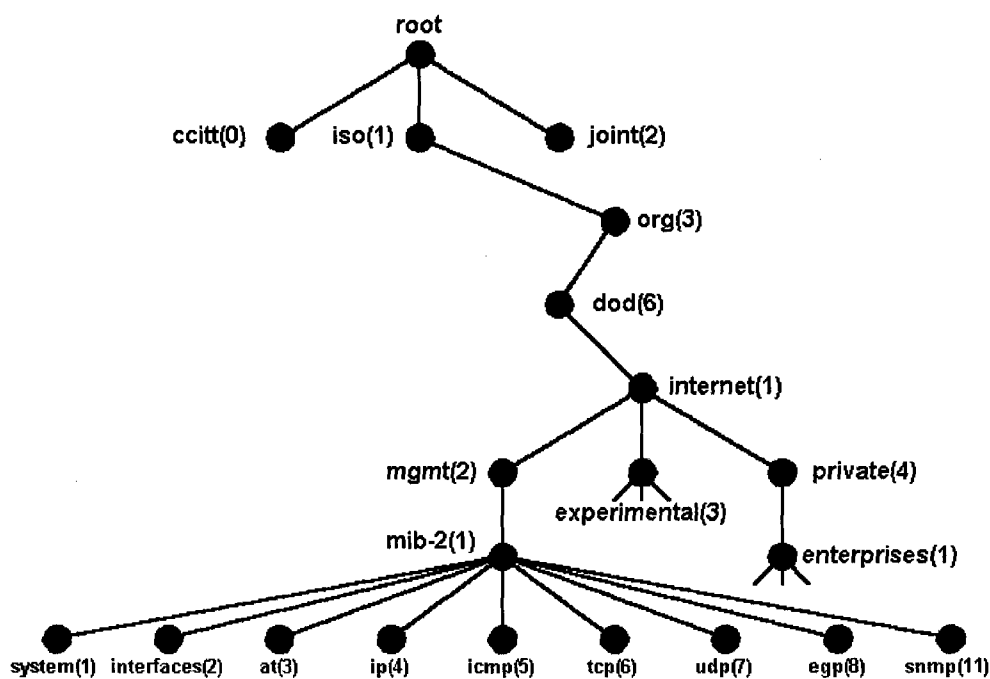
- ✓ **udp (mib-2 7)** – grupo obrigatório caso o dispositivo implemente o protocolo udp e provê informações importantes para o gerenciamento do udp. Este grupo é subdividido em dois grupos: objetos gerais sobre o udp e entradas sobre as aplicações udp que estão recebendo datagramas correntemente na entidade;
- ✓ **egp (mib-2 8)** – grupo obrigatório caso o dispositivo implemente o protocolo egp e contém várias informações de estado e endereço de roteadores vizinhos. O grupo egp está dividido em dois subgrupos: informações sobre o egp na entidade e uma tabela de entradas contendo informações sobre cada vizinho egp;
- ✓ **transmission (mib-2 10)** – uma entrada obrigatória para cada meio de transmissão suportado pelo dispositivo de rede. Para cada padrão de transmissão existe uma sub-árvore. Por exemplo a sub-árvore do padrão *ethernet* 802.3 é representada por dot3;
- ✓ **snmp (mib-2 11)** – grupo obrigatório se o snmp é suportado e contém informações úteis para verificação de tráfego snmp e tentativas de acesso mal sucedidas.

Apesar de amplamente difundido e utilizado no gerenciamento de redes de computadores, o SNMPv1 possui as seguintes limitações:

- ✓ não é apropriado para o gerenciamento de redes muito grandes, devido à limitação de performance de *polling*;
- ✓ *traps* SNMP não são reconhecidos, pois são implementados sobre protocolos sem reconhecimento/conexão;
- ✓ o padrão SNMPv1 provê somente autenticação trivial;
- ✓ o modelo da MIB é limitado e não suporta aplicações que questionam o gerenciamento baseado em valores ou tipos de objetos;

- ✓ não é possível ter uma idéia do tráfego existente nas redes onde os recursos gerenciados estão instalados pois estas informações referem-se ao próprio recurso onde o agente está executando;
- ✓ incapacidade de analisar seus próprios dados e enviar notificações quando alguns limiares forem atingidos; e
- ✓ não suporta a comunicação gerente-gerente.

Figura 2.4 – MIB II



2.3.2 O RMON

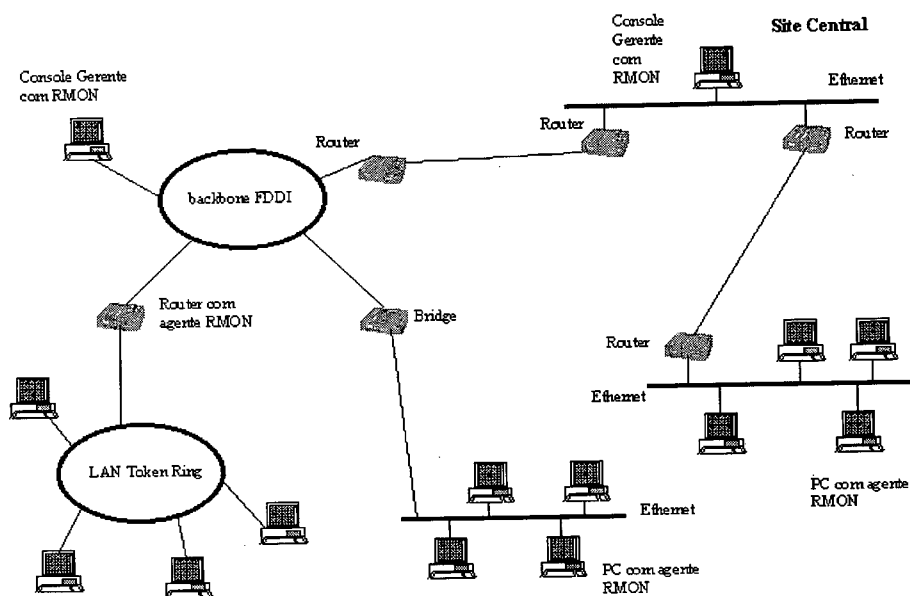
À medida em que as redes foram crescendo e se tornando geograficamente e logicamente distribuídas, o gerenciamento de redes tornou-se mais desafiador. Uma solução seria a instalação de dispositivos remotos de gerenciamento, denominados probes, nos segmentos remotos. A MIB RMON (Remote Network Monitoring MIB)

padronizou as informações de gerenciamento enviadas para e recebidas desses probes na RFC1757.

Specialski (2000, p.16) classifica a MIB RMON como a mais importante adição ao conjunto de padrões SNMP. Segundo Black (1998 , p.54), a MIB RMON pode ser vista como uma extensão da MIB II e melhora bastante o nível de gerenciamento da rede. Na MIB II a informação é recuperada através de variáveis que retornam o valor em determinado instante. A fim de monitorar o dispositivo é necessário que sejam recuperadas inúmeras variáveis e aplicar fórmulas sobre os valores conseguidos. Para ver a alteração das informações com o tempo é necessário recuperar continuamente e armazenar os valores para comparação.

O RMON divide o processo de captação de dados em duas partes. Os dados são coletados pelo agente RMON que pode estar em um segmento próximo ao dispositivo ou implementado no dispositivo. Uma ou mais estações de gerenciamento falam com o agente RMON (usando SNMP) em lugar de falar diretamente com o dispositivo gerenciado. Por terminologia, um sistema que implementa a MIB RMON é chamado de probe RMON. Mesmo que a estação de gerenciamento perca conexão ao probe a coleta de dados continua, uma vez que o probe está conectado diretamente à rede sendo monitorada. Para implementar um agente RMON em um dispositivo deve ser capaz de operar no modo promíscuo, em que poderá aceitar dados não endereçados especificamente para ele.

Figura 2.5 – Rede com agentes RMON



fonte: Data Communications Magazine - Maio 1992.

As metas definidas pelo grupo de trabalho para a definição das MIBs RMON são definidas nos RFCs 1757 e 2021. São elas:

- ✓ **operação off-line** – o probe acumula estatísticas e executa diagnósticos continuamente, mesmo que a comunicação com a estação gerente não seja possível ou eficiente. As notificações podem ser enviadas para o gerente quando eventos excepcionais ocorrerem. Além disso o gerente pode recuperar informações do probe RMON quando melhor lhe aprouver, utilizando o protocolo SNMP;
- ✓ **monitoramento pró-ativo** - se o monitor tiver recursos suficientes, pode executar continuamente diagnósticos e logar performance da rede. Em uma falha na rede, pode notificar a estação gerente da falha e prover informações proveitosas no diagnóstico da falha;
- ✓ **deteção e registro de problemas** - O monitor pode passivamente reconhecer certas condições de erro e outros, como congestionamento, no tráfego observado.

Quando uma condição configurada ocorrer, pode logar e tentar notificar a estação gerente;

- ✓ **análise de dados** - o monitor pode executar análises específicas depois de coletados os dados na subrede. Por exemplo, pode determinar que *host* gera a maior parte do tráfego ou erros na subrede;
- ✓ **múltiplos gerentes** - uma configuração de rede pode ter mais do que uma estação gerente como medida de redundância, que podem executar funções diferentes e prover capacidades de gerência para unidades diferentes na organização.

O RMON provê informações estatísticas e de diagnóstico, o que minimiza o tráfego de gerenciamento, reduz o impacto de perda de conectividade, serve várias estações de gerenciamento simultaneamente e provê um conjunto padrão de métricas que pode ser usado por vários dispositivos que suportam RMON.

A MIB RMON, que possui OID {1.3.6.1.2.1.16}, foi originalmente definida para redes *ethernet* em novembro de 1991 no RFC 1271, em 1995 foi substituída pelo RFC 1757, que foi, em maio de 2000, substituído pelo RFC 2819. Originalmente a MIB RMON só contemplava redes *ethernet*, mas em setembro de 1993 foi desenvolvido o RFC 1513, que trazia extensões para redes *token ring*. A MIB RMON contém 10 grupos. Os grupos RMON são:

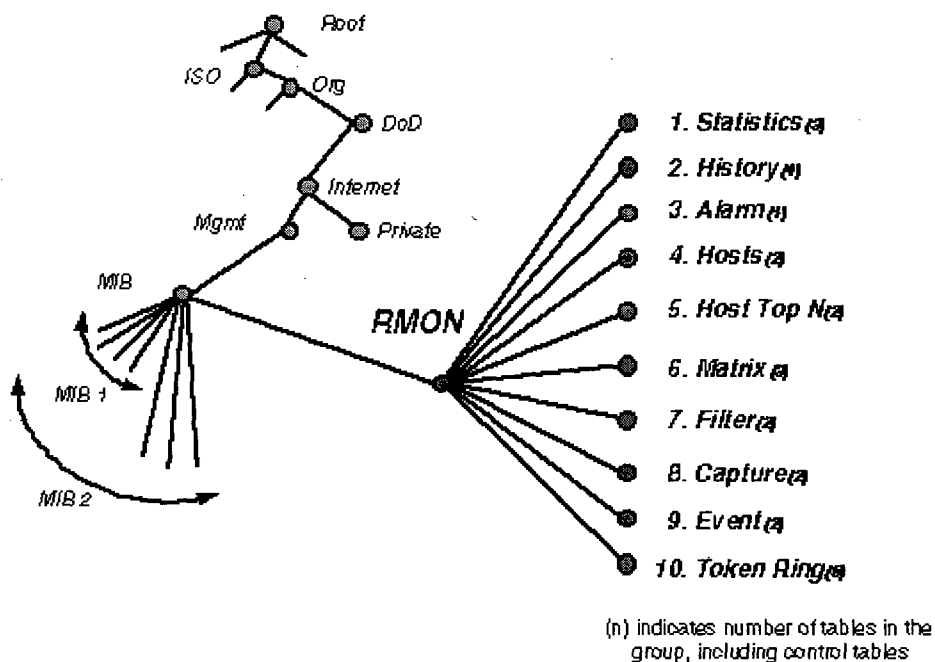
- ✓ **statistics (rmon 1)** – provê estatísticas medidas pelo probe no segmento, tais como número e tamanho dos pacotes, *broadcast*, colisões, etc;
- ✓ **history (rmon 2)** - grava amostras estatísticas periódicas do tráfego para permitir análise posterior;

- ✓ **alarm (rmon 3)** - compara amostras estatísticas com limiares configurados gerando alarmes quando estes limiares forem ultrapassados;
- ✓ **host (rmon 4)** - mantém estatísticas dos *hosts* na rede, incluindo o *MAC address* dos *hosts* ativos;
- ✓ **hostTopN (rmon 5)** - provê relatórios indicando quais *hosts* estão no topo de uma categoria em particular;
- ✓ **matrix (rmon 6)** - armazena estatísticas de tráfego sobre conversações entre *hosts*;
- ✓ **filter (rmon 7)** - permite que pacotes sejam selecionados de acordo com um critério especificado;
- ✓ **capture (rmon 8)** - permite que pacotes sejam capturados depois de passarem pelo filtro;
- ✓ **event (rmon 9)** - controla a geração e notificação de eventos, o que pode incluir mensagens de *trap* SNMP;
- ✓ **tokenRing (rmon 10)** – provê parâmetros adicionais para redes *token ring*.

Todos os grupos são opcionais, mas a implementação de alguns grupos requer outros grupos. Existem as seguintes dependências:

- ✓ o grupo *alarm* requer a implementação do grupo *event*;
- ✓ o grupo *hostTopN* requer a implementação do grupo *host*;
- ✓ o grupo *capture* requer a implementação do grupo *filter*.

Figura 2.6 – Grupos RMON1

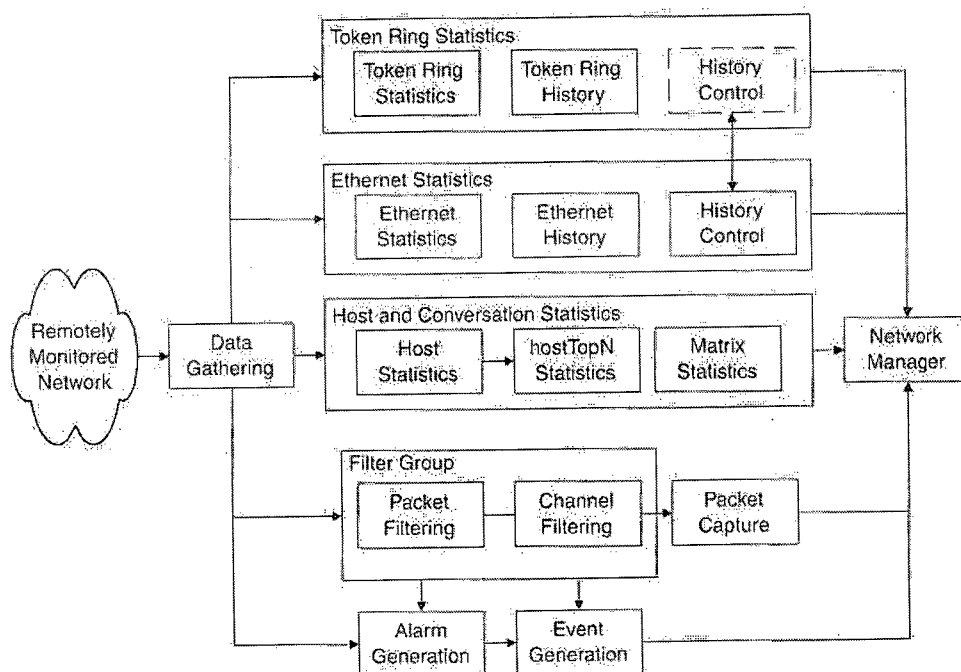


Subramanian (2000, p.327) enquadra os grupos RMON em três grandes categorias: a maior é a dos grupos que analisam as informações e geram estatísticas. Nesta categoria enquadram-se os grupos *statistics*, *history*, *host* e *host top N*. A segunda categoria trata de eventos da rede e funções de geração de relatórios. Estes são os grupos de *alarm* e *event*. A terceira categoria trata com filtragem e captura de pacotes. Nesta categoria enquadram-se os grupos *filter* e *packet capture*.

Tipicamente, um monitor remoto necessitará ser configurado para coletar dados. A configuração dita o tipo e forma de coleta dos dados. A MIB é organizada em grupos funcionais. Cada grupo terá uma ou mais tabelas de controle e uma ou mais tabelas de dados. Uma tabela de Controle contém parâmetros que descrevem o dado na tabela de Dados, que é somente para leitura. Assim, a estação gerente seta os parâmetros apropriados para configurar o monitor remoto para coletar os dados desejados. Os parâmetros são setados pela adição de um novo registro na tabela, ou alterando um

registro existente. Desse modo, funções para serem executadas pelo monitor são definidas e implementadas na tabela. Por exemplo, uma tabela de Controle pode conter objetos que especifiquem a origem dos dados coletados, tipos de dados, hora/data da coleta etc...

Figura 2.7 – Classificação dos grupos RMON



Fonte: Subramanian (2000, p.326)

2.3.3 O RMON2

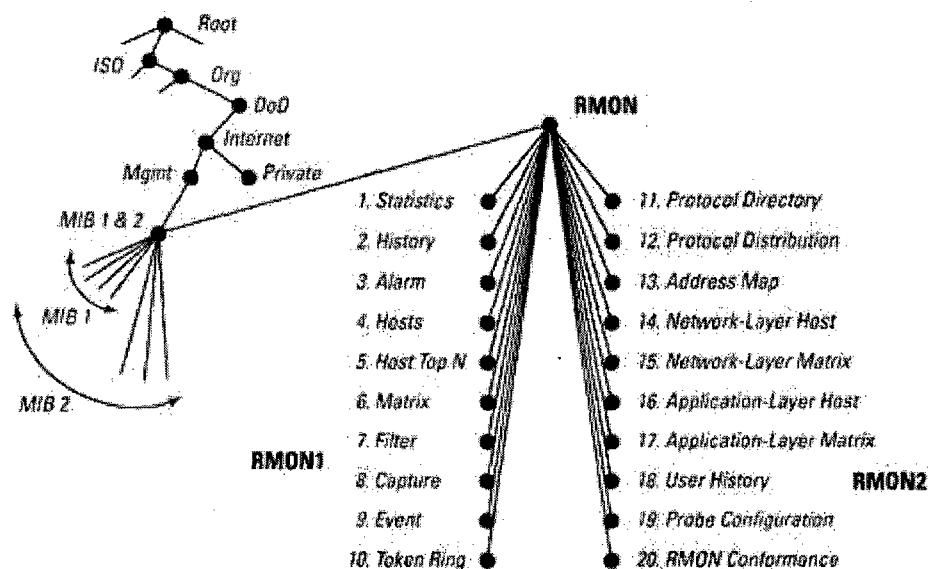
A MIB RMON original se preocupava basicamente com operação e gerenciamento das camadas física e de enlace de uma rede remota. O RMON2 definido no RFC2021, estende as capacidades do RMON às camadas superiores, adicionando 10 novos grupos: (Miller 1997, Subramanian 2000)

✓ *protocol directory (rmon 11)* - identifica os protocolos que o probe pode monitorar.

Os protocolos que podem ser monitorados foram definidos no RFC2074;

- ✓ *protocol distribution* (**rmon 12**) - provê informação relativa ao tráfego de diferentes protocolos, tanto em bytes quanto em pacotes. Ele coleta estatísticas que ajudam o administrador de rede a gerenciar a banda alocada para cada protocolo;
- ✓ *address map* (**rmon 13**) - correlaciona os endereços de rede com endereços MAC, armazenando-os em uma tabela. A tradução de endereços permite a geração de mapas topológicos aprimorados e a detecção de endereços ip duplicados;
- ✓ *network-layer host* (**rmon 14**) – coleciona estatísticas sobre o volume de tráfego de entrada e saídas das estações com base no endereço de nível de rede. Como consequência, o gerente pode observar além dos roteadores que interligam as sub-redes e identificar as reais estações que estão se comunicando;
- ✓ *network-layer matrix* (**rmon 15**) – provê estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de rede;
- ✓ *application-layer host* (**rmon 16**) – agrega estatísticas sobre o volume de tráfego por protocolo de nível superior gerado de ou para cada endereço de rede;
- ✓ *application-layer matrix* (**rmon 17**) – coleciona estatísticas sobre o volume de tráfego, por protocolo, trocados por pares de endereços de rede;
- ✓ *user history collection* (**rmon 18**) - combina mecanismos vistos nos grupos *alarm* e *history* para prover informações de coleção de dados históricos especificados pelo usuário;
- ✓ *probe configuration* (**rmon 19**) – define parâmetros de configuração padrões para probes RMON. Deste modo, a estação de gerenciamento com software de um fabricante é capaz de configurar remotamente um probe de outro fabricante;
- ✓ *rmon conformance* (**rmon 20**) – descreve os requisitos de conformidade para a MIB RMON2.

Figura 2.8 – Grupos RMON2

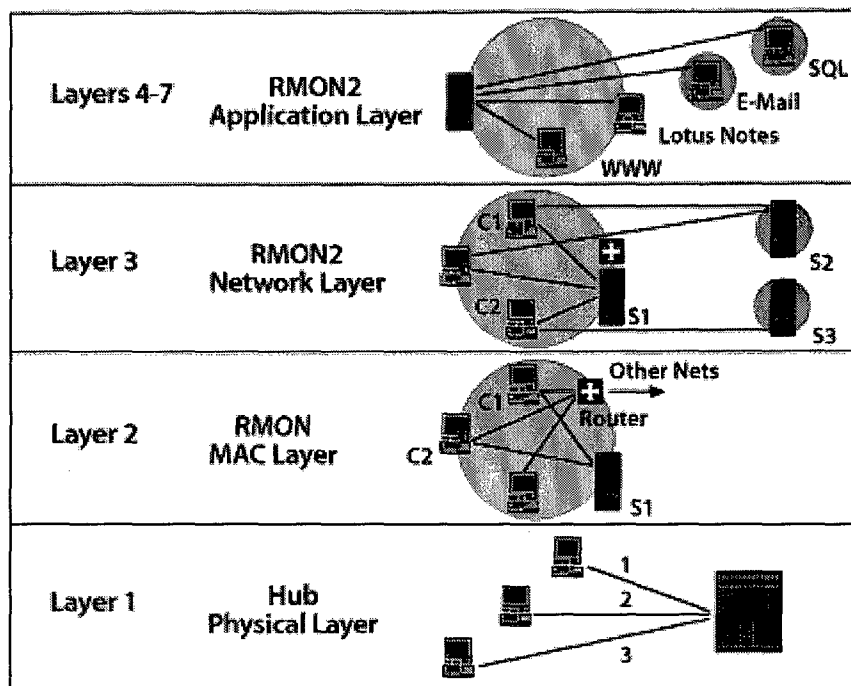


Stallings (1999, p.277) cita duas implicações importantes decorrentes do fato de que o RMON2 decodifica pacotes das camadas 3 a 7 do modelo OSI:

- ✓ o probe RMON2 pode monitorar o tráfego baseado nos endereços e protocolos de camada de rede, incluindo o IP. Isto possibilita que o probe veja acima da rede local ao qual está conectado;
- ✓ como o RMON2 pode decodificar e monitorar tráfego da camada de aplicação, o probe pode gravar tráfego para aplicações específicas.

A figura 2.9 mostra o nível de visibilidade que RMON e RMON2 provêm dentro de um segmento LAN ou de uma rede em cada uma das camadas do OSI.

Figura 2.9 – Visibilidade RMON1 x RMON2



As restrições com relação à performance para implementação do RMON1 são ainda maiores no RMON2, pois ele necessita ainda de mais recursos de memória e processamento para ser implementado. Para atender a estas demandas, os fabricantes de dispositivos RMON2 estão oferecendo probes *stand-alone* que executam em plataformas de hardware de alta capacidade de memória e processamento. (Stallings 1999, p.326)

2.3.4 O SNMPv2

O SNMP foi desenvolvido como uma solução temporária para prover um gerenciamento mínimo da rede, a solução definitiva viria com o gerenciamento baseado no modelo OSI. Alguns motivos fizeram que esta transição não acontecesse da forma planejada, principalmente porque:

- ✓ o modelo OSI usava a abordagem orientada a objeto que era mais complexa do que o que se planejava implementar no SNMP que implementou uma MIB escalar, o que tornava a transição mais complexa.
- ✓ o desenvolvimento de padrões OSI de gerenciamento e subsequente disponibilização de sua implementação em dispositivos de rede demorou muito mais do que o esperado, abrindo uma janela de oportunidade que foi aproveitada pelo SNMP.

A versão 2 do SNMP (SNMPv2) foi desenvolvida quando tornou-se óbvio que o padrão de gerenciamento OSI não seria implementado em um futuro próximo. Os maiores fabricantes de dispositivos de rede já haviam incorporado módulos SNMP em seus equipamentos e estava claro para todos que o SNMP necessitava de melhoramentos.

O primeiro projeto do SNMPv2 não foi amplamente aceito pelo mercado. As razões citadas freqüentemente para esta falta de aceitação são a complexidade dos melhoramentos de segurança e administração do *framework*. Várias tentativas de simplificação foram tentadas, entretanto não se chegou a nenhum consenso. Como resultado ocorreram três ações (Miller 1997, p.201):

- ✓ os documentos que tinham atingido consenso foram publicados em janeiro de 1996 como RFC's 1902-1908;
- ✓ modificações menores no modelo de administração e segurança do SNMPv2, denominados *communit-based* SNMPv2 (SNMPv2c), foram publicados em janeiro de 1996, documento RFC 1901;

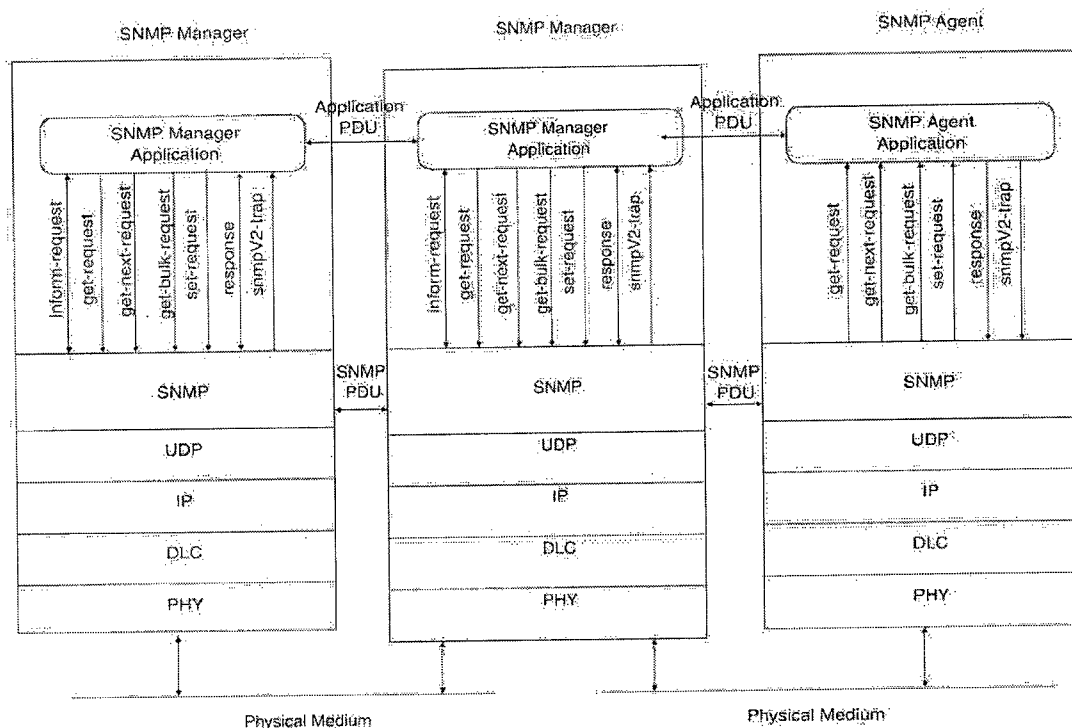
- ✓ o trabalho continuou em outras áreas: segurança, *framework* administrativo, MIB de configuração remota e comunicação gerente-gerente.

Várias mudanças significativas deveriam ter sido introduzidas no SNMPv2. Uma das mais significativas seria a de prover funções de segurança, que inexistiam no SNMPv1. Infelizmente, depois de muito esforço, não houve consenso, então a *feature* de segurança foi retirada da especificação final.

Apesar do modelo organizacional permanecer praticamente inalterado e a despeito da falta de melhorias na parte de segurança, várias melhorias foram feitas na arquitetura SNMPv2: novos tipos de dados, novas macros, convenções textuais, operações que facilitam a transferência de grandes quantidades de dados (*bulk*), transferência de blocos de dados (*bulk*), códigos de erro mais detalhados, suporte a multiprotocolos na camada de transporte, inclusão de mensagem de gerente para gerente, definição de uma nova estrutura de informações de gerenciamento (SMIv2 definida nas RFCs 1902 a 1904 e posteriormente padronizada nos RFCs 2578 a 2580), comandos de conformidade, melhorias em tabelas e inclusão de dois novos grupos na MIB, *security* e SNMPv2. (Subramanian 2000, Miller 1997)

O SNMPv2 provê três tipos de acesso a informações de gerenciamento de redes. O primeiro tipo de interação chamado *request-response* é quando o gerente SNMP envia uma solicitação a um agente SNMPv2 que responde. O segundo tipo de interação é um *request-response* onde ambas as entidades são gerentes SNMP. O terceiro tipo é uma interação não confirmada, onde um agente SNMPv2 envia uma mensagem não solicitada, ou *trap*, para o gerente e nenhuma resposta é retornada. Somente a segunda forma é nova no SNMPv2, as outras duas já existiam no SNMPv1.

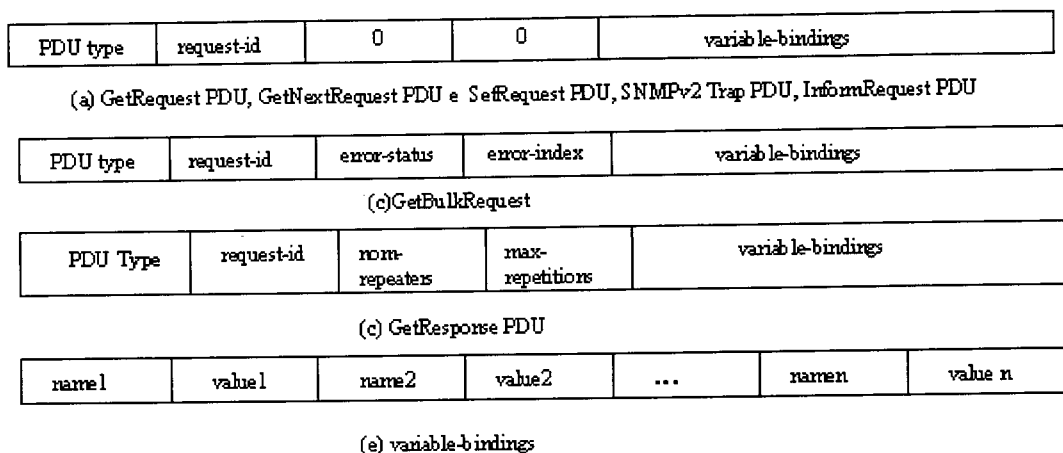
Figura 2.10 – Arquitetura de gerenciamento de rede SNMPv2



Fonte: Subramanian (2000, p. 232)

A alteração mais importante nas operações do SNMPv2 foi a inclusão de duas novas PDU's. A *get-bulk-request* que permite ao gerente recuperar grandes blocos de dados eficientemente, em particular várias linhas de tabelas. A PDU *information-request* é gerada por um gerente para informar a outro gerente informação contida em sua visão da MIB. Uma resposta é gerada pelo gerente que recebeu a mensagem para o gerente que a enviou. A estrutura de dados PDU foi padronizada para que todas as mensagens possuam um formato comum, a informação nos *traps* na versão 2 do SNMP foi modificada para ficar com o mesmo padrão das outras PDU's. Isto aumenta a eficiência e performance na troca de mensagens entre sistemas.

Figura 2.11 – Formato de PDUs do SNMPv2



As PDUs *Get-request* e *Get-next-request* são idênticas às do SNMPv1 em formato e semântica. A diferença é que no SNMPv1 as operações eram atômicas: ou todos os valores eram retornados ou nenhum valor retornava. No SNMPv2 a lista de *variable-bindings* é preparada, mesmo se valores não podem ser recuperados para todas as variáveis. Se uma condição de exceção é encontrada para uma variável então a variável é retornada com a indicação da exceção em lugar do valor.

A versão 1 do SNMP foi originalmente definida para transmissão sobre o UDP e IP. Pesquisas subseqüentes exploraram o uso do SNMP com outros protocolos de transporte, incluindo o OSI (RFC 1418), appletalk (RFC 1419) e IPX (RFC 1420). O SNMPv2 formalmente define implementações sobre outros protocolos de transporte no RFC 1906. Apesar de definido para vários protocolos de transporte, o RFC 1906 sugere que agentes continuem ouvindo o UDP na porta 161 e gerando notificações na porta 162 do UDP.

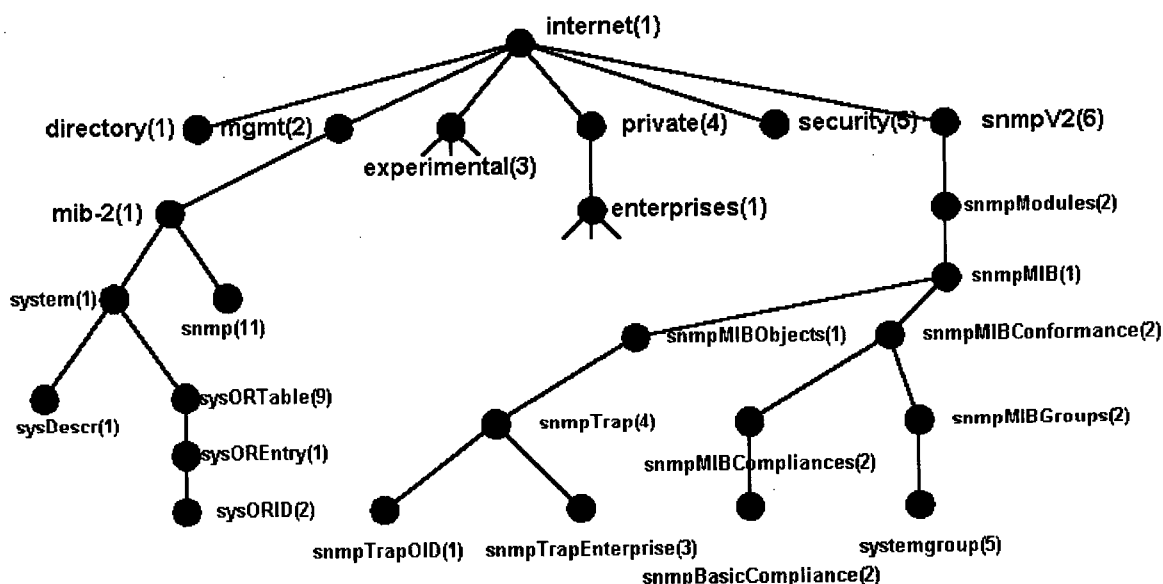
O grupo de trabalho do IETF responsável pelo SNMPv2 propôs dois esquemas de migração (RFC 1908) do SNMPv1 para o SNMPv2: o gerente bilíngüe que falaria

com o agente SNMP na versão que ele entendesse e o SNMP *proxy server* que receberia as mensagens SNMPv2 e, atuando como *proxy*, as transmitiria para o agente como SNMPv1.

Algumas modificações foram introduzidas na MIB internet: o grupo *system* do SNMPv2 é composto pelos mesmos objetos do SNMPv1 expandindo com a inclusão de novos objetos que permitem a uma entidade SNMPv2 agindo como agente descrever seus recursos dinamicamente. Além disso, o grupo SNMP na versão do SNMPv2 comparado com o originalmente definido da MIBII tem muito menos objetos. A razão é que as estatísticas detalhadas definidas na MIB II não auxiliam na solução de problemas e adicionam complexidade desnecessária aos agentes.

Apesar das vantagens apresentadas pelo SNMPv2 ele apresenta algumas limitações: é pouquíssimo utilizado, sua complexidade implica em dificuldades de implementação e não foi bem recebido pela comunidade de gerência.

Figura 2.12 – Árvore do SNMPv2



2.3.5 O SNMPv3

Depois de muita controvérsia, o SNMPv2 foi liberado como um *framework* SNMP, SNMPv2C, sem qualquer implementação adicional de segurança. Esta deficiência foi solucionada no SNMPv3. Os documentos do grupo de trabalho do SNMPv3 não são de fato especificações completas de um protocolo de gerenciamento de redes. Na verdade estes documentos definem um conjunto de características de segurança e um *framework* que poderia ser utilizado com as capacidades funcionais do SNMPv2 ou SNMPv1. (Stallings 1999, Subramanian 2000)

Uma das características chave do SNMPv3 é a modularidade da documentação e arquitetura. O projeto da arquitetura integrada das especificações SNMPv1 e SNMPv2 com as do SNMPv3. Esta integração permite a continuação de uso do legado de SNMP por agentes e gerentes SNMPv3.

O RFC 2571, documento que definiu a arquitetura do SNMPv3, define os seguintes objetivos que guiaram seu desenvolvimento:

- ✓ utilizar o trabalho existente. Os conceitos de segurança do SNMPv3 se baseiam fortemente no SNMPv2u e SNMPv2*;
- ✓ resolver o problema de segurança, principalmente para a operação *set-request*, considerada a deficiência mais importante no SNMPv1 e SNMPv2C;
- ✓ ser modular para possibilitar o desenvolvimento de parte da arquitetura, mesmo que o consenso não tenha sido atingido no todo;
- ✓ definir uma arquitetura que permita longevidade ao *framework* SNMP que já tinha sido definido e que venha a ser definido no futuro;

- ✓ manter o SNMP o mais simples possível;
- ✓ projetar uma arquitetura modular que permita a implementação sobre diversos ambientes operacionais; e
- ✓ acomodar modelos de segurança alternativos.

Um dos principais objetivos do SNMPv3 foi a área de segurança. Autenticação, privacidade, bem como a autorização e controle de acesso foram incorporados na especificação SNMPv3. O SNMPv3 é projetado para prover segurança contra as seguintes ameaças:

- ✓ modificação da informação – uma entidade poderia alterar uma mensagem em trânsito gerada por uma entidade autorizada;
- ✓ *masquerade* – uma entidade não autorizada assumir a identidade de uma entidade autorizada;
- ✓ modificação de *stream* de mensagem – como o SNMP é projetado para operar sobre um protocolo não orientado à conexão, existe a ameaça de que as mensagens SNMP possam ser reordenadas, atrasadas ou duplicadas;
- ✓ descoberta – uma entidade poderia observar trocas de mensagens entre gerentes e agentes e aprender o valor de objetos gerenciados e eventos notificados.

O SNMPv3 não contém mecanismos de segurança contra duas ameaças:

- ✓ *denial of service* – uma pessoa poderia impossibilitar trocas de mensagens entre gerente e agente;
- ✓ análise de tráfego – uma pessoa poderia observar o padrão de tráfego entre gerentes e agentes.

A arquitetura SNMP, conforme definida no RFC 2571, consiste de uma coleção de entidades SNMP distribuídas e interagindo. Cada entidade implementa uma parte das características do SNMP e pode atuar como um nó agente, um nó gerente ou uma combinação dos dois. Cada entidade SNMP consiste de uma coleção de módulos que interagem entre si para prover serviços.

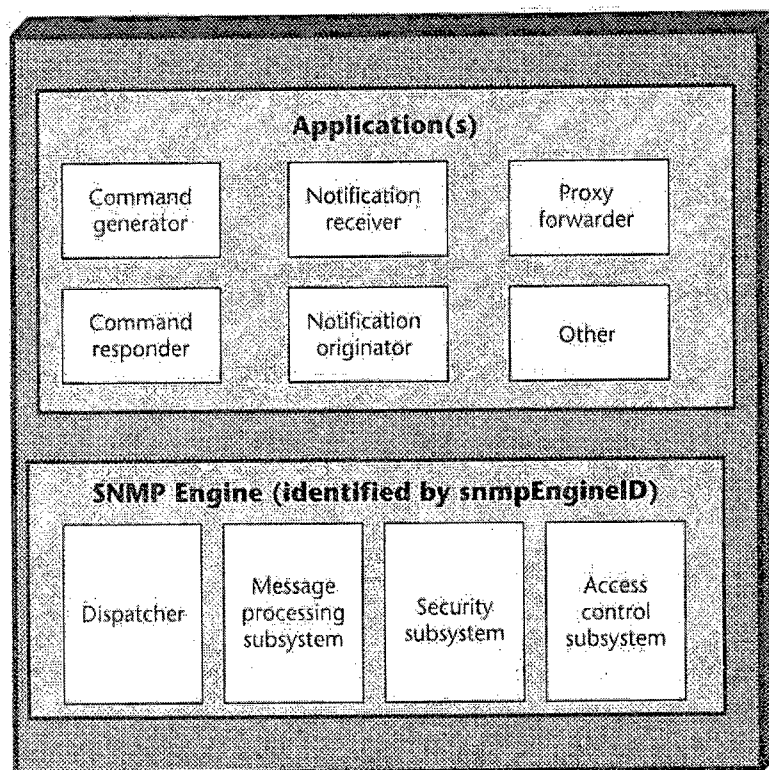
A figura 2.13, definida no RFC 2571, mostra detalhes de uma entidade SNMP e seus componentes:

- ✓ ***dispatcher*** – permite o suporte concorrente a múltiplas versões de mensagens SNMP no *engine* SNMP;
- ✓ ***message processing subsystem*** – responsável por preparar mensagens para envio e extrair dados de mensagens recebidas;
- ✓ ***security subsystem*** – provê serviços de segurança tais como autenticação e privacidade de mensagens. Este subsistema pode conter múltiplos modelos de segurança;
- ✓ ***access control subsystem*** – provê um conjunto de serviços que uma aplicação pode usar para checagem de direitos de acesso;
- ✓ ***command generator*** – inicializa as PDUs SNMP (*get*, *get-next*, *get-bulk*, *set-request*) e processa a resposta gerada para uma requisição;
- ✓ ***command responder*** – recebe as PDUs SNMP destinadas para o sistema local. A aplicação *command responder* executará a operação apropriada do protocolo, usando o controle de acesso, e gera a mensagem de resposta a ser enviada;
- ✓ ***notification originator*** – monitora o sistema por eventos e condições particulares e gera mensagens (*trap/inform*) baseado nos eventos e condições. Devem existir

mecanismos para determinar para onde enviar as mensagens, qual versão do SNMP utilizar e quais parâmetros de segurança devem ser utilizados;

- ✓ *notification receiver* – ouve as mensagens de notificação e gera mensagens de resposta quando uma mensagem contendo uma PDU inform é recebida;
- ✓ *proxy forwarder* – repassa mensagens SNMP. Sua implementação é opcional.

Figura 2.13 – Entidade SNMPv3 (RFC 2571)

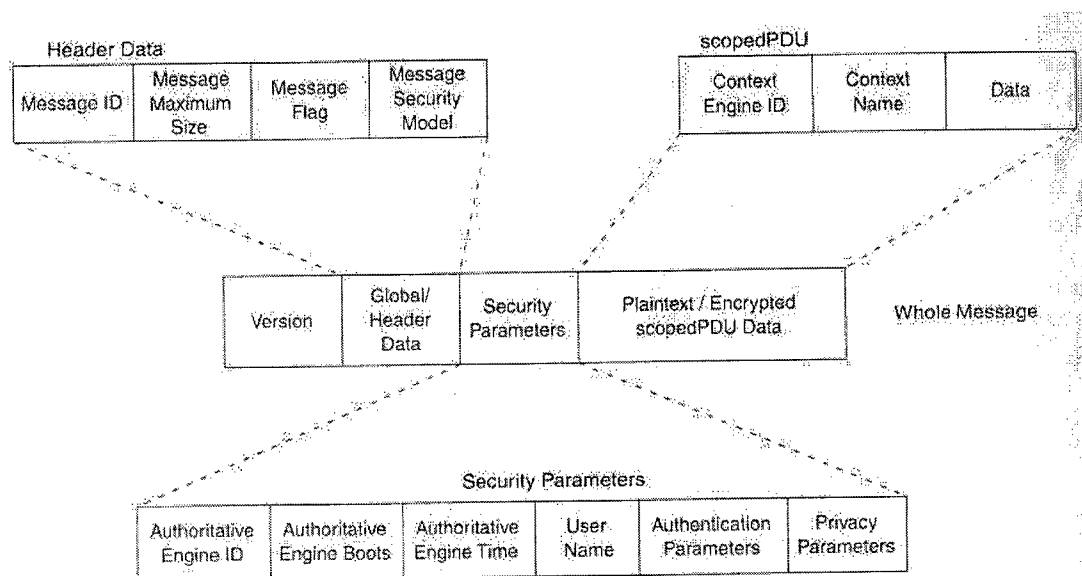


Fonte: Stallings (1999, p.456)

O formato das mensagens SNMPv3 consiste de quatro grupos, mostrados na figura 2.14. O primeiro grupo é um campo simples, que é o número da versão e está na mesma posição que no SNMPv1 e SNMPv2, o subsistema *dispatcher* verifica o número da versão e encaminha para o modelo de processamento de mensagem apropriado. O segundo grupo, denominado *global/header data*, contém parâmetros administrativos da mensagem, incluindo o modelo de segurança utilizado, vários modelos são permitidos. O terceiro grupo contém parâmetros de segurança e é usado pelo modelo de segurança

na comunicação entre entidades. O quarto grupo de dados contém os campos da PDU, conforme da versão do SNMP utilizada, podendo estar criptografado ou em texto claro.

Figura 2.14 – Formato de mensagens SNMPv3



O modelo de segurança do SNMPv3 é um modelo de segurança baseado em usuários (USM – User-based Security Model) que reflete o conceito tradicional de nome de usuários e senhas. A base de segurança no uso de esquemas de autenticação e privacidade são chaves secretas. A chave secreta para autenticação é derivada de uma senha escolhida pelo usuário.

O controle de acesso trata de quem pode acessar os componentes de gerenciamento das redes e o que pode ser acessado. Nas versões anteriores do SNMP, este tópico era coberto pela política de acesso baseada em nomes de comunidade. No SNMPv3 o controle de acesso tornou-se muito mais seguro e flexível pela introdução do modelo de controle de acesso baseado em visão (VACM – View-based Access Control

Model). O VCAM define um conjunto de serviços que uma aplicação em um agente podem usar para validar comandos de requisição e notificação.

2.3.6 O SMON

Um *switch* é um dispositivo de rede utilizado para reduzir a contenção e congestionamento da rede, comumente verificados em redes compartilhadas. Os *switches* permitem também a comutação entre diferentes tecnologias (*ethernet*, *token ring*, *fast ethernet*, etc.). Além disso, é comum a implementação de VLANs (Virtual LAN ou Redes Locais Virtuais) em *switches*, de tal forma que diferentes redes locais possam coexistir em um mesmo equipamento e uma mesma rede local virtual possa ser implementada por vários equipamentos, desde que os mesmos obedeçam a um padrão. Neste sentido foi desenvolvido o padrão de identificação de VLAN IEE 802.1Q.

A principal diferença entre gerenciar uma rede local compartilhada e uma rede com *switches* é o nível de granularidade necessário. Em redes tradicionais o monitoramento de performance, segurança e contabilização pode ser feito monitorando-se uns poucos pontos na rede por onde flui o tráfego. Em redes que utilizam *switches*, cada *switch* contém vários segmentos de rede, o que aumenta enormemente o número de pontos onde se faz necessário o monitoramento.

Para contornar os problemas gerados pela excessiva segmentação de redes baseadas em *switch*, pela implementação de priorização de tráfego e também pela criação de VLANs, foi definido no RFC 2613 um padrão que estende o RMON para

adequá-lo melhor ao gerenciamento de redes com *switch*, este padrão foi inicialmente definido pela Lannet e denominado de SMON.

O SMON estende o conceito de fonte de dados, que na MIB II e RMON eram somente instâncias das interfaces, acrescentando VLANs e entidades físicas, conforme definido no RFC 2037, como a sub-árvore 22 do RMON. Dessa forma, os grupos *host* e *matrix* do RMON e seus similares do RMON 2 devem ser estendidos para suportar as novas fontes de dados definidas no SMON.

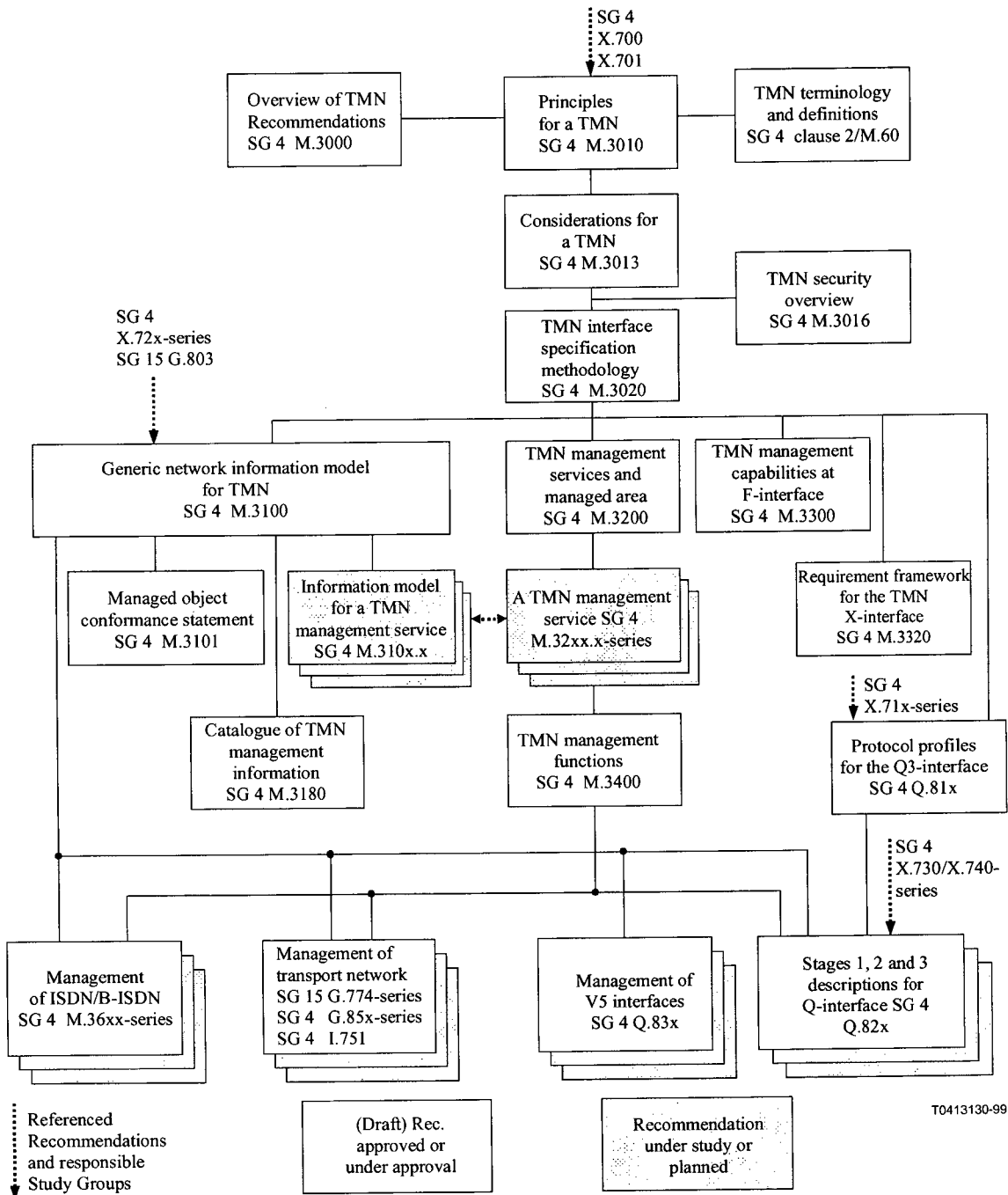
2.4 TMN – Telecommunications Management Network

O conceito básico do TMN é prover uma arquitetura organizada para permitir a interconexão entre diferentes sistemas e equipamentos de telecomunicação, possibilitando a troca de informações de gerenciamento usando uma arquitetura comum com interfaces padronizadas, incluindo protocolos e mensagens.

As recomendações TMN da ITU-T, conhecidas como série M.3000, descrevem os princípios, arquitetura, definições e especificações necessárias para implementar todos os tipos de TMN. A figura 2.15 mostra as recomendações TMN e seus relacionamentos.

Segundo a recomendação M.3000 da ITU-T, todos os tipos de redes de telecomunicação e elementos de rede (e.g. redes analógicas, redes digitais, redes públicas, redes privadas, sistemas de comutação, sistemas de transmissão, software de telecomunicação e recursos lógicos da rede) são passíveis de monitoramento via TMN.

Figura 2.15 – Recomendações TMN



Fonte: Recomendação ITU-T M.3000

Para lidar com a complexidade do gerenciamento de redes de telecomunicações, o gerenciamento foi dividido em vários níveis funcionais. Essa divisão em níveis de funcionalidade implica no agrupamento das funções dos sistemas de telecomunicação em níveis. Os níveis foram definidos como: Negócio, Serviço, Rede e Elemento de Rede:

- ✓ O nível de gerenciamento de elementos de rede é responsável por gerenciar cada elemento de rede de forma individual ou em grupos de elementos correlacionados;
- ✓ O nível de gerenciamento de rede é responsável por gerenciar a rede como um todo, seja ela LAN ou WAN. Neste nível identificam-se quais os recursos estão disponíveis na rede, como eles estão inter-relacionados e distribuídos geograficamente e, finalmente, como eles podem ser controlados;
- ✓ O gerenciamento de serviço é responsável pelos aspectos contratuais de serviços que estão sendo providos aos clientes ou disponíveis para potenciais clientes;
- ✓ O gerenciamento do nível de negócio é responsável pela empresa como um todo. Enquanto as principais funções dos níveis de gerenciamento de serviço e rede dizem respeito a boa utilização dos recursos de telecomunicações existentes, o nível de gerenciamento de negócio se preocupa com a otimização dos investimentos e a utilização de novos recursos.

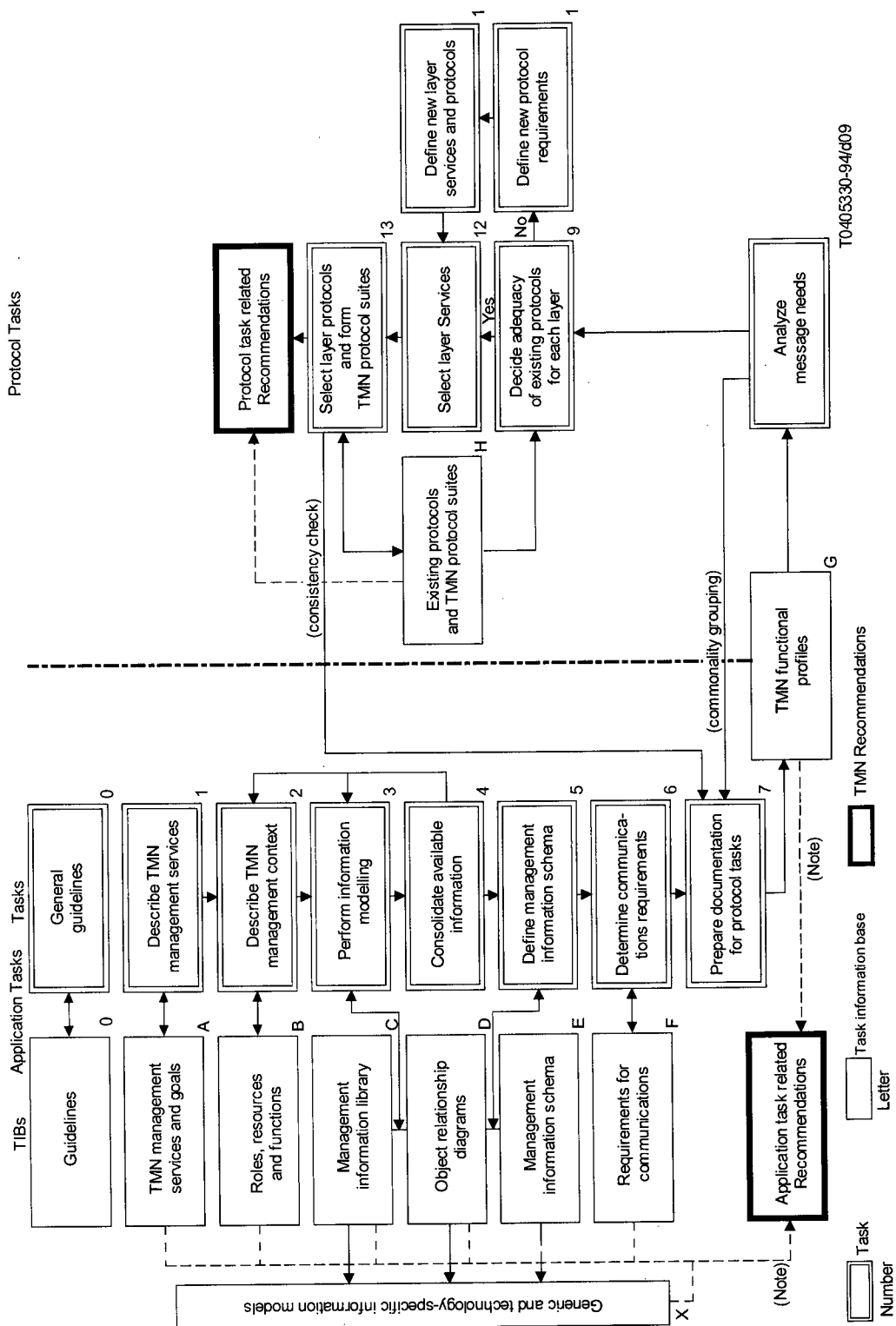
A recomendação M.3010 sugere que a implementação da TMN deve iniciar-se com o gerenciamento de sistemas de operação crítica que provêm as funções mínimas para o funcionamento do negócio e expandir o gerenciamento para incluir todas as funções recomendadas na arquitetura TMN.

A recomendação M.3020 dita que na implementação do gerenciamento de rede é necessário que se levante todas as informações de gerenciamento e operações necessárias para gerenciar a rede como um todo. Segundo esta recomendação, a execução da metodologia nos recursos de telecomunicação escolhidos resulta em um modelo informacional. Este modelo é especificado em termos de classes de objetos gerenciados com atributos associados, ações e notificações. As classes de objeto representam todos os aspectos de gerenciamento necessários dos recursos de telecomunicação escolhidos.

O levantamento do modelo informacional torna claro do ponto de vista dos recursos de telecomunicação quando eles devem enviar mensagens ou responder ao sistema de gerenciamento. Do ponto de vista do sistema de gerenciamento torna-se claro sob quais circunstâncias eventos de notificação serão gerados e como conseguir as informações de gerenciamento. Torna-se também claro qual o tipo de influencia o sistema de gerenciamento tem sobre os recursos de telecomunicação e como controlá-los. Entretanto, a metodologia não especifica como o sistema deveria analisar a informação recebida e como reagir a ela.

A metodologia de especificação de interface TMN, definida na recomendação M.3020 e representada na figura 2.16, é dividida em duas áreas principais de atividades: aplicação e protocolo. Dentro de cada área é definido um conjunto de tarefas, as tarefas 0 a 7 referem-se à área de aplicação, enquanto as tarefas 8 a 13 referem-se à área de protocolo. A definição de cada interface inclui um modelo de objetos e especificações de protocolo que suportam os serviços de gerenciamento TMN.

Figura 2.16 – Metodologia de especificação de interface TMN



NOTE – The dotted lines show possible inputs to TMN Recommendations.

FIGURE 10/M.3020

CAPÍTULO III – SISTEMAS E INFORMAÇÕES DE GERENCIAMENTO

3.1 Ferramentas e Sistemas de Gerenciamento

Um sistema de gerência de rede pode ser definido como um conjunto de processos, procedimentos e atividades que, associados ao uso de técnicas e ferramentas adequadas, permite a observação contínua da rede, coletando e armazenando dados referentes ao seu funcionamento. Uma rede deve ser observada não somente para direcionar o seu crescimento e desenvolvimento, mas para mantê-la em funcionamento sempre nas melhores condições possíveis. (Reiter 1997, p.6)

Um bom projeto de gerenciamento de redes pode ajudar a organização a alcançar metas de disponibilidade, desempenho e segurança. Os processos de gerenciamento de rede efetivos podem ajudar toda a organização a medir como estão sendo atendidas as metas de projeto e a ajustar os parâmetros da rede, se as metas não estiverem sendo satisfeitas. A administração de rede também auxilia as metas de facilidade de escalonamento, porque pode ajudar a organização a analisar o comportamento atual da rede, aplicar atualizações de forma adequada e solucionar quaisquer problemas com atualizações.

Alguns aspectos significativos devem ser observados na implantação da gerência da rede: a coleta de dados deve ser representativa, a monitoração deve ser contínua, o tráfego das informações de gerenciamento não deve aumentar significativamente o tráfego de rede e o agente do protocolo no dispositivo gerenciado não deve aumentar significativamente o resultado de processamento a ponto de prejudicar a função principal daquele dispositivo.

As atividades básicas do gerenciamento de redes consistem na detecção e correção de falhas, em um tempo mínimo, e no estabelecimento de procedimentos para a previsão de problemas futuros. A eficiência na realização destas tarefas está diretamente ligada à existência de ferramentas que as automatizem e de pessoal qualificado. Atualmente, existem no mercado diversos tipos de ferramentas que auxiliam o administrador nas atividades de gerenciamento. Estas ferramentas podem ser divididas em quatro categorias:

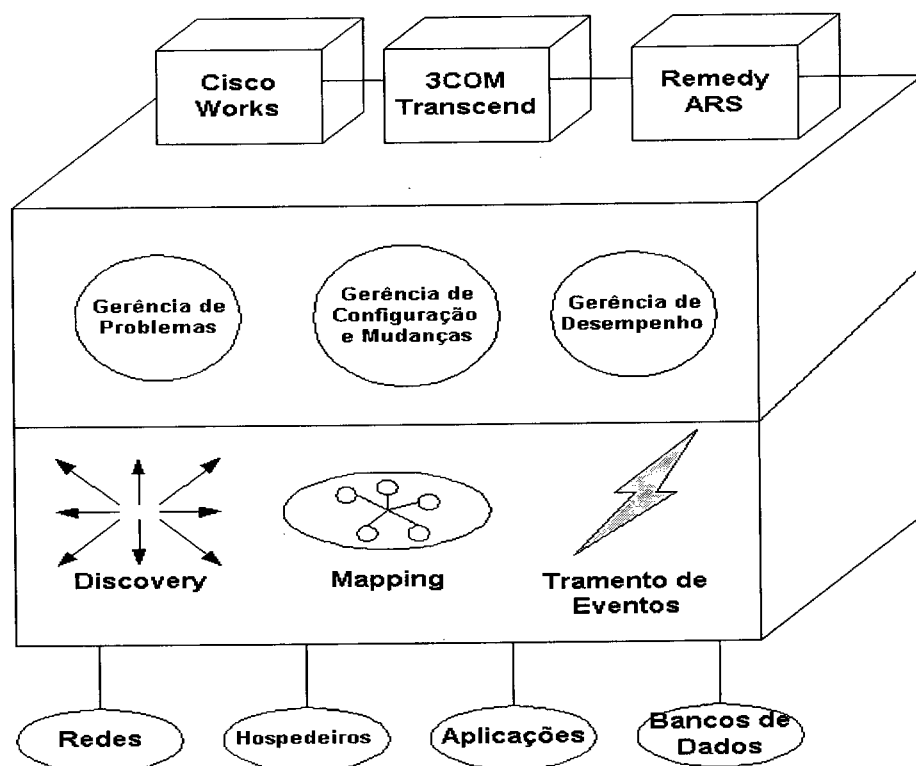
- ✓ ferramentas a nível físico, que detectam problemas em termos de cabos e conexões de hardware;
- ✓ monitores de rede, que se conectam as redes, monitorando o tráfego;
- ✓ analisadores de rede, que auxiliam no rastreamento e correção de problemas encontrados nas redes; e
- ✓ sistemas de gerenciamento de redes, os quais permitem o monitoramento e controle de uma rede.

Os sistemas de gerenciamento de redes apresentam a vantagem de ter um conjunto de ferramentas/aplicações integradas para análise e depuração da rede, através de uma única interface gráfica baseada em janelas, incluindo funções de

descoberta da rede e gerenciamento de configuração . Estes sistemas podem apresentar também uma série de mecanismos que facilitam a identificação, notificação e registro de problemas, por exemplo:

- ✓ alarmes que indicam, através de mensagens ou bips de alerta, anormalidades na rede;
- ✓ geração automática de relatórios contendo as informações coletadas;
- ✓ facilidades para integrar novas funções ao próprio sistema de gerenciamento;
- ✓ suporte a MIBs estendidas;
- ✓ geração de gráficos estatísticos em tempo real; e
- ✓ apresentação gráfica da topologia das redes.

Figura 3.1 – Arquitetura de um Sistema de Gerenciamento de Redes

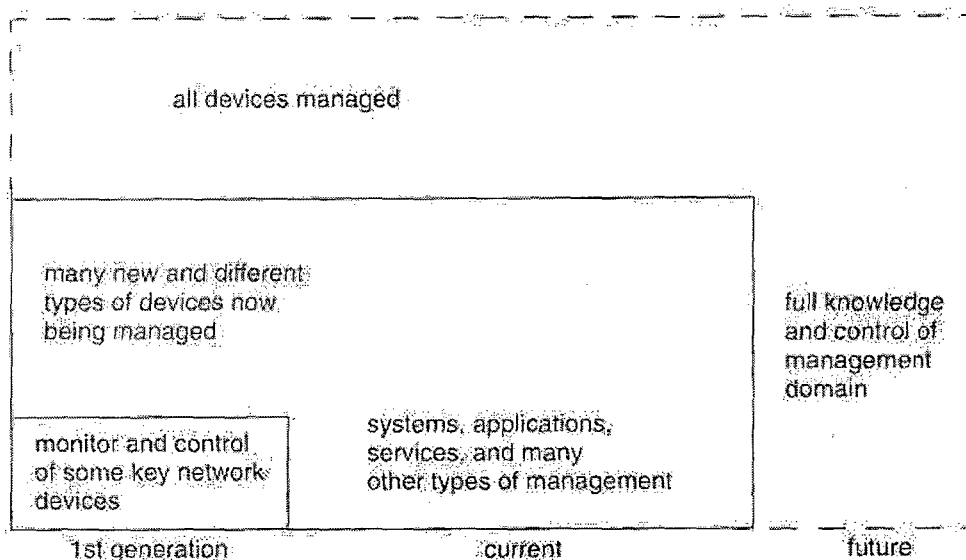


Serviços e aplicações adicionais, tais como distribuição de *software*, *trouble ticketing*, gerenciamento baseado em políticas, processamento avançado de alarmes, correlação de eventos, utilização de inteligência artificial e simulação da rede, podem também fazer parte da plataforma de gerenciamento implementada. Sistemas de gerenciamento podem ter vários níveis diferentes de *expertise*, desde aqueles que somente recuperam e armazenam informações em uma base de dados, passando por outros que executam ações, baseados em dados coletados sem intervenção humana e chegando àqueles que agem, como se fossem um ser humano, encontrando, isolando problemas e sugerindo modificações.

Alguns requisitos devem ser considerados na aquisição e implementação das ferramentas de gerência de rede: utilização de padrões, escalabilidade, flexibilidade, gerenciamento de serviços, integração, interoperabilidade, possibilidade de cruzamento de dados, visualização de dados de maneira integrada e centralizada e possibilidade de extração de dados para estabelecimento de *baseline*.

A figura 3.2 mostra a evolução dos sistemas de gerenciamento de redes, proposta por Hardeny (1997, p.7), iniciando com as ferramentas *ad-hoc* para gerenciamento de equipamentos específicos, passando pelo estágio de sistemas e aplicações de gerenciamento que monitoram vários tipos de equipamentos e inclui diferentes tipos de gerenciamento e finalmente chegando aos sistemas que gerenciam toda a rede e serviços e que possui ferramentas com inteligência artificial para identificação de problemas, aprendizado e tomada de decisões.

Figura 3.2 – Evolução dos sistemas de gerenciamento de redes



3.2 Público Alvo das Informações de Gerenciamento

Não basta monitorar, coletar e tratar um grande número de informações se elas não são analisadas, publicadas ou se não chegam aos seus eventuais interessados. O grupo de gerência de rede não é o único interessado nas informações de gerência. A divulgação de informações traz inclusive credibilidade, sendo preferível a utilização de representação gráfica. (Reiter, 1997, p.51).

Quanto à forma de divulgação pode ocorrer variação em função do público alvo. Segundo Subramanian (2000, p.44), parte da função de gerenciamento inclui a geração de relatórios adequados enviados às pessoas certas. Existem, em geral, três classes de relatórios: sistemas, gerenciamento e usuários. Os relatórios relativos à área de gerenciamento de redes podem ser divididos em três categorias:

- ✓ relatórios de planejamento e gerenciamento – mantêm informações de gerenciamento de mais alto nível e verificação de níveis de serviço, além disso, são úteis para propósitos de planejamento e alocação/justificativa de custos;
- ✓ relatórios de sistema – são mais direcionados para gerência da rede e auxiliam na verificação de seu funcionamento e em ajustes da rede; e
- ✓ relatórios de usuários – devem manter informados os usuários a cerca de quão bem atingidos estão os níveis de serviço acordados.

O quadro a seguir separa os relatórios em categorias destinados a cada público alvo, enumerando alguns relatórios que se enquadram na categoria.

Quadro 3.1 – Relatórios de Gerenciamento de Redes por Público Alvo

Planejamento e gerenciamento	Relatórios
Qualidade de serviço – SLA	. disponibilidade de rede e sistemas . problemas ocorridos . satisfação do usuário
Análise de tráfego	. padrão de tráfego . análise de volume de tráfego interno e externo
Tendências tecnológicas	. estado atual . projeção de tendências
Custos operacionais	. custos fixos e variáveis . custos de pessoal . outros custos
Operacionais/Sistemas	Relatórios
Tráfego	. carga interna e externa – detalhado
Falhas	. falas na rede e sistemas – detalhado
Performance	. de rede, aplicações e servidores
Usuários	Relatórios
SLA	. disponibilidade de serviços . carga de tráfego . performance
Customizados	. relatórios definidos para usuários específicos

Além de informações diferenciadas, o próprio conceito do o gerenciamento de redes pode significar coisas diferentes para diferentes pessoas na organização. Para o

CIO o gerenciamento de rede é a habilidade de balancear os requisitos crescentes dos usuários com a quantidade decrescente de recursos, que é a habilidade de prover mais serviços com menos dinheiro. (Miller, 1997, p.3)

3.3 Estabelecimento de *Baseline*

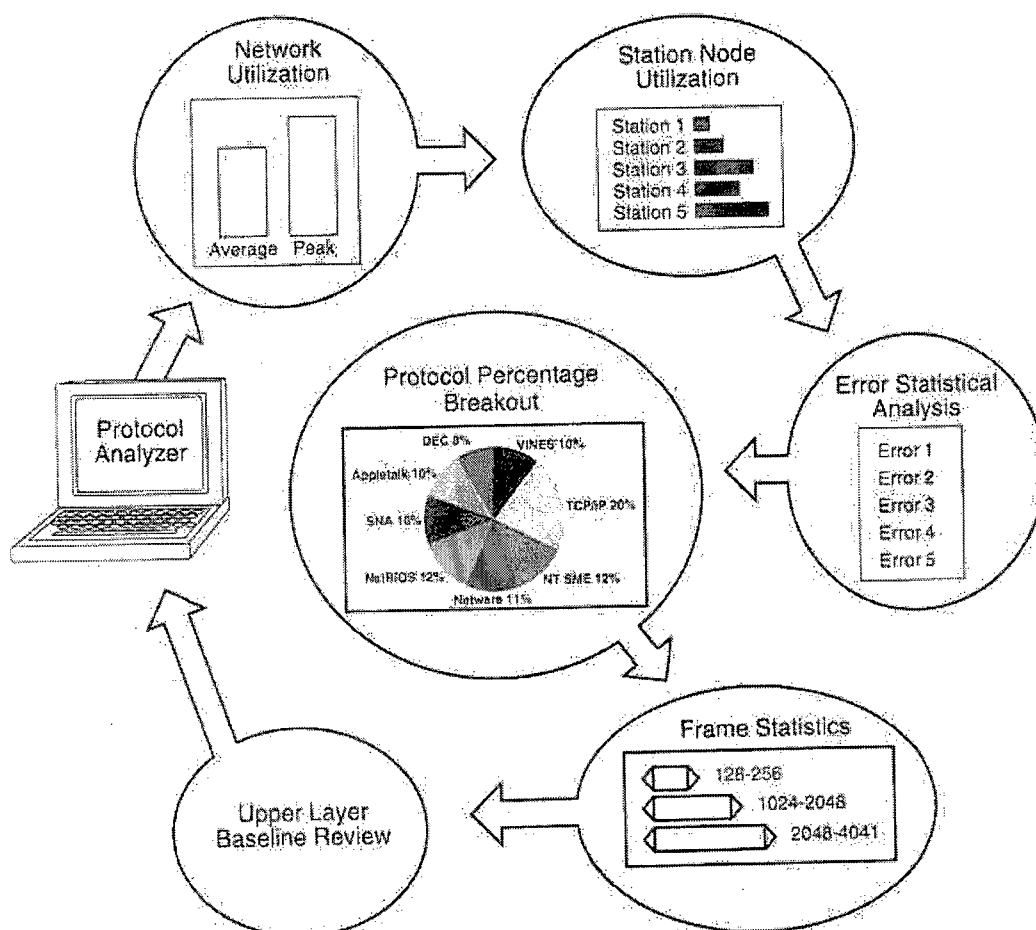
O estabelecimento de *baseline* é o processo de utilização de sistemas de gerenciamento e ferramentas de análise de protocolo com o propósito de estabelecer um padrão de comportamento da rede sobre um período de tempo específico. É importante salientar que o levantamento de dados deve ser feito no período de utilização real da rede. Arnett (1997, p.197) sugere que este levantamento seja feito por alguns dias (no mínimo 15) e que sejam encontrados os valores médios para diferentes períodos do dia.

É importante conhecer o comportamento normal da rede – *baseline*. Este conhecimento é essencial para resolver problemas de performance, tais como usuários reclamando que a rede está lenta. Conhecendo-se o comportamento normal da rede pode-se verificar as mudanças ocorridas em função de disponibilização de novos serviços ou mudança de comportamento da rede que possa trazer problemas para sua utilização.

Um projeto de estabelecimento de *baseline* de rede deve incluir três estágios principais: planejamento do estudo do *baseline*, aquisição dos dados e estabelecimento do *baseline* e composição e construção do relatório de *baseline* da rede.

Quando estiver fazendo o projeto do estabelecimento do *baseline* deve-se procurar levantar todos os dados relevantes ao funcionamento e arquitetura da rede, incluindo topologias e protocolos, sistemas operacionais e serviços utilizados. No primeiro estágio deve-se também levantar um histórico de problemas ocorridos. Depois de levantados todos os dados, deve ser feito um projeto que deve incluir pontos de monitoração, ferramentas e objetivos: o quê, como, onde, para quê e por quanto tempo monitorar. A figura 3.3 mostra as principais medidas que são executadas na rede para estabelecimento de *baseline* em rede.

Figura 3.3 – Principais medidas no estabelecimento de baseline de redes



O projeto pode variar dependendo se o levantamento do *baseline* tem uma finalidade de estabelecer o padrão de uma rede que não está apresentando problemas (estudo pró-ativo) ou se está sendo feito devido a problemas identificados na rede (estudo reativo). Se o processo de estabelecimento de *baseline* é pró-ativo, a medida deve ser feita em toda a rede. Se o processo é reativo, deve-se identificar os melhores pontos onde se fazer a amostragem. (Nassar, 2000, p.665)

3.4 Acordo de Nível de Serviço - SLA

O objetivo maior do gerenciamento de redes é garantir que os usuários tenham acesso aos serviços de que necessitam com a qualidade esperada. A fim de alcançar estes objetivos, o gerenciamento deveria estabelecer uma política para, formalmente ou informalmente, contratar um SLA (*Service Level Agreement*) com os usuários. Subramanian (2000, p.552) define o SLA como um contrato entre o provedor de serviço e o cliente especificando os serviços a serem providos e a qualidade prometida, dessa forma, o SLA é um processo de:

- ✓ identificar os serviços e características associadas a eles;
- ✓ negociar um SLA, que normalmente inclui tempo de resposta, disponibilidade, *downtime* e MTTR;
- ✓ utilizar agentes para monitorar e controlar a performance da rede, sistemas e aplicações; e
- ✓ produzir relatórios de nível de serviço.

Gerentes de rede se beneficiam do SLA de várias formas. Comparando a performance real da rede com a especificada pelo SLA, os gerentes podem obter uma visão adequada do sucesso em alcançar os objetivos. Gerentes gastam menos tempo justificando custos de rede para os usuários e torna-se mais claro justificar a aquisição de novos produtos e serviços. Orçamentos são mais fáceis de ser justificados e investimentos são feitos de acordo com objetivos do negócio.

O estabelecimento de SLA não beneficia somente os gerentes de rede, os usuários vêem melhorias em três áreas: reatividade da área de informática, serviços direcionados para aplicações críticas e controle de custo. Finalmente, os gerentes de TI se beneficiam pela melhoria de avaliação de recursos, relacionamento com usuários finais e justificação de investimentos.

Métricas para estabelecimento de SLA podem ser divididas em duas categorias: externa e interna. Métricas externas incluem dados compartilhados com e entendidos pelos usuários (e.g. disponibilidade, tempo de resposta) e referem-se a suas expectativas com relação à rede. Métricas internas são tipicamente causas de problemas e podem incluir congestionamento, taxas de erro e erros de sistema. Normalmente usadas somente na área de informática, estas métricas podem indiretamente afetar os objetivos dos usuários, mas não são diretamente relacionadas aos objetivos do negócio. Deve-se ressaltar que os usuários estão preocupados com tempo de resposta e disponibilidade, *jitter*, retardo e tamanho de pacotes nada significam para eles.

Dois fatos importantes devem ser considerados no estabelecimento de SLA:

- ✓ a implementação de um SLA não tem que ser um esforço descomunal que abranja toda a organização. É inteiramente aceitável, e ainda assim com benefícios significativos, que se inicie com um único departamento ou aplicação;
- ✓ a área de informática deve manter-se no papel de provedor de serviço, definindo o que é e o que não é possível tecnicamente. Ela não deveria assumir a posição de árbitro estabelecendo objetivos e prioridades.

3.5 Gerenciamento de Performance

A maioria dos produtos disponíveis para gerenciamento de redes e sistemas tem provado ser inadequada à tarefa de gerenciamento de performance. Estes produtos estão primariamente preocupados com a emissão de relatórios de estados e com a identificação e resolução de problemas, o que significa apagar incêndio. Estas ferramentas geralmente não têm facilidades no sentido de geração de relatórios de performance, o que é crítico no estabelecimento do *baseline* e na verificação se as expectativas de performance estão sendo atendidas.

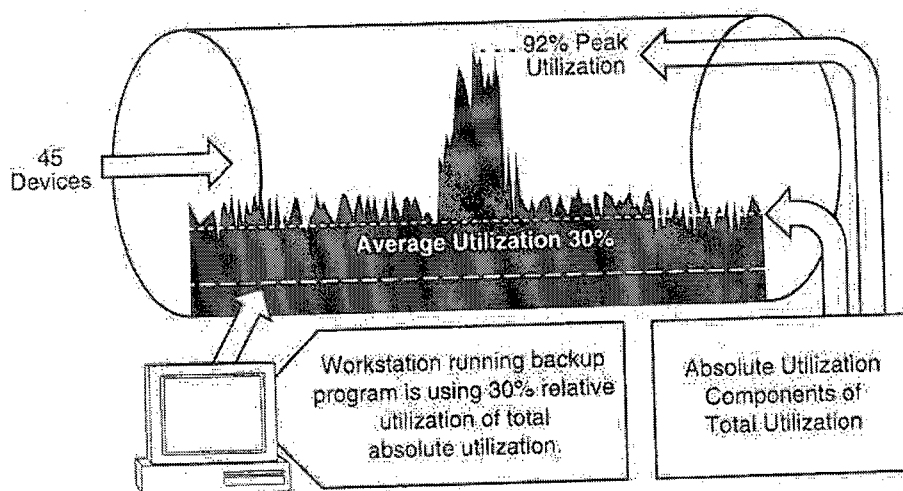
Um pré-requisito absoluto para gerenciamento de redes de comunicação é a habilidade de medir a performance da rede. Uma das dificuldades encontradas pelo administrador de redes é a seleção e uso de indicadores apropriados para mensurar a performance. Dentre os problemas encontrados para medir o desempenho da rede pode-se citar:

- ✓ grande número de indicadores;

- ✓ o significado da maioria dos indicadores não é claramente entendida;
- ✓ alguns indicadores são introduzidos e suportados por apenas alguns fabricantes;
- ✓ a maioria dos indicadores não serve para comparação com outros;
- ✓ freqüentemente são medidos corretamente, mas interpretados erroneamente; e
- ✓ em alguns casos o cálculo de indicadores leva tanto tempo que o resultado final dificilmente pode ser utilizado para controlar o ambiente.

Segundo Rocha (1996, p.31), uma das principais atividades da gerência de desempenho é auxiliar os técnicos e administradores de rede no planejamento da capacidade, de maneira a oferecer a seus usuários um nível satisfatório de serviços. Com o uso da gerência de desempenho, o gerente de rede pode monitorar a utilização dos dispositivos e enlaces, sendo possível isolar problemas de desempenho com a finalidade de resolvê-los antes que esses impliquem maior impacto. É importante levantar os valores de pico e média de utilização, conforme figura 3.4, bem como os horários de pico e uma análise histórica de utilização para identificação de tendências.

Figura 3.4 – Valores de pico e média de utilização de circuitos de comunicação

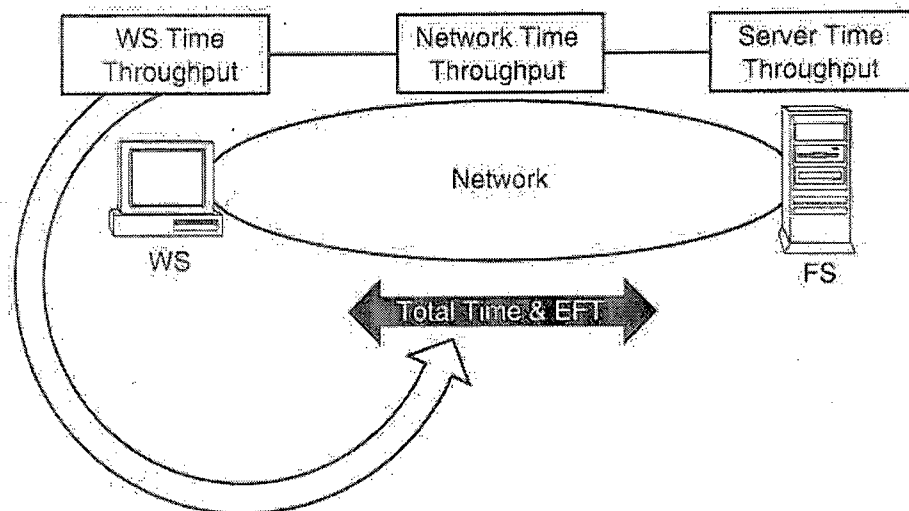


Se a performance não pode ser adequadamente medida e confrontada com os requisitos de negócio, torna-se difícil mostrar que os investimentos em rede se pagam e que trazem melhorias em termos de disponibilidade, tempo de resposta e aumento de produtividade.

Stallings (1999, p.5) aponta algumas perguntas que podem ser respondidas pelo gerenciamento de desempenho: o tráfego está distribuído uniformemente entre os usuários ou está concentrado em pares origem e destino com tráfego excessivamente pesado? qual a percentagem de cada tipo de pacote? qual a distribuição dos pacotes por tamanho? qual o *delay* dos *links* de comunicação? a taxa de colisões está atrapalhando o desempenho da rede? qual a utilização e *throughput* dos canais? qual o efeito do aumento de tráfego na utilização do *throughput* e *delay*? quando a carga da rede começa a degradar a performance? qual a máxima utilização da rede em condições normais e o que é necessário para passar este limiar? pacotes grandes melhoram ou pioram a performance da rede? como a mudança de técnicas de enfileiramento afeta a performance?

Além da medição do *delay* dos *links* de comunicação, é também importante medir a vazão dos links, uma vez que esta característica afeta diretamente a performance das aplicações em rede. O EFT (*Effective File Throughput*) é definido como o tempo que se gasta para transmitir uma certa quantidade de informação. Necessariamente os *links* que apresentam *delay* alto não são ruins; por exemplo, os satélites possuem *delay* elevado e podem ter uma vazão também elevada.

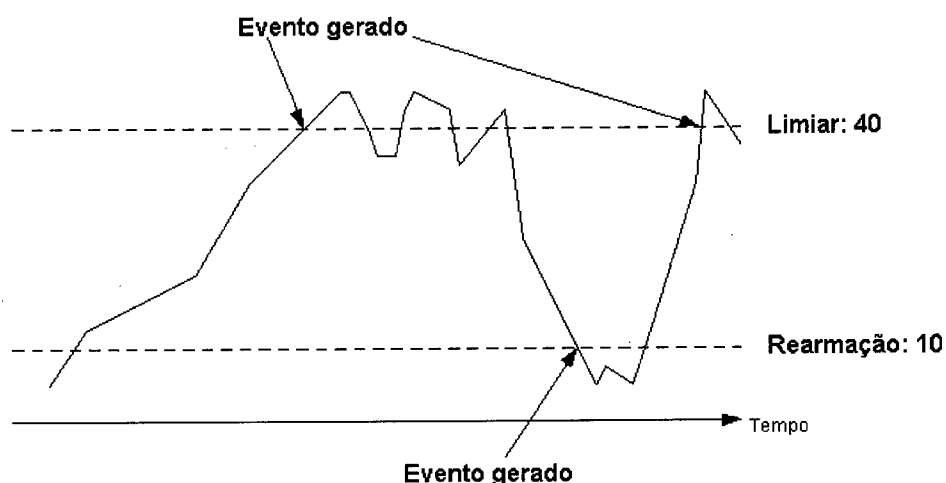
Figura 3.5– Levantamento de taxa de transferência efetiva (EFT)



Fonte: Nassar (2000, p.33)

Deve-se determinar também, quando um dispositivo está operando corretamente e as características de falha de cada equipamento, estabelecendo-se os *thresholds* de cada dispositivo. O RMON definiu um mecanismo, denominado de mecanismo de histerese, que evita a geração de um número excessivo de alarmes na rede com pequenas flutuações próximas aos limiares. Pode-se pensar no mecanismo de histerese como um mecanismo contendo dois estados: estado de alarme de subida e estado de alarme de descida. Quando está em estado de alarme de subida, o alarme de descida está desabilitado, ou seja, só será gerado um alarme se um valor definido como limiar de subida for ultrapassado. Quando está em estado de alarme de descida, o alarme de subida está desabilitado, ou seja, só será gerado um alarme se um valor menor que o limiar de descida for atingido.

Figura 3.6 – Mecanismo de histeresse RMON



Problemas de performance de rede podem causar dois tipos de queda de produtividade. O primeiro tipo denominado “*hard downtime*” ocorre quando falhas físicas ou de equipamentos causam parada de serviço. O segundo tipo denominado “*soft downtime*” ocorre quando o mau funcionamento da rede causa degradação das aplicações.

O “*soft downtime*” ou degradação de serviço é menos catastrófico em sua natureza, mas ocorre com mais frequência do que a interrupção do serviço. A degradação de serviço e conseqüente perda de produtividade custa às organizações duas vezes mais, segundo a Infonetics, do que a interrupção dos serviços. A degradação de serviços ocorre com mais frequência, é mais difícil de ser detectada e medida e causa mais danos.

O planejamento requerido para proativamente evitar o *downtime* recebe menos atenção dos gerentes de rede, pois os mesmos consomem a maior parte de seu tempo

consertando problemas urgentes que afetam a disponibilidade da rede. Devido a seu enfoque em manter a rede funcionando, eles não dispõem de recursos e tempo para antecipar problemas e tomar medidas pró-ativas para evitá-los. Conseqüentemente, a maioria dos gerentes de rede não pode garantir níveis de performance em suas redes.

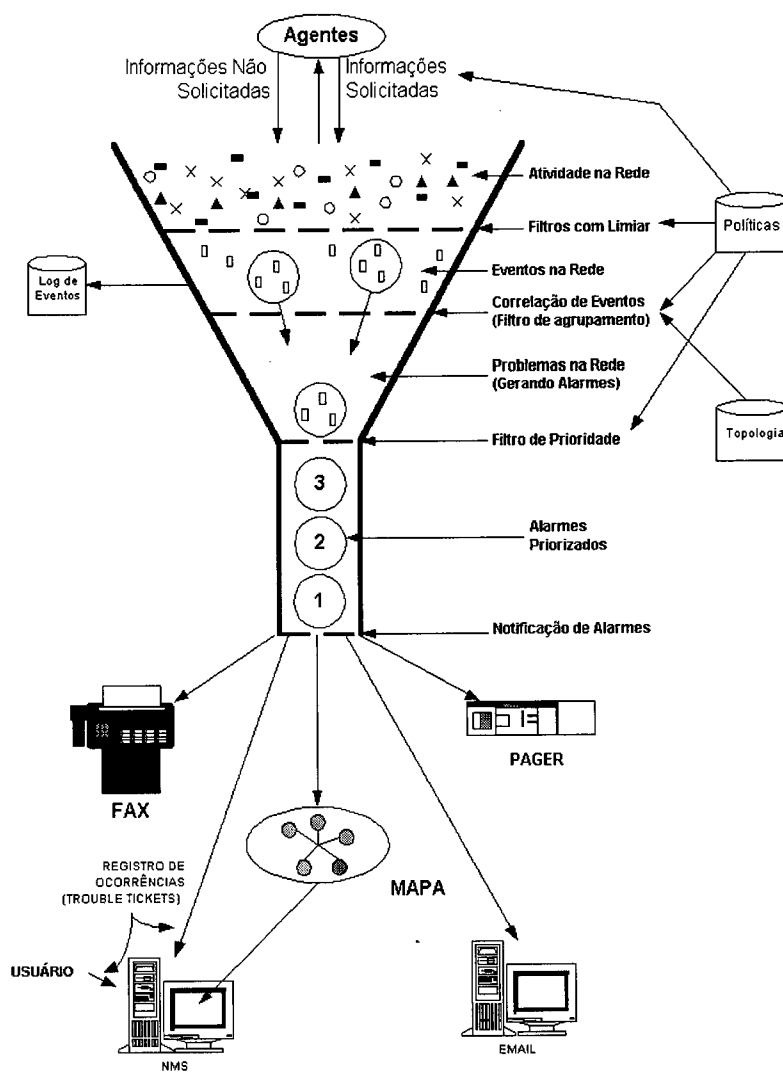
3.6 Controle Operacional de Redes – NOC

O RFC 1297 define o *Network Operational Control* (NOC) como uma coleção de atividades requeridas para manter dinamicamente o nível de serviço em uma rede ou conjunto de redes. Estas atividades asseguram alta disponibilidade de recursos pelo rápido reconhecimento de problemas e degradação de performance, disparando funções de controle quando for necessário. O sistema de monitoração gera alertas e tendências do perfil de tráfego da rede. O sistema de coletas quando olha problemas atua na área de gerência de falhas, quando verifica performance/utilização da rede atua como gerência de desempenho

Para verificar o se o nível de serviço atual corresponde ao desejado, informações são extraídas da rede para obter a funcionalidade e performance em tempo real. As informações são extraídas continuamente ou sob demanda e armazenadas no banco de dados da gerência da rede. Estes dados são submetidos à análise para verificar se o *status* real da rede corresponde ao desejado. Análises podem ser feitas com relação ao tempo médio entre falhas (MTBF - *Mean Time Between Failures*) e tempo médio para reparo (MTTR - *Mean Time To Repair*) dos dispositivos e serviços de rede, e conseqüentemente de disponibilidade que pode ser calculada em função das duas

medidas anteriores (disponibilidade = $MTBF / (MTBF + MTTR)$). A disponibilidade expressa o percentual de tempo que um sistema componente ou aplicação de rede fica disponível para o usuário.

Figura 3.7 – Mecanismos de geração de alertas



A utilização de um Sistema de Registro de Problemas (*Trouble Ticket System*) auxilia o NOC no diagnóstico do problema e permite criar um banco de dados de experiência com problemas, viabilizando a utilização de sistemas especialistas para a

solução dos problemas ou mesmo a resolução mais rápida de um problema que já tenha acontecido no passado ou que tenha havido um caso similar.

A integração das ferramentas de gerenciamento com o sistema de TTS, a automatização de ações e a utilização de sistemas especialistas diminuem bastante o *downtime* e o MTTR da rede.

No próximo capítulo serão apresentadas a estratégia proposta para implementação do gerenciamento e a rede em que a estratégia será aplicada.

CAPÍTULO IV – ESTRATÉGIA PROPOSTA PARA IMPLEMENTAÇÃO DO GERENCIAMENTO

4.1 Apresentação da Estratégia

Stallings (1999, p.23) sugere que o monitoramento de redes consiste em três grandes áreas:

- ✓ Acesso à informação – definir a informação a ser monitorada e como obter a informação do recurso pelo gerente;
- ✓ Projeto de mecanismos de monitoramento – definir a melhor forma de obter a informação dos recursos;
- ✓ Aplicação da informação de monitoramento – como utilizar a informação obtida pelo gerente sobre os recursos monitorados.

No processo de definição da informação a ser monitorada, uma boa alternativa é utilizar o conceito de identificação de hierarquias. Uma classificação em três níveis pode ser utilizada para monitoração dos equipamentos de rede:

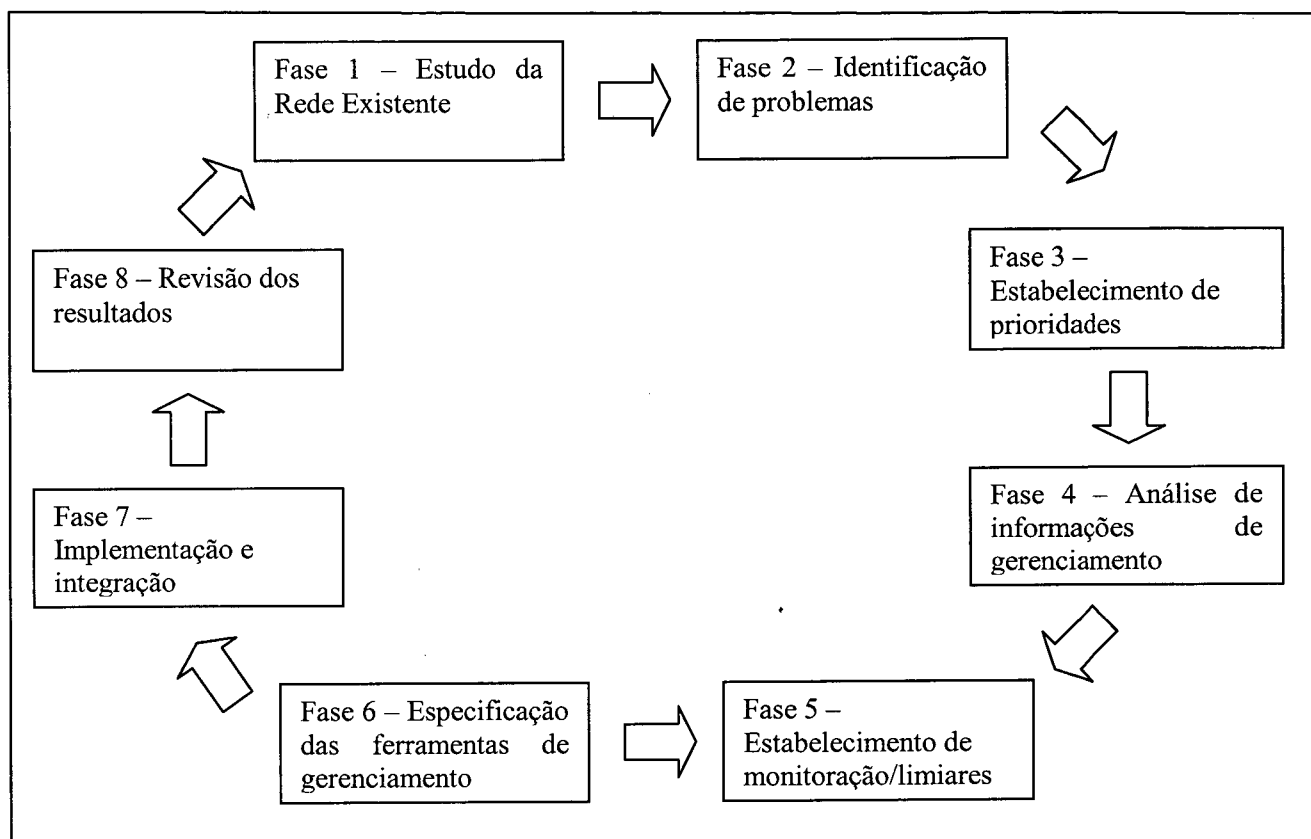
- ✓ o primeiro nível seria o correspondente aos recursos chave, tais como *clusters* de servidores, *backbones* e *links* de WAN. Se estes recursos estiverem fora do ar podem trazer sérios problemas à companhia, pois são considerados recursos de missão crítica. Eles requerem monitoramento contínuo e redundante.

- ✓ o segundo nível seria o dos recursos importantes, tais como servidores de e-mail e intranet. Se um recurso importante fica fora por uma hora, a produtividade na empresa fica prejudicada e o problema piora com o tempo. Esses recursos requerem monitoramento contínuo.
- ✓ o terceiro nível seria o dos recursos não críticos, tais como estações de trabalho. Estes recursos não precisam ser monitorados.

Diferentes autores sugerem diferentes estratégias para construir um sistema de gerenciamento de redes. Enquanto o TMN adota um enfoque *top-down* visualizando o gerenciamento de redes a partir dos serviços disponibilizados e estabelecendo uma política de gerenciamento antes mesmo da implementação da rede. A estratégia proposta, esboçada na figura 4.1, adota um enfoque *bottom-up* iniciando pelo monitoramento dos principais equipamentos de rede.

A diferença do enfoque resulta do fato de que, normalmente, as redes são implementadas ou crescem demasiadamente sem que haja tempo, dinheiro ou vontade política de implementação do gerenciamento. A estratégia proposta neste trabalho destina-se à implementação de gerenciamento em redes de computadores já implementadas e operacionais. Por este motivo a primeira fase é o estudo da rede existente, envolvendo a topologia física e lógica da rede, serviços disponibilizados e expectativa de crescimento.

Figura 4.1 – Estratégia proposta para implementação do gerenciamento



Depois de efetuado o estudo da rede, faz-se necessário identificar quais os principais problemas que ocorrem na rede ou que se ocorrerem afetam fortemente os usuários. Na fase 2 propõe-se a identificação destes problemas e dos requisitos dos usuários com relação à rede. Nesta fase pode ser necessário até mesmo a utilização de questionários submetidos aos usuários para o levantamento de informações.

Embora a estratégia proposta não fale em gerenciamento de serviços, o estabelecimento de prioridades, proposto na fase 3, é feito com base nos serviços críticos disponibilizados na rede levando-se em consideração que a rede já está operacional e que o responsável pela rede reconhece ou pode levantar com relativa facilidade quais são os serviços mais críticos. Caso o responsável pela rede não tivesse

este conhecimento previamente, ele teria sido adquirido através dos levantamentos efetuados na fase 2.

O conhecimento da rede também é importante na análise de informações de gerenciamento disponibilizada pelos equipamentos, definida como fase 4 da estratégia proposta. Dentre todas as informações acessíveis é necessário levantar quais são aquelas que podem fornecer informações relevantes para o gerenciamento. Esta fase assemelha-se ao levantamento do modelo informacional definido na recomendação M.3020 da ITU-T.

Conhecendo-se as informações disponibilizadas pelos equipamentos e selecionadas as informações relevantes, deve-se estabelecer como fazer o monitoramento e como transformar essas informações em uma forma inteligível para os usuários dos diversos níveis, sejam eles administradores de rede, usuários finais ou gestores. Na fase 5, além de definir como fazer o monitoramento é feito o levantamento do comportamento normal da rede (*baseline*) e a identificação de limiares (*thresholds*), quando aplicável, para os valores monitorados.

Na fase 6 é feita a especificação funcional das ferramentas de gerenciamento e a seleção da plataforma de integração, considerando o atendimento aos serviços e/ou facilidades para o desenvolvimento de aplicações que proporcionem o seu atendimento. A preocupação inicial nesta fase deve ser com a funcionalidade e posteriormente buscar no mercado quais as ferramentas atendem a estes requisitos, não perdendo de vista o orçamento disponível, uma vez que existem ferramentas nos mais diversos níveis de preço, de *freeware* a ferramentas de custo bastante elevado.

Depois de adquiridas as ferramentas, na fase 7 é feita a instalação, configuração e integração das ferramentas, deve-se revisar os resultados alcançados, fase 8, reiniciando o ciclo de implementação do gerenciamento. Pode-se optar pela implementação do gerenciamento de forma gradativa, adquirindo-se e implementando-se primeiramente o considerado mais urgente e adotando-se uma abordagem evolutiva ampliando-se o gerenciamento. Isto muitas vezes é necessário até mesmo para mostrar um resultado efetivo da implementação do gerenciamento de forma a justificar mais investimentos na área.

No capítulo 5, que descreve a implementação da proposta na rede do TCU, as fases propostas para o estabelecimento do gerenciamento são explicadas em maiores detalhes, ao mesmo tempo em que é explicado como ocorreu a execução de cada fase.

Muito embora a estratégia esteja altamente focada na rede do TCU, ela serve como referência para implementação de gerenciamento em qualquer rede que já esteja instalada e operacional. No caso de redes não instaladas o ideal seria o estabelecimento de uma política de gerenciamento antes da instalação da rede e que a implementação do gerenciamento junto com a instalação da rede.

4.2 Opções de implementação

Várias decisões devem ser tomadas no sentido de implementar a solução de gerenciamento escolhida:

- ✓ Gerenciamento *in-band* x *out-of-band* – o gerenciamento é denominado *in-band* quando usa a mesma rede de tráfego de dados para executar o gerenciamento, enquanto no gerenciamento *out-of-band* uma rede diferente é utilizada para tráfego

de informações de gerenciamento. O modelo SNMP geralmente impõe uma leve carga no mecanismo de transporte, e, desse modo, uma abordagem de gerenciamento *in-band* mostra-se eficiente e fornece alto desempenho. Entretanto, se o caminho de transporte entre uma aplicação agente e uma aplicação gerente não está operacional, será impossível diagnosticar e recuperar um problema sem a intervenção externa, o que não ocorreria no gerenciamento *out-of-band*. O principal fator que dificulta a adoção de uma abordagem de gerenciamento *out-of-band* é o custo de implementação;

- ✓ Gerenciamento centralizado x distribuído – no gerenciamento centralizado uma estação de gerenciamento é responsável pelo levantamento de informações de gerenciamento de toda a rede, enquanto que, no gerenciamento distribuído, várias estações desempenham esta função, sendo interessante a realização de medição na extremidade mais próxima da estação gerente. A abordagem distribuída oferece vários benefícios: o *overhead* gerado pelo tráfego de gerenciamento é minimizado, principalmente na rede WAN, aumento da escalabilidade, permitindo que estações menores gerenciem partes da rede e inexistência de ponto único de falha. Probes RMON e comunicação gerente-gerente implementada no SNMPv2 facilitam bastante a implementação de gerenciamento distribuído de forma eficaz;
- ✓ Gerenciamento pró-ativo x reativo – o gerenciamento reativo ocorre quando o gerente da rede reage a problemas que já aconteceram, enquanto o gerenciamento pró-ativo tenta antever os problemas e solucioná-los antes mesmo que eles causem problemas aos usuários da rede;
- ✓ Utilização de MIBs padrão x proprietárias – Vários fabricantes desenvolvem MIBs proprietárias porque precisam de objetos específicos para seus equipamentos que

podem não estar definidos ou disponíveis em MIBs padrão (Maxell, 2000), portanto pode-se, normalmente, obter mais informações das MIBs proprietárias do que das MIBs padrão. Além disso, MIBs proprietárias não precisam se tornar padrão, desde que somente o fabricante e seus clientes precisam acessar a MIB. Só faz sentido desenvolver uma MIB padrão quando vários fabricantes podem implementar a mesma coleção de MIBs em um grande número de equipamentos.

4.3 Efetividade do Gerenciamento

Reiter sugere algumas perguntas que devem ser feitas posteriormente à implementação da solução de gerenciamento para verificar sua efetividade:

- ✓ O processo de monitoração é adequado?
- ✓ Os dados coletados estão sendo suficientes e efetivos (atingem os interessados)?
- ✓ Que novas facilidades podem ser incluídas?
- ✓ Que informações são pouco utilizadas e poderiam ser revistas?
- ✓ Seu processo de controle é abrangente e funcional?
- ✓ Os parâmetros inicialmente definidos ainda são válidos?
- ✓ Caso determinado alerta comece a ocorrer com determinada frequência, trata-se de um problema recorrente ou o *threshold* deve ser redefinido?

A seguir será apresentada a rede onde a estratégia de implementação proposta será aplicada, analisando-se as informações de gerenciamento disponíveis e analisando-se os resultados obtidos.

4.4 Ambiente Para Validação da Estratégia Proposta

4.4.1 A Instituição TCU

A atual Constituição estabelece que a fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder. Estabelece, também, que o controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União, ao qual atribuiu uma série de competências exclusivas.

Portanto, o Tribunal de Contas da União - TCU é um órgão de auxílio ao Congresso Nacional tem suas competências previstas nos artigos 33, § 2º, 71 a 74 e 161, parágrafo único, da Constituição Federal. Além disso, em razão do exercício das competências constitucionais, outras incumbências lhe foram atribuídas por lei. As competências constitucionais e legais do TCU estão listadas nos quadros 4.1 e 4.2.

Quadro 4.1 – Competências Constitucionais do TCU

COMPETÊNCIAS CONSTITUCIONAIS	FUNDAMENTO
Apreciar as contas anuais do Presidente da República	art.71, I
Julgar as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos	art. 33, § 2º e art. 71, II
Apreciar a legalidade dos atos de admissão de pessoal e de concessões de aposentadorias, reformas e pensões civis e militares	art. 71, III
Realizar inspeções e auditorias por iniciativa própria ou por solicitação do Congresso Nacional	art. 71, IV
Fiscalizar as contas nacionais das empresas supranacionais	art. 71, V
Fiscalizar a aplicação de recursos da União repassados a Estados, ao Distrito Federal ou a Municípios	art. 71, VI
Prestar informações ao Congresso Nacional sobre fiscalizações realizadas	art. 71, VII
Aplicar sanções e determinar a correção de ilegalidades e irregularidades em atos e contratos	Art. 71, VIII a XI

Fiscalizar as aplicações de subvenções e a renúncia de receitas	art. 70
Emitir pronunciamento conclusivo, por solicitação da Comissão Mista Permanente de Senadores e Deputados, sobre despesas não autorizadas	art. 72, § 1º
Apurar denúncias apresentadas por qualquer cidadão, partido político, associação ou sindicato sobre irregularidades ou ilegalidades	art. 74, § 2º
Fixar os coeficientes dos fundos de participação dos Estados, do Distrito Federal e dos Municípios, e fiscalizar a entrega dos recursos aos governos estaduais e às prefeituras	art. 161, parágrafo único

Quadro 4.2 – Competências Legais do TCU

COMPETÊNCIAS LEGAIS	FUNDAMENTO
Decidir sobre consulta formulada por autoridade competente acerca de dúvida na aplicação de dispositivos legais ou regulamentares concernentes à matéria de competência do Tribunal	Lei nº. 8.443/92
Exercer o controle da legalidade e legitimidade dos bens e rendas de autoridades e servidores públicos	Lei nº. 8.730/93
Apreciar o processo de privatização das empresas incluídas no Programa Nacional de Desestatização	Lei nº. 8.031/90
Apreciar representações apresentadas por licitante, contratado ou pessoa física ou jurídica acerca de irregularidades na aplicação da Lei de Licitações e Contratos	Lei nº. 8.666/93
Apreciar representações apresentadas pelas Câmaras Municipais acerca de não-comunicação da liberação de recursos federais	Lei nº. 9.452/97

A fim de otimizar o uso racional dos recursos do Tribunal, foi elaborada, no primeiro semestre de 1999, a segunda versão do Plano Estratégico do TCU. Nessa versão foram incorporados novos elementos, tais como: negócio, visão e missão do Órgão.

Quadro 4.3 – Negócio, Missão, Visão e Objetivos Institucionais do TCU

Negócio	Controle externo da administração pública e da gestão dos recursos públicos federais
Missão	Assegurar a efetiva e regular gestão dos recursos públicos
Visão	Ser instituição de excelência no controle e contribuir para o aperfeiçoamento da administração pública
Objetivos Institucionais	<ul style="list-style-type: none"> . Atender as expectativas da sociedade e do Congresso Nacional em relação às atividades de controle externo; . Manter-se na vanguarda de métodos, técnicas e tecnologias de controle externo; . Priorizar ações de controle em áreas de risco, relevância e materialidade;

	<ul style="list-style-type: none"> . Avaliar a regularidade, efetividade e economicidade da prestação dos serviços públicos; . Monitorar o cumprimento e o impacto das deliberações do TCU, avaliando os resultados delas decorrentes; . Difundir e consolidar a importância dos controles externo e social; . Contribuir para o contínuo aperfeiçoamento da gestão pública; . Manter política de valorização profissional de seus servidores.
--	---

Fonte: Planejamento Estratégico do TCU

Verificando-se as competências, missão e objetivos funcionais do Tribunal de Contas da União pode-se constatar o alto nível de interação e de troca de informações que ele necessita ter com outros órgãos. Nota-se que o produto básico do TCU são informações que ele recebe de ou levanta em outros órgãos ou empresas, sendo necessária uma boa infra-estrutura de rede para trâmite destas informações. Adicionalmente, fala-se atualmente muito em controle social e de ampla disponibilização de informações à sociedade, principalmente através da Internet, tornando assim a rede de computadores importante também para o público externo.

Conforme o Artigo 4º de sua Lei Orgânica, “O Tribunal de Contas da União tem jurisdição própria e privativa, em todo o território nacional, sobre as pessoas e matérias sujeitas à sua competência”. Devido a esta jurisdição decidiu-se que haveria uma unidade do tribunal em cada uma das capitais brasileiras. Estas unidades recebem o nome de Secretaria de Controle Externo Estadual – SECEX estadual e estão subordinadas a uma Secretaria Geral de Controle Externo - SEGECEX em Brasília.

O Artigo 88 da Lei Orgânica do TCU cria um instituto que será responsável pelos concursos de ingresso de novos funcionários e pelo treinamento e aperfeiçoamento do Quadro de Pessoal do Tribunal. Esse instituto denominou-se Instituto Serzedello Corrêa - ISC e localiza-se em um prédio localizado a uma distância aproximada de 8Km da sede do TCU em um local denominado Asa Norte.

4.4.2 O Histórico da Rede de Computadores do TCU

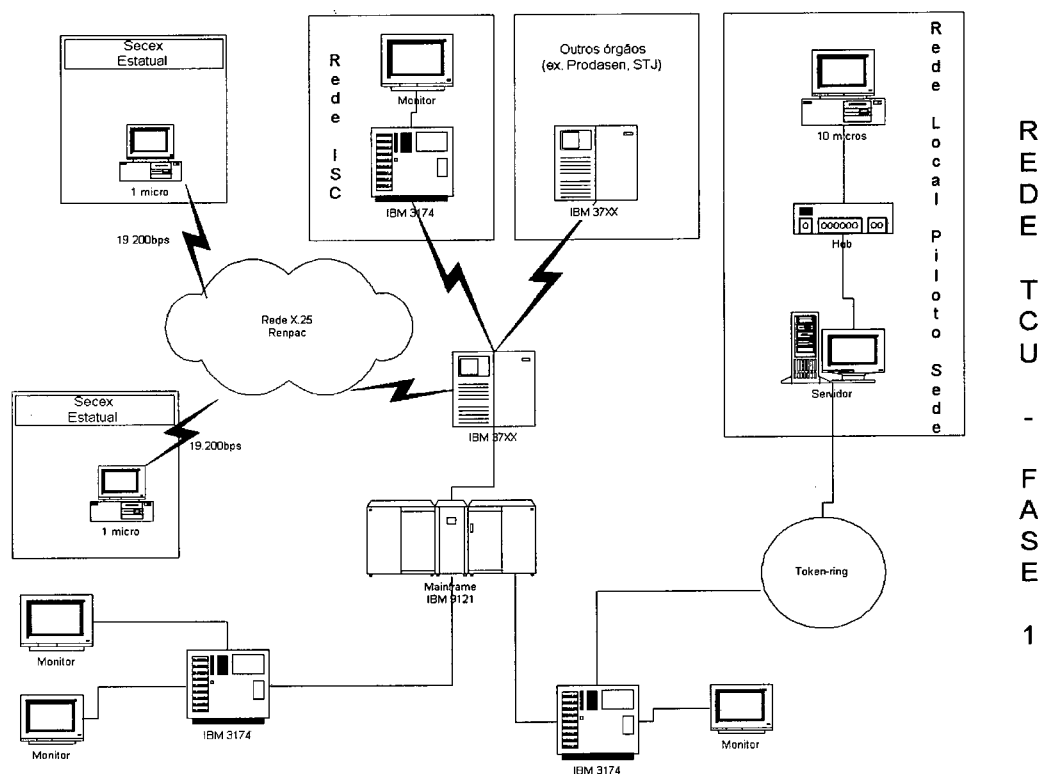
Até 1986 o tribunal utilizava pouco os recursos de informática. Ele dispunha de um computador Burroughs (atual Unisys) modelo L-8000 e mantinha convênios com o SERPRO para processamento da folha de pagamento e com o PRODASEN para controlar andamento de processos e pesquisar a legislação federal e a jurisprudência dos tribunais superiores. Em 1987 foi alugado um *mainframe* da IBM, mas o TCU dispunha de poucos profissionais da área de informática, que desenvolveram alguns sistemas para dar suporte administrativo ao órgão (e.g. folha de pagamento e pessoal).

Em 1990 foram contratados vinte analistas de sistemas e quinze programadores e iniciou-se o processo de informatização em larga escala, sempre no ambiente de grande porte. Essa primeira fase da rede de comunicação de dados era caracterizada por sistemas desenvolvidos em CSP e Cobol e somente a unidade da Sede em Brasília tinha acesso aos sistemas através de controladoras de terminais locais modelo IBM-3274. As secretarias nos estados tinham acesso à rede SERPRO através de terminais disponibilizados pela Secretaria de Fazenda Nacional e podiam acessar o SIAFI e sistemas de órgãos que tinham ligação com o SERPO, o que não era o caso do TCU.

A primeira expansão da rede de comunicações foi no sentido de estender o acesso ao grande porte a todas as unidades do TCU e a instalação de uma rede local piloto que serviria de embrião para a futura rede local. Para possibilitar esta expansão foram contratados uma controladora de comunicações com suporte a linhas remotas, uma controladora de terminais remota, diversos terminais de vídeo e placas seriais síncronas para serem colocados em microcomputadores nas Secretarias Estaduais para acesso à Sede através da rede RENPAC da Embratel, utilizando um acesso dedicado

síncrono de 19.200bps (serviço 3025). Foram também contratados equipamentos, programas e serviços de instalação de uma rede local piloto com dez pontos de rede. O resultado da implantação destes equipamentos que aconteceu em 1993 foi chamado, conforme o Projeto da Rede de Comunicação de Dados do TCU, de Fase 1 da rede. A figura 4.2 representa o esquema de interligação dos componentes nesta fase.

Figura 4.2 – Fase 1 da Rede de Comunicação de Dados

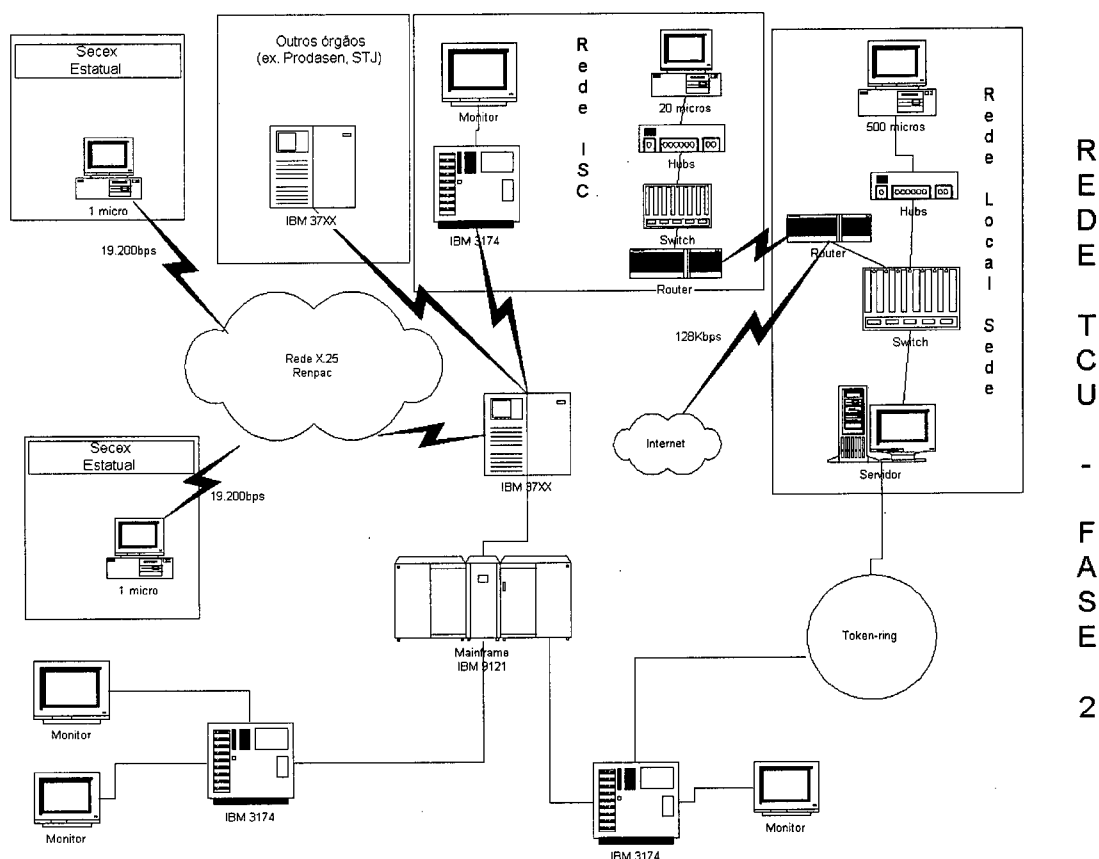


Fonte: Projeto da Rede de Comunicação de Dados do TCU

A chamada Fase 2 da rede aconteceu em 1996 com a implantação de redes locais nos edifícios Sede e da Asa Norte. Esta rede constituindo-se 730 pontos no Edifício Sede e 95 pontos na Asa Norte. As duas redes inicialmente utilizavam o *link* de comunicações de 64kbps que foi logo mudado para 128kbps. Nesta fase as SECEX estaduais acessavam somente os sistemas de grande porte, não havendo nenhuma

ligação das mesmas com a rede local que estava sendo implementada. A figura 4.3 mostra como ficou o esquema de ligação nesta Fase 2.

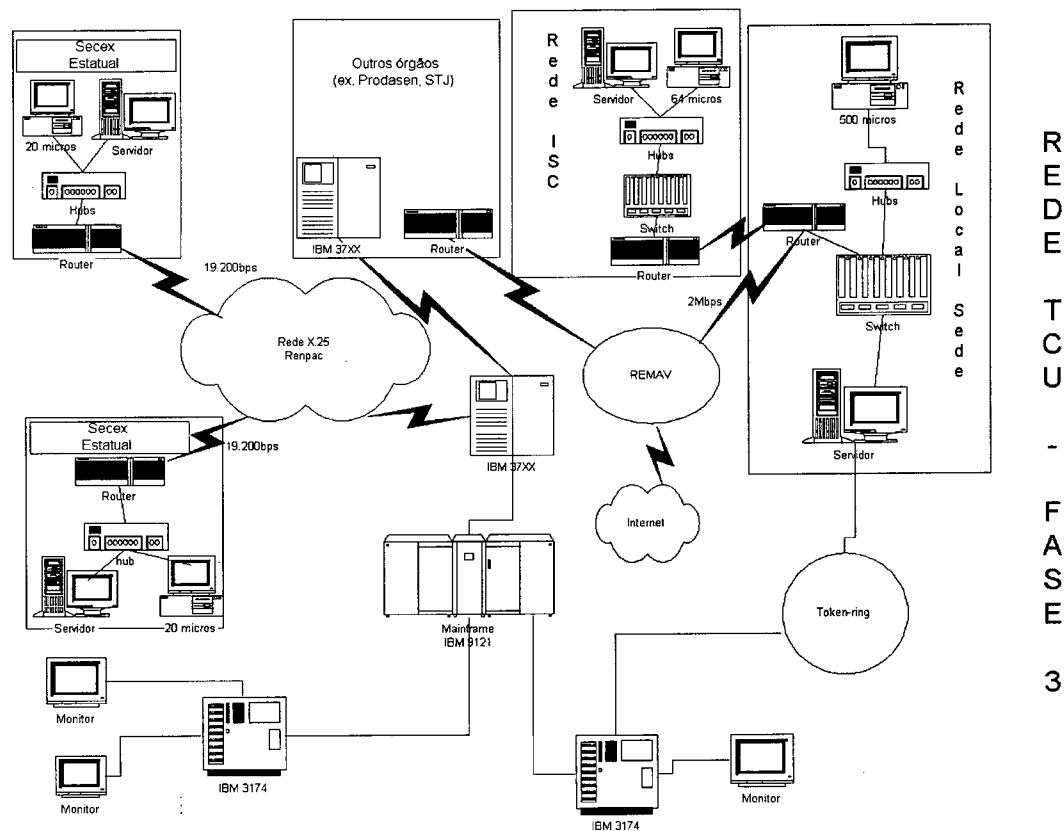
Figura 4.3 – Fase 2 da Rede de Comunicação de Dados



Fonte: Projeto da Rede de Comunicação de Dados do TCU

E, finalmente, na última fase prevista no Projeto da Rede de Comunicação de Dados do TCU, de 1996 a 1998, foram instaladas redes locais em todas as unidades do TCU e estas redes eram interligadas, conforme figura 4.4, utilizando-se da rede RENPAC da Embratel. As redes das SECEX nos estados têm em média de 30 a 40 pontos.

Figura 4.4 – Fase 3 da Rede de Comunicação de Dados

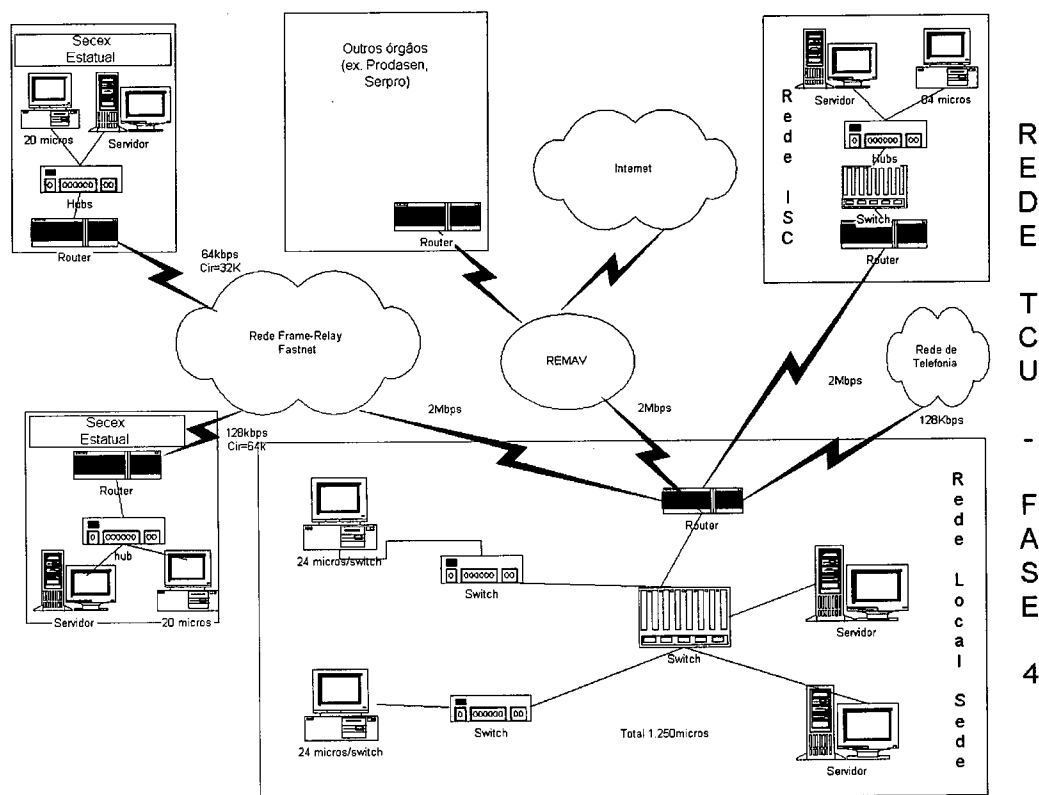


Fonte: Projeto da Rede de Comunicação de Dados do TCU

Como era previsível, a importância da rede só aumentou e a necessidade de cada vez mais banda devido à disponibilização de novos serviços e sistemas e também devido ao aumento do número de estações e usuários acessando-a. Como adotou-se a utilização de sistemas cliente servidor e o servidor de banco de dados localiza-se na sede houve um rápido congestionamento da rede WAN que estava montada sobre X.25 com acessos de 19.200bps. Em consequência deste congestionamento e também em função dos custos elevados da RENPAC para elevado volume de tráfego, a rede WAN foi migrada para Frame-Relay, num momento inicial com acesso de 64kbps e CIR de 32kbps para todos os estados.

Em função da obsolescência do hardware e software que estavam instalados no computador de grande porte do TCU, de seus elevados custos e do problema que causaria a atualização do software uma vez que seria necessária a migração para outro banco de dados textual e, conseqüentemente, o redensolvimento dos sistemas implantados, optou-se pela desativação deste equipamento com desenvolvimento dos novos sistemas na plataforma de rede, mantendo-se somente um *gateway* SNA para acessar computadores de grande porte de outros órgãos (SERPRO, PRODASEN, STJ, BB, CEF, etc.). Esse processo conhecido como *downsizing* foi concluído em 1998.

Figura 4.5 – Situação atual da Rede de Computadores do TCU



Em 1998 também concluiu-se a construção de dois novos prédios – Anexos I e II, que viriam a ampliar o espaço de trabalho dos funcionários do Tribunal. Como a tecnologia de redes locais já era uma realidade na época de construção dos Anexos,

decidiu-se pela implantação de cabeamento estruturado nestes edifícios e aquisição de equipamentos de rede ativos para essa nova rede, que poderia ser chamada de Fase 4. Esta rede foi implantada com 1.880 pontos (incluindo telefonia e dados) e seu esquema de ligação pode ser visto na figura 4.5, que representa a situação atual da Rede de Computadores do TCU.

4.4.3 O Problema do Gerenciamento

O Tribunal de Contas da União - TCU possui redes locais em quatro edifícios em Brasília (Sede, Anexo I, Anexo II e ISC) e também em todas as capitais brasileiras. Até 1996 todos os sistemas de informação do TCU estavam residentes em um *mainframe* IBM, só havia uma rede experimental com 10 microcomputadores em Brasília. Atualmente, o *mainframe* foi desativado, todas as aplicações foram migradas para a plataforma de rede, utiliza-se maciçamente a internet e o correio eletrônico e foram implantadas redes locais em todas as capitais. Dos 10 microcomputadores da rede local a rede passou para mais de 1.900 micros, cerca de 1.400 em Brasília com perspectiva de aquisição de mais 500 micros ainda no decorrer do ano 2.001, deste montante 300 substituirão micros antigos e o restante será acrescido à rede.

Paralelamente ao fato de aumento da complexidade da rede do TCU, devido ao aumento da abrangência e da oferta de novos serviços e sistemas temos o fato de só haverem profissionais de informática em Brasília, a maioria deles dedicada ao desenvolvimento e manutenção de sistemas. Isto torna o processo de gerenciamento da rede corporativa bastante pesado trazendo alguns transtornos para o usuário, pois o gerenciamento acontece de forma reativa, ou seja, o usuário reclama do problema e a equipe de suporte técnico é acionada para resolvê-lo.

Outro agravante é que não existem estudos no sentido de identificar qual é o comportamento normal da rede (*baseline*) e nem quanto de recurso, principalmente referente a comunicação, está sendo consumido por cada tipo de serviço (e-mail, acesso a banco de dados, internet, sincronismo de diretórios, etc.).

Estes fatos citados anteriormente são resultantes do fato de que a rede de computadores do TCU cresceu vertiginosamente e não houve tempo suficiente para a implementação de metodologia de gerência. A cada dia que passa os usuários e o próprio TCU estão se tornando mais dependentes da rede local, sendo imprescindível que a identificação e solução dos problemas seja o mais rápido eficiente possível, ou seja, diminuição de *downtime*.

O estudo de demanda de tráfego e estabelecimento de *baseline* deve levar a um dimensionamento melhor da rede, poupando expansões desnecessárias de banda e equipamentos e melhorando a performance geral da rede. Isso implica em economia de recursos públicos e melhoria no tempo de resposta das aplicações e, conseqüentemente, no aumento da satisfação do usuário.

CAPÍTULO V – IMPLEMENTAÇÃO DO GERENCIAMENTO

Este capítulo relata a experiência obtida com a implementação de um sistema de gerenciamento no ambiente escolhido para estudo de caso. A implementação do sistema de gerenciamento no ambiente do Tribunal de Contas da União foi guiada pelas etapas estabelecidas na estratégia de implementação definida no capítulo 4 deste trabalho.

5.1 Fase 1 – Estudo da Rede Existente

A rede do Tribunal de Contas da União, conforme apresentada no capítulo 4, é uma rede em estrela, possuindo redes pequenas ou médias nos estados e uma grande rede na Sede, onde encontram-se os servidores de banco de dados, principais servidores de arquivos, acesso à internet e outros órgãos e pessoal especializado na área de informática.

Todas as estações de trabalho da rede utilizam protocolo TCP/IP e sistema operacional Windows 95 ou Windows 2000 *professional*. Os servidores corporativos (banco de dados, correio, internet, intranet, etc.) utilizam sistema operacional Windows NT 4.0 ou 2000, possuindo um domínio único, justificado pelo fato da centralização da administração de recursos e usuários. A maioria dos sistemas em produção ainda utiliza a tecnologia cliente/servidor, acessando o servidor de banco de dados Oracle residente em Brasília. As Secex nos estados possuem servidores de arquivos, onde são armazenados os programas executáveis dos sistemas e arquivos de interesse local.

Recentemente, definiu-se que os novos sistemas seriam desenvolvidos para plataforma Web, acessando servidores localizados em Brasília.

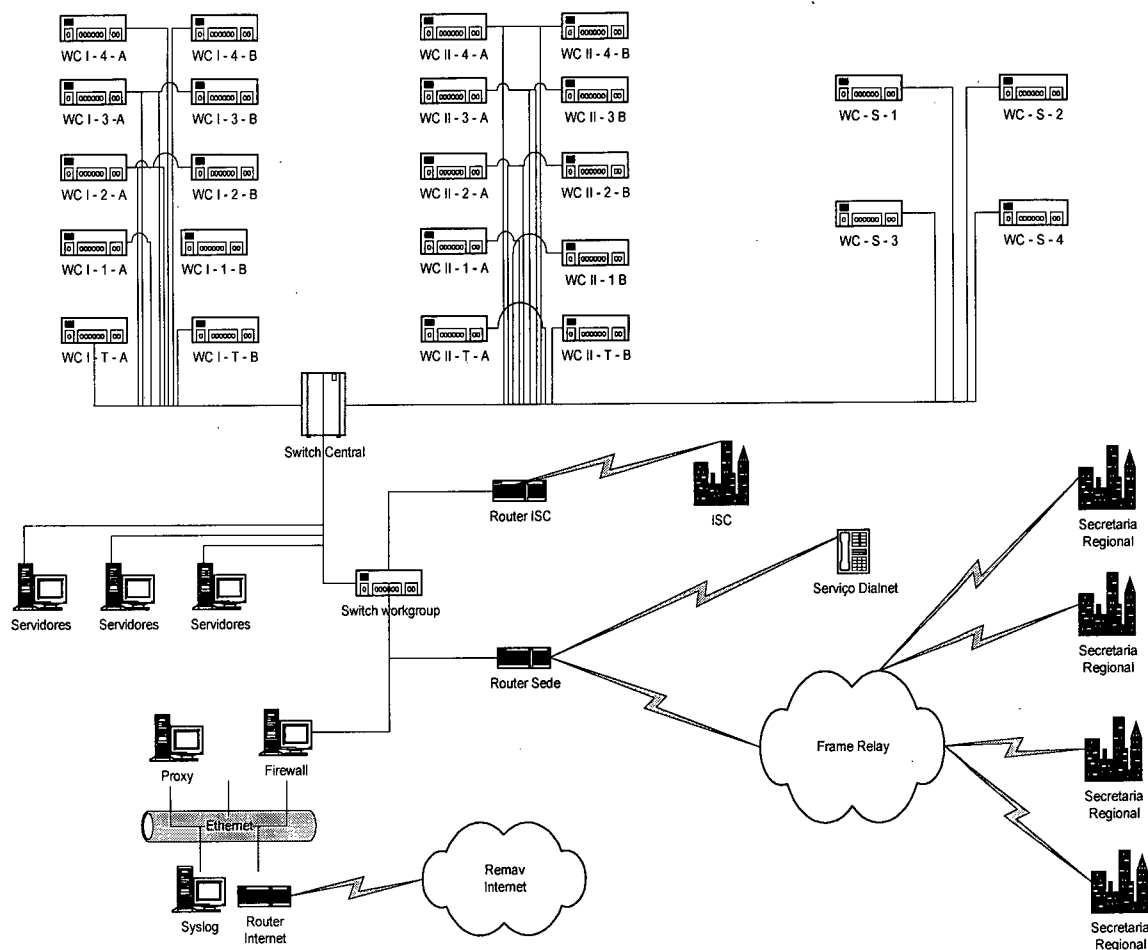
5.1.1 Rede LAN do TCU

A rede local em Brasília, apresentada na figura 5.1, está dividida em três prédios: Edifício Sede, Anexo I e Anexo II. Esses edifícios possuem em conjunto cerca de 1.600 computadores que estão ligados em armários de fiação a *switches* de *workgroup* com tecnologia 10/100BaseT. Esses *switches* estão ligados a um *switch* central utilizando *uplinks* 100BaseF. Esse mesmo *switch* está ligado aos servidores corporativos através de ligações *fast-ethernet* ou *gigabit ethernet*.

A rede local do ISC possui cerca de 100 microcomputadores e também possui um *switch* central ao qual estão ligados os *hubs* 10BaseT localizados nos andares. O ISC, assim como as Secretarias Regionais, possui um servidor de arquivos e de autenticação.

As redes locais nos estados possuem em média 30 microcomputadores e são implementadas utilizando redes *ethernet* compartilhadas com tecnologia 10BaseT (*ethernet* a 10Mbps). Em função do reduzido número de estações de trabalho, elas ainda não são providas de *switches*.

Figura 5.1 – Esquema de ligações da rede TCU



5.1.2 Rede WAN do TCU

A interligação das redes dos estados à rede da Sede se dá através de uma rede Frame Relay. O Frame Relay é um exemplo de tecnologia *packet-switched* (comutação de pacotes). Uma rede de comutação de pacotes permite às estações finais compartilharem dinamicamente o “miolo” da rede e a banda de passagem de dados disponível. Tamanhos variáveis de pacotes são usados para transferências mais eficientes e flexíveis. Estes pacotes então são encaminhados entre os vários segmentos

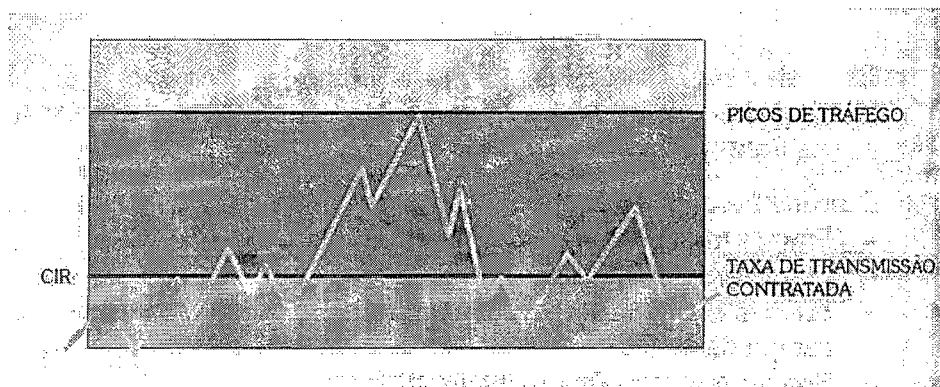
da rede até que alcancem seu destino. Técnicas de multiplexação estatística controlam o acesso a rede em uma rede de comutação de pacotes. A vantagem desta técnica é que ela acomoda mais flexibilidade e eficiência no uso da banda de passagem.

O Frame Relay provê uma comunicação orientada a conexão na camada de enlace de dados. Isto significa que existe uma definição de comunicação entre cada par de dispositivos e que estas conexões são associadas com um identificador de conexões. Este serviço é implementado usando um Circuito Virtual Frame Relay, como se fosse uma conexão lógica criada entre dois equipamentos terminais de dados (DTE) através de uma rede de comutação Frame Relay.

Os circuitos virtuais fornecem um caminho de comunicação bi-direcional de um dispositivo DTE para um outro e são unicamente identificados por um identificador da camada de enlace de dados – *Data-Link Connection Identifier* (DLCI). Vários circuitos virtuais podem ser multiplexados dentro de um simples circuito físico para a transmissão de dados através da rede. Esta capacidade geralmente reduz a complexidade do equipamento e da rede requisitadas para conectar múltiplos dispositivos DTE.

Quando um circuito Frame Relay é contratado, alguns parâmetros são definidos, o principal deles é o CIR – *Committed Information Rate*. O CIR é a banda garantida pelo provedor do serviço de telecomunicações, no caso do TCU os *links* são de 64Kbps (exceto a Secex-RJ, que é de 128Kbps) com CIR igual a 50% da sua capacidade. O usuário pode tentar ultrapassar o limite do CIR, se a rede tiver disponibilidade ela entrega o *frame*, caso contrário os dados excedentes são descartados.

Figura 5.2 – Tráfego em circuito Frame Relay



O Frame Relay reduz a sobrecarga da rede por implementação de mecanismos de notificação de congestionamento explícito, para controle de fluxo no circuito virtual. O Frame Relay é tipicamente implementado em rede intermediária segura, então a integridade dos dados não é sacrificada porque o controle de fluxo pode ser efetuado por protocolos de camadas mais elevadas. O Frame Relay implementa dois mecanismos de notificação de congestionamento: *Forward-explicit congestion notification* (FECN) e *Backward-explicit congestion notification* (BECN)

Entretanto, o controle do congestionamento em um aplicativo que utiliza TCP normalmente é independente dos mecanismos FECN e BECN. Ao ocorrer a perda de pacotes, o TCP diminui o tamanho de sua janela de transmissão, efetivamente tornando mais lenta sua taxa de transmissão. Em seguida, ele aumenta gradualmente o tamanho da janela, até voltar a ocorrer o congestionamento. (Black, 1999)

A rede do ISC, que centraliza todas as atividades relativas a treinamento do TCU, liga-se à rede da Sede através de uma LPCD (Linha Privada de Comunicação de

Dados) de 2Mbps. Devido ao seu elevado volume de tráfego, número de computadores e usuários, faz-se necessário um *link* de alta velocidade.

5.1.3 Equipamentos de Rede

A rede de computadores do TCU é altamente homogênea em termos de hardware. Equipamentos ativos de rede local (*hubs* e *switches*) são da marca Lucent e roteadores são da marca Cisco.

Os *hubs* Lucent modelo SH-E24 são gerenciáveis e possuem 24 portas 10BaseT e uma porta de *uplink* AUI/Fibra ótica. Eles estão instalados nos estados, no prédio do ISC e uma pequena quantidade instalada na Sede. Os poucos *hubs* instalados na sede serão substituídos por *switches* ainda no corrente ano.

Os *switches* Lucent são de quatro modelos:

- ✓ Lucent P115 – é um *switch* de *workgroup* de 24 portas. Funciona como um *group switch*, possuindo três grupos de oito portas. Cada um destes grupos funciona internamente como um pequeno *hub* e a ligação entre os grupos funciona como *switch*. Cada grupo pode ser configurado para trabalhar como 10BaseT ou 100BaseTx. Ele possui ainda uma porta de *uplink* 100BaseF para ligação ao *switch* central. Possui módulo de gerenciamento que suporta SNMP, RMON e SMON.
- ✓ Lucent P330 – é um *switch* de *workgroup* de 24 portas. Funciona como *port switch*, possuindo 24 portas 10BaseT/100BaseTx, *autosense*. Possui ainda duas portas de *uplink* 100BaseF para ligação ao *switch* central, possibilitando redundância e *trunking*. Possui módulo de gerenciamento que suporta SNMP, RMON e SMON.

- ✓ Lucent LET36 – é um *switch* modular com dezoito *slots*. É o *switch* central da rede do ISC e também utilizado para concentrar os *hubs* remanescentes no Edifício Sede. Possui módulos de 100BaseTx para ligação dos servidores e *uplink* 10BaseF *uplink* dos *hubs*. É gerenciável e suporta SNMP, RMON e SMON.
- ✓ Lucent M770 – é um *switch* modular com 14 *slots*, sendo estes *slots* separados em dois grupos de 7 *slots* denominados de domínios (esquerdo e direito). É o *switch* central da rede da sede. Embora possua menos *slots* do que o LET36, ele permite maior número de conexões, é mais veloz e possui módulos com maior concentração de portas. Possui módulos com portas 100BaseTx e 1000BaseSx para ligação dos servidores e 100BaseF para ligação aos *switches* de *workgroup*. É gerenciável e suporta SNMP, RMON e SMON.

Os roteadores Cisco, modelo 2501, 2600 e 4500 possuem as características enumeradas no quadro 5.1, todos os roteadores possuem *software* com suporte a X.25 e Frame Relay. Além de implementarem o SNMP, disponibilizando a MIB-II e diversos RFCs além da MIB proprietária Cisco, os roteadores implementam os grupos *events* e *alarms* do RMON.

Quadro 5.1 – Configuração dos roteadores

	Cisco 2501	Cisco 2600	Cisco 4500
Utilização	Ligação das unidades remotas à sede	Ligação da Sede às unidades remotas e à internet	Ligação da Sede ao ISC
Número de portas	1 LAN / 2 WAN	1 LAN / 2 WAN	2 LAN / 4 WAN
<i>Software</i>	IOS 11.2	IOS 12.0	IOS 11.2
Gerenciamento SNMP	Possui	Possui	Possui
Memória	4MB	8MB	8MB
<i>Software</i> de criptografia	Não possui	Possui	Não possui

5.2 Fase 2 – Identificação dos Problemas e Requisitos de Gerenciamento

O maior problema na rede de computadores do TCU é a falta de informações que permitam o gerenciamento pró-ativo e que subsidiem o planejamento de capacidade. Isto implica em diversos problemas:

- ✓ demora na identificação, isolamento e correção de falhas, conseqüentemente em baixo MTBF e elevado MTTR;
- ✓ o dimensionamento da rede ocorre de forma empírica, devido à inexistência de medidas sistemáticas de utilização e de comportamento de tendência da rede;
- ✓ a inexistência de *baseline* implica também no desconhecimento do comportamento normal da rede e em saber o que alterou quando os usuários reclamam de problemas, principalmente de performance;
- ✓ dificuldade de estabelecer qualidade de serviço, uma vez que as falhas não são sistematicamente anotadas para cobrança dos provedores de serviço. Se não se tem como cobrar qualidade de serviço, então é impossível fornecer qualidade de serviço;
- ✓ falta de informações disseminadas às diversas áreas interessadas em informações de gerenciamento;
- ✓ baixa performance das aplicações cliente/servidor quando executadas nas secretarias dos estados;
- ✓ inexistência de SLA, dificultando a identificação de objetivos a serem alcançados pela rede e na justificação dos custos.

Os maiores objetivos no estabelecimento de funções de gerenciamento na rede do TCU são:

- ✓ a manutenção de informações de problemas, incluindo MTBF e MTTR;
- ✓ a implementação de gerenciamento pró-ativo;
- ✓ o estabelecimento de *baseline* e análise de tendência;
- ✓ melhoria da performance das aplicações, principalmente nas Secex estaduais; e
- ✓ implementação de planejamento de capacidade.

5.3 Fase 3 – Estabelecimento de Prioridades

Como o principal problema existente é a falta de informações de gerenciamento torna-se prioritária a instalação e customização de um NMS- Sistema de Gerenciamento de Redes e de um TTS – Sistema de Chamados para organizar os chamados gerados pelos usuários, além da disponibilização de informações necessárias para subsidiar a tomada de decisão pelos gerentes de TI – Tecnologia da Informação.

Já estava implementado um TTS, adquirido da CA – Computer Associates, denominado AHD – *Advanced Help Desk*. O sistema permite a abertura de chamados através da intranet e a distribuição para as pessoas responsáveis pela solução dos problemas. Entretanto, o ponto de partida dos chamados ainda é o usuário final, o que implica em gerenciamento reativo.

O TCU adquiriu recentemente o *framework* TNG, também da CA, e algumas *options* de gerenciamento. Faz-se necessária portanto a instalação e configuração do

TNG e também a sua integração ao AHD. Além disso, estuda-se a aquisição de analisadores de protocolo e a utilização de diversas ferramentas *freeware* de gerenciamento, disponíveis na internet para a plataforma linux.

A baixa performance das aplicações nas secretarias estaduais, a necessidade de disponibilização de novas aplicações corporativas, os elevados custos associados aos *links* de comunicação da rede WAN e o iminente aumento de capacidade da rede Frame Relay tornam também prioritária a análise de sua utilização. Segundo Nassif (1997, p.3), a não avaliação sistemática e científica dos enlaces pode gerar congestionamentos de tráfego e tempos de resposta fora de padrões aceitáveis, ou por outro lado, desperdício de banda passante de linhas superdimensionadas. A avaliação dos enlaces vai subsidiar a tomada de decisão sobre necessidade de *upgrade*, além de mostrar como efetivamente cada enlace está sendo utilizado por aplicação, como está o seu desempenho, se estão ocorrendo gargalos, quando e por que motivo.

5.4 Fase 4 – Análise das Informações de Gerenciamento Disponíveis

Specialski (2000, p.2) defende a idéia que a adoção de um *software* de gerenciamento não resolve todos os problemas. Além disso, existe uma sobrecarga muito grande de informações que podem ser coletadas e disponibilizadas aos usuários. É essencial identificar quais as informações são importantes, resumizá-las e disponibilizá-las de forma inteligível e simplificada aos usuários.

Existe uma variedade grande de ferramentas de gerenciamento de rede para coleta e apresentação de métricas de gerenciamento de rede. Entretanto, não existe um

consenso sobre quais métricas deveriam ser regularmente coletadas e como elas deveriam ser apresentadas. As métricas utilizadas para avaliação de tráfego de rede podem ser classificadas em, pelo menos, quatro categorias: utilização, performance, disponibilidade e estabilidade.

As métricas de utilização descrevem diferentes aspectos do total de tráfego passando pela rede, pode incluir: total de pacotes e octetos entrantes e saídes, métricas de pico e métricas de utilização por aplicação, nó ou protocolo.

As métricas de performance dizem respeito à qualidade de serviço, identificando situações de *delay* e congestionamento. Pode incluir: RTT em diferentes níveis de protocolo, número de colisões em um barramento de rede, número de mensagens ICMP *source quench* e número de pacotes descartados.

As métricas de disponibilidade podem ser vistas como medida de acessibilidade de longo tempo em diferentes camadas de protocolo. Pode incluir: disponibilidade de linha como percentual de tempo ativo, disponibilidade de rota e disponibilidade de aplicação.

As métricas de estabilidade descrevem flutuações rápidas na rede que podem degradar o nível de serviços. Mudanças no padrão de tráfego também poderiam ser identificadas utilizando estas métricas. Pode incluir: número de mudanças de rota, número de rotas por interface em tabelas de roteamento, estabilidade de contadores de *next hop* e comportamento de ICMP de curta duração (e.g. *destination unreachable*).

Algumas métricas são facilmente recuperáveis pois são definidas como variáveis em MIBs padrão. Outras métricas podem ser recuperadas por estarem

definidas em MIBs proprietárias. Finalmente, algumas métricas são consideradas não recuperáveis ou porque não é possível sua inclusão no conceito do SNMP ou porque sua medida requereria uma carga de *polling* muito grande.

A MIB II, definida no RFC 1213, foi definida como uma MIB genérica para recuperação de informações SNMP. Entretanto, vários fabricantes desenvolveram MIBs proprietárias porque precisam de objetos específicos para seus equipamentos que podem não estar definidos ou disponíveis nas MIBs padrão. Dessa forma faz-se necessário avaliar não somente as informações disponíveis nas MIBs padrão quanto nas MIBs proprietárias implementadas pelos equipamentos da empresa.

Entretanto, o excesso de MIBs proprietárias e de variáveis nas MIBs torna necessário um estudo cuidadoso para levantar quais variáveis devem ser gerenciadas. Em função deste problema optou-se por levantar primeiramente quais eram as informações de gerenciamento (OIDs) disponibilizadas pelos dispositivos para depois encontrar quais as MIBs descreviam-nas. Utilizou-se, com esta finalidade, o programa *snmpwalk* na plataforma Linux que percorre as MIBs dos dispositivos gerenciados fazendo uso da operação *get-next* do *snmp*. Para percorrer toda a árvore, incluindo a parte privada, e para gerar a saída em arquivos foi utilizado o comando: “*snmpwalk endereço-ip community-name .1 > arquivo*”. Esse comando foi executado uma vez para cada tipo/modelo de dispositivo a ser gerenciado e, posteriormente, o arquivo de saída foi confrontado com as MIBs padrão e proprietárias, que já haviam sido buscadas na internet, para verificar quais as informações eram disponibilizadas e selecionar aquelas mais relevantes. No Anexo IV são listadas partes dos arquivos gerados pelo comando *snmpwalk*.

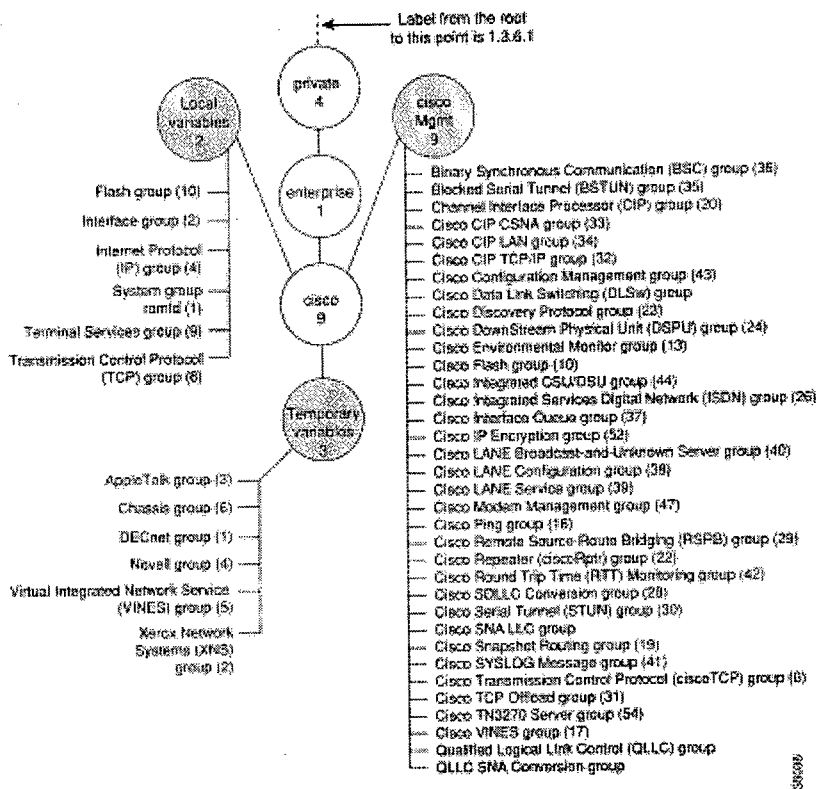
A partir da análise citada anteriormente, verificou-se que alguns valores não eram acumulados em algumas variáveis, que havia duplicidade de informações em outras e, ainda, que outras traziam a mesma informação acumulada de forma diferente.

Baseado no conhecimento da rede e na verificação das variáveis mantidas e que retornavam valores confiáveis, foram selecionadas aquelas a partir das quais seria possível o fornecimento de informações relevantes. Definiu-se então como passíveis de monitoramento as variáveis listadas no Anexo I.

5.4.1 MIB Privada Cisco

A MIB privada Cisco é representada pelo identificador de objeto 1.3.6.1.4.1.9 (iso.org.dod.internet.private.enterprise.cisco). A MIB Cisco, conforme figura 5.3, possui as seguintes sub-árvores: local (2), temporary (3) e ciscoMgmt (3). A sub-árvore local contém os objetos definidos nas versões IOS anteriores ao release 10.2. Estes objetos implementam a SMI do SNMPv1. As versões posteriores à versão 10.2 são definidas de acordo com a SMI do SNMPv2. Estes objetos são incluídos na sub-árvore ciscoMgmt. As MIBs definidas na sub-árvore local estão sendo gradualmente descontinuadas e substituídas por novos objetos localizados na sub-árvore ciscoMgmt. Adicionalmente, existe a sub-árvore temporary que é equivalente à experimental da MIB-II. As variáveis ali definidas estão sujeitas a alteração nas novas versões de IOS e também serão gradativamente migradas para a sub-árvore ciscoMgmt.

Figura 5.3 – MIB privada Cisco



Fonte: UniverCD da Cisco

5.4.2 MIB Privada Lannet

A Lucent, atual fabricante dos *switches* utilizados na rede do TCU adquiriu a empresa Madge que, por sua vez, havia adquirido a empresa Lannet. Por este motivo, as informações de gerenciamento destes produtos estão definidas na MIB privada Lannet.

A MIB privada Lannet é representada pelo OID 1.3.6.1.4.1.81 (iso.org.dod.internet.private.enterprise.Lannet). A MIB Lanet possui diversas sub-árvores; as principais são listadas na figura 5.4. A MIB Lannet além de definir diversos objetos adicionais à MIB II, possui uma sub-árvore específica para o SMON, tendo sido uma das pioneiras em sua definição.

Figura 5.4 – MIB privada Lannet

Lannet (81)	<ul style="list-style-type: none"> - Chassis (7) – grupo definido na MIB config.mib - GenGroup (8) – grupo definido na MIB config.mib - GenPort (9) – grupo definido na MIB config.mib - GenIntPort (10) - grupo definido na MIB config.mib - SoftRedundancy (11) - grupo definido na MIB muduls.mib - Eth (12) - grupo definido na MIB muduls .mib - Tok (13) - grupo definido na MIB muduls.mib - Ts (14) - grupo definido na MIB muduls.mib - LntOID (17) - grupo definido na MIB gen.mib - LntLanSwitch (19) - grupo definido na MIB applic.mib - SwitchChip (28) – grupo definido na MIB xswtch.mib - Smon (30) - grupo definido na MIB applic.mib - Meritage (32) - grupo definido na MIB mritag.mib
----------------	---

Infelizmente, para os equipamentos existentes no TCU as variáveis de monitoramento para a mesma medida não são as mesmas para todos os equipamentos, sendo necessário identificar e utilizar variáveis diferentes para modelos diferentes do mesmo tipo de equipamento (e.g. *switches* modulares M770 e LET36). Além disso, embora afirmem implementar a MIB-II, diversas variáveis da MIB-II não são mantidas pelos *switches* Lannet, embora a consulta a seus valores em vez de retornar erro retorna sempre o valor zerado. No presente trabalho foram utilizadas as seguintes sub-árvore da MIB Lannet: eth(12) que mantém informações relativas aos *hubs* Lannet com tecnologia *ethernet* (definida na MIB Moduls), IntLanSwitch(19) (definida na MIB Applic) que mantém informações relativas à utilização de barramentos e portas de *switch* do LET36 e switchChip(28) que mantém informações relativas aos domínios, grupos e portas do *switch* Lannet M770 (definida na MIB swtch).

5.5 Fase 5 – Estabelecimento de Monitoração e Limiares

Nesta fase foi feito o levantamento do *baseline* da rede determinando qual o comportamento normal da rede. Limiares foram estabelecidos para os diversos valores, de acordo com a literatura e valores que já estavam incompatíveis motivaram a identificação de possíveis causas e solução de problemas. Esta fase fornece informações que servirão de subsídio para planejamento de capacidade, gerência de performance, contabilização e falhas.

De acordo com Oppenheimer (1999, p.349), todo sistema é diferente. Assim, selecionar os métodos de testes e ferramentas apropriadas requer criatividade, engenhosidade e uma compreensão completa do sistema a ser avaliado.

Além do estabelecimento de limiares, o monitoramento contínuo deve ser feito para diversos valores. Para estes valores, são definidas ações/alarmes que devem ser disparados quando os limiares forem ultrapassados.

5.5.1 Taxa de Utilização

5.5.1.1 Utilização de CPU

O monitoramento da taxa de utilização de CPU é importante para identificação de gargalos que estejam comprometendo o funcionamento adequado da rede. A implementação de novos serviços ou funcionalidades pode impactar bastante a utilização de CPU, por exemplo: a implementação de monitoramento RMON em roteadores ou a implementação de novos serviços em servidores de rede.

Diversas variáveis se relacionam à taxa de utilização de CPU em roteadores Cisco, entre elas: `cpmCPUTotal5sec` – taxa de utilização de CPU nos últimos cinco segundos, `cpmCPUTotal1min` – taxa de utilização de CPU no último minuto e `cpmCPUTotal5min` – taxa de utilização da CPU nos últimos 5 minutos. Optou-se pela utilização do `cpmCPUTotal5min`, uma vez que o tempo de 5 minutos corresponde ao período de coleta de informações dos roteadores. O valor de utilização de CPU em roteadores não deve ultrapassar 80% e a média deve ficar inferior a 50%. É recomendável a implementação de envio de *traps* caso a utilização de CPU ultrapasse o limiar estipulado.

5.5.1.2 Utilização de memória

Da mesma forma que a CPU, a taxa de utilização de memória deve ser monitorada, uma vez que a falta de memória disponível também impacta a performance da rede. Se a quantidade de memória disponível for insuficiente, recomenda-se a expansão de memória do equipamento. Os roteadores Cisco implementam variáveis para controle de quantidade de memória utilizada (`ciscoMemoryPoolUsed`) e também de quantidade de memória livre (`ciscoMemoryPoolFree`). Esses valores devem ser monitorados para cada *pool* de memória utilizado (e.g. I/O, processador).

5.5.1.3 Utilização de interfaces

Embora o uso mais importante de taxa de utilização seja para encontrar potenciais gargalos e áreas de congestionamento, a medida de taxa de utilização de interfaces é muito importante porque o tempo de resposta usualmente cresce

exponencialmente de acordo com a taxa de utilização do recurso, conforme pode ser comprovado pela teoria das filas.

Para monitoramento da taxa de utilização de interfaces é comum utilizar-se as variáveis `ifInOctets` e `ifOutOctets` por interface/sub-interface. No caso de Frame-Relay podem também ser utilizadas as variáveis `frCircuitReceivedOctets` e `frCircuitSentOctets` por DLCI, definidas no RFC 1315 (Frame Relay). No caso de interfaces dos roteadores Cisco pode-se utilizar as variáveis `locIfInBitsSec` e `locIfOutBitsSec` que já dão diretamente a média de bits que entraram na ou saíram da interface nos últimos cinco minutos. Optou-se pela utilização das variáveis `locIfInBitsSec` e `locIfOutBitsSec` para as interfaces, uma vez que o valor médio para cinco minutos já é calculado pelo roteador e pelas variáveis `ifInOctets` e `ifOutOctets` para as sub-interfaces, uma vez que as variáveis anteriores só são calculadas para interfaces.

O cálculo da taxa de utilização pode variar em função das variáveis monitoradas e do tipo de circuito. Para as interfaces o cálculo de taxa de utilização será feito com a seguinte fórmula:

$$\text{Taxa de utilização} = \frac{\text{locIfInBitsSec} + \text{locIfOutBitsSec}}{\text{ifSpeed}}$$

Para verificar a utilização dos circuitos Frame Relay em função do CIR contratado e para equipamentos que não mantenham valores de média de bits, o cálculo deverá ser feito utilizando a seguinte fórmula, onde a velocidade é a velocidade da interface ou o valor do CIR:

$$\text{Taxa utilização} = \frac{(\Delta \text{InOctets} + \Delta \text{OutOctets}) * 8}{(\text{time B} - \text{time A}) * \text{velocidade}}$$

Para monitorar a utilização das portas nos *switches* Lannet deve-se utilizar a MIB proprietária da Lannet, uma vez que estes *switches* não mantêm os valores das variáveis do grupo interfaces da MIB II. A MIB Lannet define em diferentes sub-árvores os contadores dos *switches* M770 e LET36. Enquanto o *switch* LET36 define as variáveis de quantidade de octetos e pacotes que passam na interface na tabela lsPortTable (variáveis lsPortInOctets, lsPortInPkts), definida na MIB Applic, o *switch* M770 o faz na tabela scEthPortTable (variáveis scEthPortGoodOctetsReceived, scEthPortGoodOctetsSent, scEthPortGoodPktsRec e scEthGoodPktsSent), definida na MIB Xswitch. Nestes dois casos pode-se utilizar a fórmula genérica anterior substituindo-se as identificações de objetos por aquelas apropriadas ao caso, ressaltando-se o fato que o *switch* LET36 não armazena em variáveis independentes valores para octetos e pacotes que estejam entrando na ou saindo da interface.

A taxa de utilização de interfaces deve ter média inferior a 70% para *links* WAN e 35% para segmentos *ethernet* compartilhados. Caso os valores médios ultrapassem esses limiares deve-se avaliar que tipo de tráfego está sobrecarregando o canal, se existe alguma providência a ser tomada para redução da utilização ou aumento da capacidade de transmissão. Essa análise pode levar à mudança de localização de arquivos/servidores, identificação de uso indevido do recurso e também dos maiores consumidores da banda.

5.5.1.4 Utilização do barramento

Em segmentos *ethernet* compartilhados, a quantidade de colisões cresce à medida que aumenta a utilização do barramento. A MIB Lannet define variáveis relativas à utilização do barramento (*ethBusUtilization*) e ao pico de utilização do barramento (*ethBusPeakUtilization*). Como estes valores são expressos em percentual, eles podem ser monitorados diretamente, sem a necessidade de utilização de nenhuma fórmula. Como limiar vale a definição do item anterior de média inferior a 35% de utilização para barramentos *ethernet* compartilhados.

Os *switches* também trabalham com um conceito semelhante ao do barramento, que é denominado de *backplane*. No *backplane* passam todos os pacotes que trafegam internamente entre as portas do *Switch*. O *switch* LET36 mantém uma variável contabilizando o percentual de utilização do barramento (*lsBusStatsUtilization*) e também da quantidade de pacotes descartados por falta de recursos no *switch* (*lsBusStatsDropEvents*). O *switch* M770 mantém variáveis relativas à quantidade de octetos que trafegaram no domínio e número de descartes que aconteceram por insuficiência de recursos, respectivamente *scGenMonGoodOctets* e *scGenMonDropEvents*.

5.5.2 Taxa de Erros

A taxa de erros é um forte indicativo da qualidade dos canais de comunicação. O quanto antes for identificada a deterioração da qualidade de um canal de comunicação, mais rápida será a correção do problema. A correção do problema pode ocorrer antes

mesmo que o usuário venha a tomar consciência do mesmo, ou seja, antes que o usuário perceba um aumento no tempo de resposta nas aplicações.

Embora os mecanismos de camada de enlace e de camada de transporte normalmente executem a correção de erros, é importante a medida destes valores, uma vez que eles dão indicação de erros intermitentes ou ruídos na linha que devem ser identificados e corrigidos.

5.5.2.1 Taxa de erros de pacotes

A taxa de erros de pacotes é calculada como uma razão entre a quantidade de erros identificados em uma interface dividido pela quantidade total de pacotes recebidos pela interface. Várias podem ser as causas que originaram um erro no pacote: tamanho fora do padrão do protocolo ou meio físico, erro de CRC, alinhamento ou formato do pacote incorreto. Existem variáveis Cisco identificando todos estes erros, entretanto, recomenda-se o monitoramento do valor genérico de erros da interface (ifInErrors e ifOutErrors) e caso verifique-se algum aumento na quantidade de erros no canal de comunicação, deve-se utilizar as variáveis específicas para identificar o tipo de erro.

Portanto, para calcular a taxa de erro devem ser utilizadas as variáveis de erros e totais de pacotes, incluindo *unicast* e não *unicast*. A fórmula apresentada a seguir deve ser utilizada tanto para erros de entrada quanto de saída, bastando alterar as variáveis *in* por *out*, e aplica-se a todos os equipamentos que mantenham os valores do grupo interfaces da MIB II, incluindo os roteadores Cisco e *Switches* Lucent modelo M770:

$$\text{Taxa de erros} = \frac{\Delta \text{ifInErrors}}{\Delta \text{ifInUcastPkts} + \Delta \text{ifInNUcastPkts}}$$

Como os *hubs* e *switches* LET36 não mantêm informações relativas ao grupo interfaces da MIB II, a taxa de erros deve ser calculada de forma diferente nestes equipamentos. Nos *hubs*, ela deve ser calculada em função da quantidade de pacotes errados que passaram no barramento (`ethBusTotalErrors`) e do número total de pacotes detectados no barramento (`ethBusTotalPackets`), utilizando a seguinte fórmula:

$$\text{Taxa de erros} = \frac{\Delta \text{ethBusTotalErrors}}{\Delta \text{ethBusTotalPackets}}$$

Os *switches* LET36 e M770 mantêm informações relativas a erros por porta e no barramento. O cálculo por porta deve levar em consideração a quantidade de erros na porta (`lsPortInTotalErrors` no LET36 e `scEthPortBadPkts` no M770) e a quantidade de pacotes sem erros recebidos na porta (`lsPortInPkts` no LET36 e `scEthPortGoodPktsRec` no M770). Neste caso, o cálculo seria efetuado utilizando-se a seguinte fórmula:

$$\text{Taxa de erros (LET36) por porta} = \frac{\Delta \text{lsPortInTotalErrors}}{\Delta \text{lsPortInTotalErrors} + \Delta \text{lsPortInPkts}}$$

$$\text{Taxa de erros (M770) por porta} = \frac{\Delta \text{scEthPortBadPkts}}{\Delta \text{scEthPortBadPkts} + \Delta \text{scEthPortGoodPktsRec}}$$

O cálculo da taxa de erros no barramento deve levar em consideração a quantidade de pacotes *ethernet* recebidos com erro (`lsBusStatsBadEthPkts` no LET36 e `scGenMonBadPkts` no M770) e a quantidade de pacotes *ethernet* onde não se constate a presença de erros (`lsBusStatsGoodEthPkts` no LET36 e `scGenMonGoodPkts` no M770). O cálculo deve ser efetuado utilizando-se a seguinte fórmula:

$$\text{Taxa de erros (LET36) barramento} = \frac{\Delta \text{lsBusStatsBadEthPkts}}{\Delta \text{lsBusStatsBadEthPkts} + \Delta \text{lsBusStatsGoodEthPkts}}$$

$$\text{Taxa de erros (M770) barramento} = \frac{\Delta \text{scGenMonBadPkts}}{\Delta \text{scGenMonBadPkts} + \Delta \text{scGenMonGoodPkts}}$$

A taxa de erros tanto nos *links* locais como remotos deve ser sempre muito baixa. O valor ideal para esta taxa é que seja próximo de zero. Nesse sentido, o valor máximo aceitável pode ser estipulado como 1%, acima do qual deve-se tentar identificar e corrigir prontamente o problema.

5.5.2.2 Taxa de colisões

A colisão é uma ocorrência normal e uma situação prevista, sendo automaticamente recuperada em redes *ethernet*. Entretanto, quando o segmento *ethernet* começa a ficar muito utilizado o nível de colisões se eleva dificultando a comunicação.

Tanto o RFC 1643 (Dot3) quanto a MIB Cisco definem variáveis para manutenção de valores de colisões experimentadas nas interfaces *ethernet*. Como na MIB Dot3 os valores de colisão estão computados em diversas variáveis e na MIB Cisco o valor pode ser obtido a partir de uma única variável, propõe-se que para verificação de taxa de colisões nas interfaces *ethernet* dos roteadores seja utilizada a variável da MIB Cisco, aplicando-se a seguinte fórmula:

$$\text{Taxa de colisões} = \frac{\Delta \text{locIfCollisions}}{\Delta \text{ifOutUcastPkts} + \Delta \text{ifOutNUcastPkts}}$$

Para os *hubs* Lannet, deve-se utilizar a MIB proprietária que mantém a variável que registra a quantidade de colisões no barramento do *hub* (*ethBusTotalCollisions*) e compará-la ao total de pacotes que passaram pelo barramento (*ethBusTotalPackets*), utilizando a seguinte fórmula:

$$\text{Taxa de colisões} = \frac{\Delta\text{ethBusTotalCollisions}}{\Delta\text{ethBusTotalPackets}}$$

Os switches LET36 e M770 também implementam a MIB proprietária Lannet. Entretanto, as variáveis de colisão são mantidas por porta, da mesma forma que na MIB Cisco. Neste caso deve-se monitorar por porta as variáveis relativas ao número de colisões (IsPortInCollisions no LET36 e scEthPortCollisions no M770) e comparar este número ao total de pacotes que entraram na porta, utilizando-se a seguinte fórmula:

$$\begin{array}{l} \text{Taxa de colisões (LET36)} = \frac{\Delta\text{IsPortInCollisions}}{\Delta\text{IsPortInTotalErrors} + \Delta\text{IsPortInPkts}} \\ \text{por porta} \end{array}$$

$$\begin{array}{l} \text{Taxa de colisões (M770)} = \frac{\Delta\text{scEthPortCollisions}}{\Delta\text{scEthPortBadPkts} + \Delta\text{scEthPortGoodPktsRec}} \\ \text{por porta} \end{array}$$

Muito embora não haja um consenso entre os autores com relação aos níveis de colisão aceitáveis, pode-se estipular um limiar de 3% sobre o total de pacotes enviados. Quando este limiar for ultrapassado com frequência deve-se tentar identificar as causas do número excessivo de colisões, que podem ser devidas ao excesso de utilização do segmento, a algum equipamento com placa de rede apresentando problemas ou mesmo a tempestades de *broadcast*.

5.5.2.3 Taxa de broadcast/multicast

O monitoramento da quantidade de pacotes de *broadcast/multicast* na rede é muito importante para identificar as chamadas tempestades de *broadcast* (*broadcast storm*), que se caracterizam por uma quantidade muito grande de pacotes de *broadcast* chegando na rede e que são recebidos por todos os computadores. A tempestade de *broadcast* normalmente é calculada em função de uma certa quantidade de pacotes de *broadcast* fluindo na rede no mesmo segundo, alguns autores defendem que 100 pacotes

de *broadcast* por segundo já caracterizam uma tempestade, enquanto outros autores defendem este número em 500 pacotes por segundo. Em função do aumento da velocidade das tecnologias, optou-se por considerar-se *broadcast storm* como ocorrências de mais de 500 pacotes não *unicast* em um segundo.

Em caso de tempestades de *broadcast* ocorrerem com frequência na rede, certamente o tempo de resposta das aplicações será afetado, uma vez que estes pacotes fluem para toda a rede e são recebidos por todos os equipamentos conectados. É interessante monitorar-se a relação entre pacotes não *unicast* sobre o total de pacotes, utilizando-se a seguinte fórmula:

$$\text{Taxa de } broadcast = \frac{\Delta \text{InNUcastPkts}}{\Delta \text{InUcastPkts} + \Delta \text{InNUcastPkts}}$$

Como foi dito anteriormente, os *Switches* Lannet LET36 não mantêm informações relativas ao grupo interfaces da MIB II e, portanto, estas informações devem ser buscadas em sua MIB proprietária. Na MIB Lannet, implementada pelo LET36, as informações sobre quantidades de pacotes *broadcast* e *multicast* não são mantidas por porta e sim por barramento. Dessa forma, deve-se levar em consideração a quantidade de pacotes de *broadcast* (`lsBusStatsEthBroadcastPkts` no LET36 e `scGenMonGoodBroadcastPkts` no M770), *multicast* (`lsBusStatsEthMulticastPkts` no LET36 e `scGenMonGoodMulticastPkts` no M770) e pacotes sem erro (`lsBusStatsGoodEthPkts` no LET36 e `scGenMonGoodPkts` no M770) que passaram pelo barramento. Para o cálculo da taxa de *broadcast* utiliza-se a seguinte fórmula:

$$\text{Taxa de } broadcast = \frac{\Delta \text{lsBusStatsEthBroadcastPkts} + \Delta \text{lsBusStatsEthMulticastPkts}}{\Delta \text{lsBusStatsGoodEthPkts}} \text{ (LET36)}$$

$$\text{Taxa de } broadcast = \frac{\Delta scGenMonGoodBroadcastPkts + \Delta scGenMonGoodMulticastPkts}{\Delta scGenMonGoodPkts} \quad (M770)$$

5.5.2.4 Taxa de retransmissão

O protocolo TCP/IP implementa na camada de transporte o protocolo TCP, que é orientado à conexão e com confirmação. Se o segmento TCP chega correto no destino, uma confirmação é enviada para a origem. Como o protocolo TCP/IP não implementa reconhecimento negativo, se houver algum erro na transmissão, em qualquer ponto intermediário entre origem e destino, o pacote é descartado. A recuperação do erro ocorre através de um processo de medida de tempo de confirmação para cada segmento transmitido. É definido um tempo máximo de espera de confirmação de recebimento, se este tempo for ultrapassado, o segmento é retransmitido. Dessa forma, tempos elevados de resposta, descartes de pacotes por qualquer motivo e erros de CRC, implicam em retransmissão de pacotes.

A MIB II implementa contadores de ocorrências relativas ao protocolo TCP. Essa contabilização ocorre somente na origem e destino da conexão TCP. Sugere-se o monitoramento do nível de retransmissão (`tcpRetransSegs`) e da quantidade de conexões reinicializadas (`tcpEstabResets`) a fim de identificar-se problemas na comunicação dos servidores críticos. Para verificação do nível de retransmissão de segmentos tcp utiliza-se a seguinte fórmula:

$$\text{Taxa de retransmissão} = \frac{\Delta tcpRetransSegs}{\Delta tcpOutSegs}$$

Sugere-se que taxas de retransmissão superiores a 5% sejam consideradas problemáticas e que sejam localizadas e solucionadas as causas destas retransmissões.

5.5.2.5 Taxa de erros de acesso SNMP

Muito embora as taxas de erro SNMP não afetem diretamente a performance da rede, é muito interessante o monitoramento das variáveis SNMP que dizem respeito a tentativas mal sucedidas de acesso ou alteração de informação nos equipamentos. A observação das variáveis que informam número de tentativas de acesso a informações SNMP com comunidade incorreta (`snmpInBadCommunityNames`) e de tentativa de execução de operação não permitida para a comunidade (`snmpInBadCommunityUses`) deve ser considerada pois podem revelar tentativas de quebra de segurança na rede.

5.5.3 Congestionamento

5.5.3.1 Taxa de congestionamento dos circuitos Frame Relay

Conforme abordado no início do capítulo, o protocolo Frame Relay utiliza *flags* nos quadros para informar a existência de congestionamento na rede. Faz-se necessário o monitoramento desses *flags* pois eles informam da possibilidade de descarte de pacotes na rede WAN.

O RFC 1315 (MIB Frame Relay), implementado pelos roteadores Cisco, define variáveis que monitoram a quantidade de quadros recebidos com o *flag* BECN ativado (`frCircuitReceivedBECNs`), com o *flag* FECN ativado (`frCircuitReceivedFECNs`) e total de quadros recebidos no circuito virtual (`frCircuitReceivedFrames`). Com base nestes valores pode-se calcular a quantidade de quadros por circuito que possuem informações de congestionamento utilizando-se a fórmula:

$$\text{Taxa de congestionamento} = \frac{\Delta \text{frCircuitReceivedBECNs} + \Delta \text{frCircuitReceivedFECNs}}{\Delta \text{frCircuitReceivedFrames}}$$

Pode-se definir como um limite tolerável até 20% de presença de congestionamento nos circuitos Frame Relay. Ultrapassado este limite deve-se identificar se o congestionamento está acontecendo no caminho de ida (elevado BECN) ou no caminho de volta (elevado FECN) e tomar medidas similares àquelas sugeridas para elevadas taxas de utilização de interfaces.

5.5.3.2 Congestionamentos de filas do roteador

O congestionamento das filas do roteador pode ser identificado através de descartes que começam a ocorrer em função do aumento do tamanho da fila sem que o roteador consiga encaminhá-los na mesma velocidade. Esse processo causa um aumento no tamanho das filas até que começa a acontecer o descarte de pacotes em função do buffer ficar lotado e não haver mais local para armazenamento.

A MIB Cisco possui variáveis que medem a quantidade de pacotes descartados na fila de entrada (`locIfInputQueueDrops`) e na fila de saída (`locIfOutputQueueDrops`).

A taxa de descartes de pacotes pode ser calculada com a seguinte fórmula:

$$\text{Taxa de descartes (entrada)} = \frac{\Delta \text{locIfInputQueueDrops}}{\Delta \text{ifInUcastPkts} + \Delta \text{ifInNUcastPkts}}$$

A taxa de descarte de saída pode ser calculada utilizando-se a mesma fórmula substituindo-se os valores de entrada pelos valores de saída. A taxa de descartes deve ser próxima de zero. Quando descartes começarem a ocorrer nas interfaces deve ser gerado um alarme para a estação de gerência para que o problema seja examinado e solucionado.

5.5.4 Responsividade dos *links*

5.5.4.1 Medida de tempo de resposta (RTT)

Deve-se medir o tempo que um pacote leva para fazer o caminho de ida e volta aos pontos remotos da rede, esse tempo é conhecido como *round trip time* (RTT). Haugdahl (2000, p.315), define que tipicamente o Frame Relay leva 30ms para percorrer o caminho de ida, o que perfaz 60ms de RTT uma boa aproximação para esta medida. Entretanto, quando existem saltos de satélite, essa medida pode aumentar para aproximadamente 600ms.

O comando ping provê dois serviços básicos. Ele pode ser usado para determinar se um dispositivo remoto está alcançável e a ajudar a solucionar problemas de conectividade. Segundo, ele pode prover estatísticas rudimentares de performance de rede, que podem ser usadas para diagnosticar problemas de rede relativos a tráfego. Propõe-se então a manutenção de medidas periódicas do RTT dos diversos circuitos remotos e a comparação com valores levantados no *baseline* para identificação de mudanças no comportamento da rede. Estas medidas podem também fornecer informações valiosas para identificação de problemas em caso de reclamação dos usuários. Recomenda-se que os valores de RTT façam parte da negociação de SLA com os provedores de serviço de telecomunicações.

5.5.4.2 Medida de vazão (EFT)

Conforme levantado no item 3.5, não basta monitorar-se somente o RTT dos circuitos, é importante também o monitoramento da vazão dos circuitos de comunicação, que é a capacidade efetiva de transmissão de informações no circuito.

Propõe-se que, no estabelecimento do *baseline* seja levantada também a vazão de cada circuito de comunicações e que esses valores sejam monitorados periodicamente da mesma forma que o RTT. A vazão mínima dos circuitos Frame Relay deve ser a banda garantida do circuito (CIR) e, caso o valor encontrado para algum circuito esteja abaixo do CIR, providências de identificação e correção do problema devem ser tomadas junto aos provedores de serviços de telecomunicações.

Embora seja uma medida importante para os circuitos remotos, o EFT deve ser levantado mesmo em redes locais quando existem casos de reclamação de baixa performance das aplicações em redes locais.

5.5.5 Disponibilidade

Problemas nos canais de comunicação podem causar a reinicialização das interfaces. A MIB Cisco contabiliza as reinicializações das interfaces na variável `locIfResets`, que indica o número de vezes que a interface foi reinicializada internamente. Esse valor deve ser sempre zerado pois reinicializações das interfaces indicam a ocorrência de problemas e devem ser prontamente sinalizadas às estações de gerência.

5.5.6 Estabelecimento de *Baseline*

Todos os valores levantados anteriormente, além de servirem para monitoramento da rede servem também para estabelecimento do comportamento normal da rede (*baseline*). No entanto, outros valores devem ser levantados para estabelecimento de *baseline*, onde nestes casos não se aplica o estabelecimento de limiares.

5.5.6.1 Utilização por protocolo

No processo de estabelecimento de *baseline* é muito importante a contabilização de quanto da banda utilizada está sendo consumida por cada protocolo. Esse levantamento pode ser feito utilizando-se analisadores de protocolo ou equipamentos que implementem RMON2. Esse levantamento deve ser refeito periodicamente a fim de verificar se ocorreram mudanças no comportamento da rede. Sugere-se o levantamento da utilização da banda por protocolo seja feita na rede WAN e também separado por unidade remota.

5.5.6.2 Utilização de tamanhos de pacote

Outra informação importante a ser levantada no processo de estabelecimento de *baseline* é a distribuição de tamanho de pacotes. Pacotes de tamanho muito pequeno podem gerar aumento significativo no tempo de resposta de aplicações, uma vez que o *overhead* de tráfego aumenta bastante e também em função da necessidade de envio e confirmação de recebimento de mais pacotes. Dessa forma, pacotes de tamanho pequeno tendem a afetar negativamente a performance. O tamanho dos pacotes é determinado fundamentalmente por três fatores: a rede física, o sistema operacional e a aplicação.

Haugdahl (2000, p.46), defende que uma das providências a serem tomadas para melhorar a performance de uma rede *ethernet* é otimizar as aplicações e protocolos para manter o tamanho médio de pacotes alto. Isto diminuiria o número de colisões e o *overhead* de protocolo, maximizando a utilização da banda. Ele defende que o tamanho médio do quadro deveria ser maior do que 300 bytes.

5.5.6.3 Distribuição por destino

Depois de fazer análise de utilização e de distribuição de pacote por tamanho, deve-se identificar as estações/servidores que mais geram/recebem tráfego e analisar o tráfego destes dispositivos.

5.6 Fase 6 – Especificação Funcional das Ferramentas

Muito embora a fase de especificação funcional das ferramentas esteja um pouco prejudicada neste trabalho, em função de alguns produtos já terem sido adquiridos, um conjunto de funcionalidades é requerido para uma implementação adequada do gerenciamento:

- ✓ Integração – é necessário que possa haver uma integração entre as diversas ferramentas, possibilitando, por exemplo, que quando seja identificado algum problema pela ferramenta de gerência, automaticamente seja aberto um chamado no sistema de *Help Desk*;
- ✓ Suporte a diversos protocolos – é necessário que as ferramentas suportem, pelo menos, os protocolos SNMPv1, SNMPv2 e RMON. É altamente desejável que elas também apresentem suporte a SMON;
- ✓ Programação de ações – as ferramentas devem permitir o estabelecimento de limiares e a execução de ações programadas quando estes limiares forem atingidos/ultrapassados;
- ✓ Acesso Web – é importante a disponibilização de informações via *browser*, facilitando o acesso de qualquer ponto, por qualquer usuário sem a necessidade de instalação de *software* adicional nas estações;

- ✓ Versão para NT – como o Windows NT é a plataforma padrão atualmente utilizada no TCU, é altamente desejável que as ferramentas de gerência possuam versão que execute neste sistema operacional;
- ✓ Suporte a MIBs proprietárias – em função dos equipamentos utilizados na rede de computadores do TCU implementarem MIBs proprietárias é exigido que as ferramentas de gerência suportem MIBs estendidas e que possuam compiladores de MIB;
- ✓ Geração de relatórios – é necessária a emissão de relatórios de problemas e que subsidiem a verificação do cumprimento do SLA;
- ✓ Recebimento de *traps* – no caso de recebimento de *traps* enviados pelos equipamentos gerenciados, as ferramentas devem possibilitar a visualização dos *traps* recebidos e também a implementação de ações quando determinados *traps* ocorrerem;
- ✓ Várias consoles – a existência de múltiplas consoles é necessária em função da necessidade de acesso permanente a informações de gerenciamento por diversos setores (e.g. suporte a rede, suporte a banco de dados, atendimento ao usuário, etc).

5.7 Fase 7 – Implementação e Integração

Inicialmente, foi configurado o SNMP em todos os equipamentos a serem gerenciados, conforme descrito no Anexo V. O *software* de Help Desk (AHD) já estava instalado e em operação, foi simplesmente configurado para permitir a abertura de chamados através de recebimento de e-mail ou *traps* SNMP, que podem ser enviados a partir de diversos *softwares*/equipamentos.

O *software* Unicenter TNG, que atende a todos os requisitos funcionais descritos e que já havia sido adquirido pelo TCU, foi instalado e configurado para gerenciar os roteadores e *switches* da rede, que foram incluídos através de um processo de descoberta baseado em suas faixas de endereço ip. Foi providenciada também a integração entre os *softwares* Unicenter e o AHD e a disponibilização das informações através de *browser*, como era um dos requisitos do sistema de gerenciamento.

Outra ferramenta utilizada para coleta e disponibilização de informações foi o MRTG (*Multi Router Traffic Grapher*). O MRTG consiste em um conjunto de *scripts* perl que efetuam a leitura de contadores de tráfego e outras variáveis SNMP em equipamentos de rede e programas em linguagem C que geram logs dos valores encontrados e gráficos representando o tráfego na conexão de rede monitorada ou identificadores de objetos solicitados. Além de monitorar variáveis SNMP ele permite que sejam executadas operações sobre os valores retornados por estas variáveis, bem como a chamada de programas externos para monitoração de valores não SNMP ou execução de outros programas/*scripts*. Outra característica importante do MRTG é que, além dele gerar gráficos dos valores recuperados nas últimas 24 horas, ele gera gráficos consolidados por dia na última semana, por semana no último mês e por mês no último ano.

5.7.1 Configuração do MRTG

A ferramenta MRTG foi desenvolvida por Tobias Oetiker para suprir uma necessidade de monitoração dos *links* internet de sua empresa. A primeira versão, escrita totalmente em perl, foi denominada de MRTG 1.0 liberada em 1995. Depois de

desenvolvidas algumas rotinas críticas em C foi liberada ao público a versão 2.0. A última versão disponível é a 2.9.12 e foi disponibilizada em abril de 2001.

Por utilizar perl e C, o MRTG pode executar tanto sobre sistema operacional Windows NT quanto no Unix. No TCU foram instaladas as duas versões, a versão NT utiliza um serviço (MRTGSvc – MRTG Statistic Updater) que é configurado para executar periodicamente na quantidade de minutos configurada e a versão linux executa periodicamente de acordo com o arquivo crontab configurado. O servidor NT foi escolhido por já estarem nele instalados os softwares de gerenciamento de rede, enquanto o linux foi escolhido como plataforma padrão onde serão instalados os coletores de dados dos diversos sites remotos, uma vez que outras ferramentas de gerenciamento também serão instaladas nesta plataforma e também pelo fato do linux requerer equipamentos de menor porte que seriam facilmente disponibilizados para este fim. Essa implementação garante, ao mesmo tempo, um tráfego mínimo na WAN, uma vez que os equipamentos que farão os acessos SNMP encontram-se localizados na mesma rede local que os equipamentos gerenciados, ao mesmo tempo em que permite a continuidade da coleta de informações em caso de queda dos *links* WAN.

Baseado nas variáveis cujos valores deveriam ser coletados de acordo com o item 5.5 e nos identificadores de objetos levantados como passíveis de monitoração, listados no Anexo I, foram configurados para levantamento de dados do MRTG. Cópias de partes destes arquivos de configuração que geram os gráficos já disponibilizados aos usuários estão listadas no Anexo III.

5.7.2 Configuração de alarmes RMON nos equipamentos

Como os roteadores Cisco utilizados na rede local implementam os grupos *events* e *alarms* do RMON, decidiu-se pela monitoração de taxas de erros e *resets* nas interfaces, configurando-se eventos e gerando registro de *logs* e *traps snmp*, caso os limiares sejam atingidos. Antes da implementação de monitoramento RMON nos roteadores foi feito o acompanhamento de suas taxas de utilização de CPU, uma vez que a ativação desse recurso consome muito processamento. Os comandos utilizados para ativação do RMON e do SNMP encontram-se listados no Anexo V.

5.7.3 Análise de tráfego

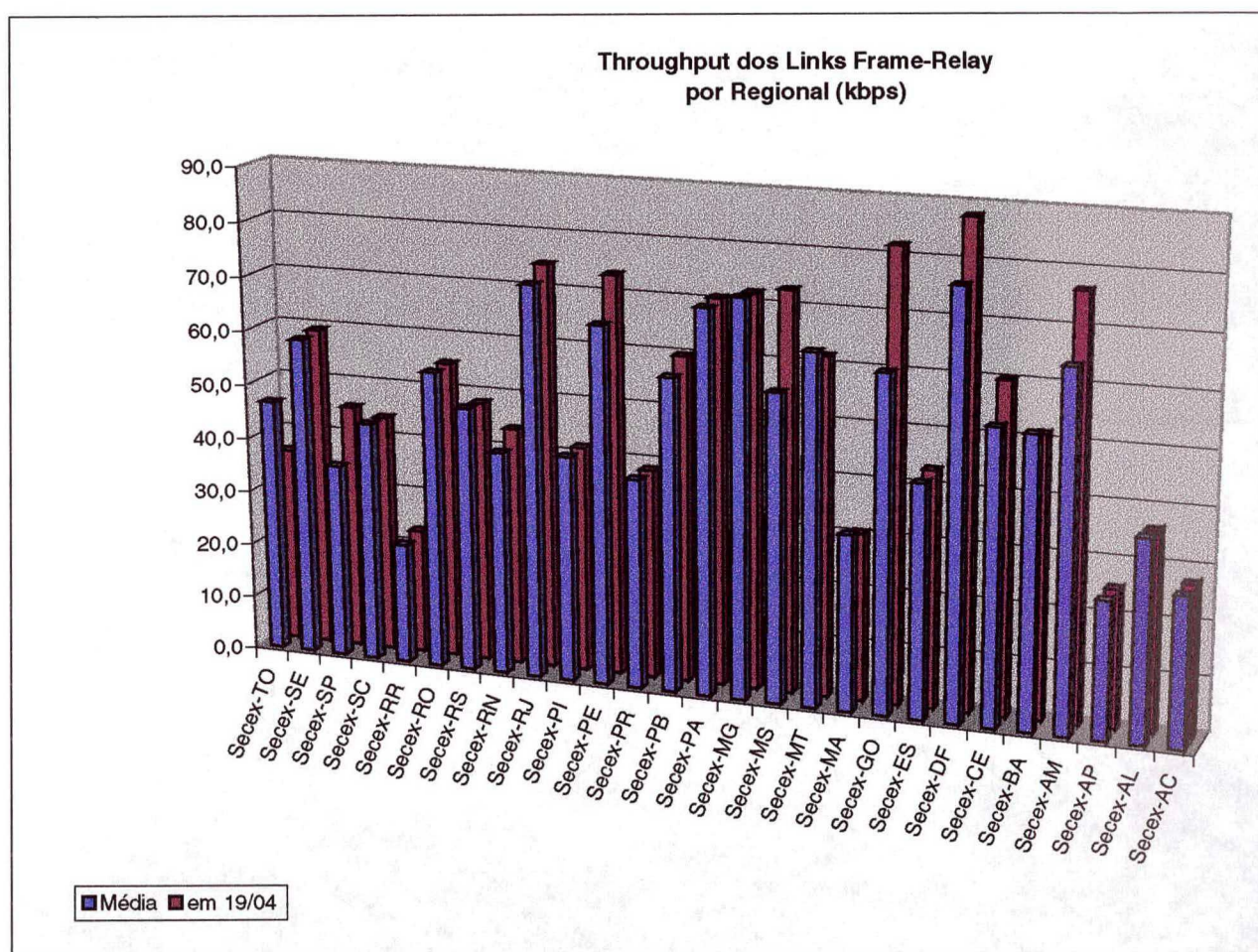
5.7.3.1 Vazão

Para análise da taxa de transmissão dos canais foi utilizado o programa *Ws_Ping Pro* comercializado pela *Ipswitch*. Este programa é um conjunto integrado de ferramentas de levantamento de informações e diagnóstico da rede. Além de fornecer uma interface gráfica para as ferramentas mais comuns utilizadas na internet (e.g. ping, traceroute, DNS lookup, snmp, etc.) ele possui uma ferramenta para análise de velocidade de transferência entre o computador local e qualquer dispositivo remoto que implemente o TCP/IP.

Para levantamento da taxa efetiva de transferência entre a sede do TCU e as diversas Secretarias nos estados, foi utilizada a funcionalidade de *throughput* do *Ws_Ping* para identificar a vazão do PVC Frame Relay para cada estado. Este levantamento foi feito durante duas semanas em horário de pico, utilizando como parâmetros do programa: 50 pacotes, *timeout* de 1 segundo e tamanho de pacote de

1.400 bytes. Os dados obtidos foram passados para uma planilha Excel que gerou o gráfico apresentado na figura 5.5, representando a vazão média dos circuitos no período. Optou-se por gerar, além da vazão média, um gráfico com a vazão em determinado dia para permitir a comparação em caso de verificação de queda de performance em algum circuito.

Figura 5.5 – Vazão média dos circuitos Frame Relay

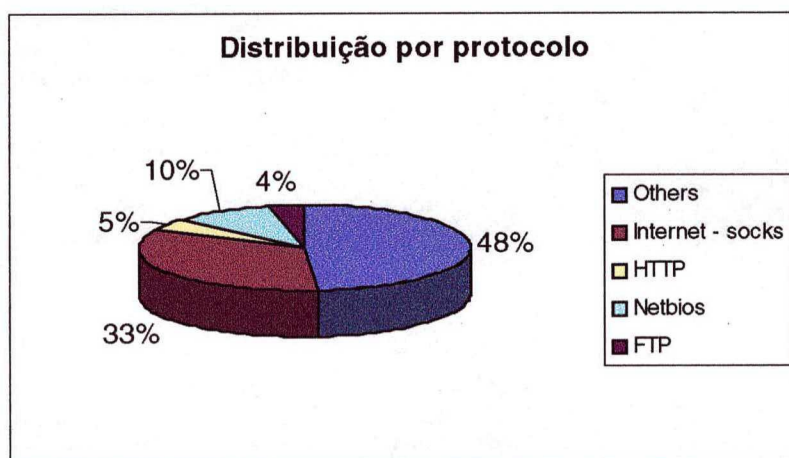


5.7.3.2 Distribuição por protocolo/destino

Para a análise da distribuição do tráfego por protocolo na rede Frame-Relay foi utilizado o *software* Sniffer da Network Associates. O Sniffer é um analisador de

protocolo que permite a configuração de critérios de seleção para definir qual o tráfego deve ser capturado. Para efeito do levantamento da distribuição por protocolo foi efetuada a captura durante quinze dias nas duas horas de pico de todo o tráfego entre Sede e Secretarias regionais. Os arquivos resultantes do tráfego capturado tiveram seu tráfego analisado por protocolo, gerando o gráfico de distribuição de tráfego da rede WAN por protocolo, apresentado na figura 5.6.

Figura 5.6 – Distribuição do tráfego WAN por protocolo

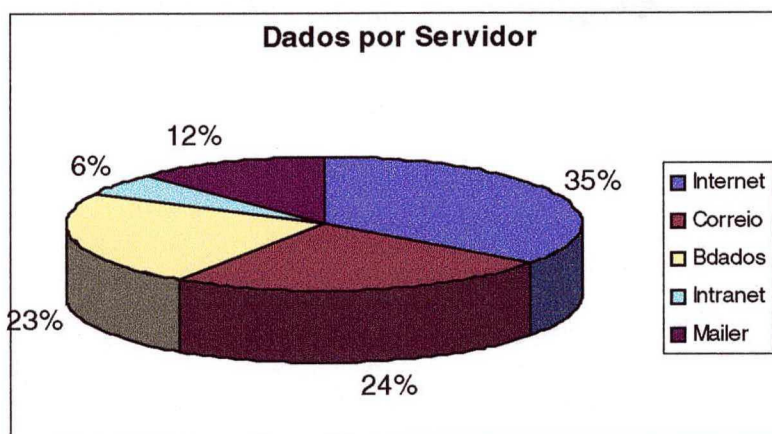


O tráfego classificado como outros (*others*) engloba todo o tráfego de correio eletrônico, acesso a banco de dados e qualquer outra aplicação servidora que trabalhe em portas variáveis. A separação entre o tráfego internet, HTTP e FTP ocorre porque todo o tráfego para a internet é feito através de socks utilizando uma porta específica, desta forma o tráfego classificado como HTTP e FTP é tráfego destes protocolos na intranet do TCU.

Como na rede do TCU serviços diferentes são fornecidos por servidores diferentes, pode-se obter uma visualização melhor do tráfego classificado como outros

na distribuição por protocolo se for feita a análise da distribuição por servidor, apresentada na figura 5.7.

Figura 5.7 – Distribuição do tráfego WAN por servidor



5.7.3.3 RTT

A análise do tempo de ida e volta dos pacotes foi implementada através do programa Whastup da Ipswitch. Este programa além de verificar se equipamentos e serviços estão funcionando, mantém histórico de médias diárias de tempo mínimo, médio e máximo de RTT dos dispositivos, utilizando *echo request* com pacotes de 50 bytes de dados (total de 92 bytes, incluindo os *headers*). Os valores de RTT podem ser recuperados por período para os dispositivos requeridos e também por dia para um período especificado para um ou vários dispositivos. A figura 5.8 mostra o gráfico obtido como tempo médio e máximo para todos os circuitos Frame Relay no mês de abril, enquanto a figura 5.9 mostra, por dia, os valores mínimo, médio e máximo para o circuito de São Paulo no mês de abril

Figura 5.8 – RTT dos circuitos Frame Relay no mês de abril/2001

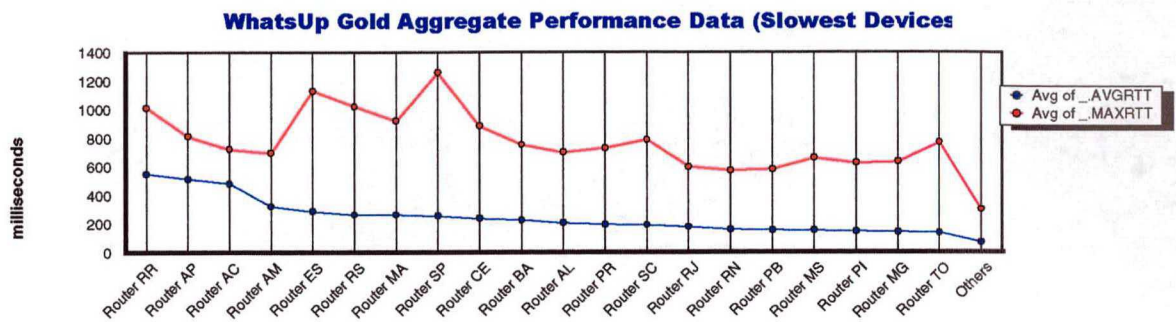
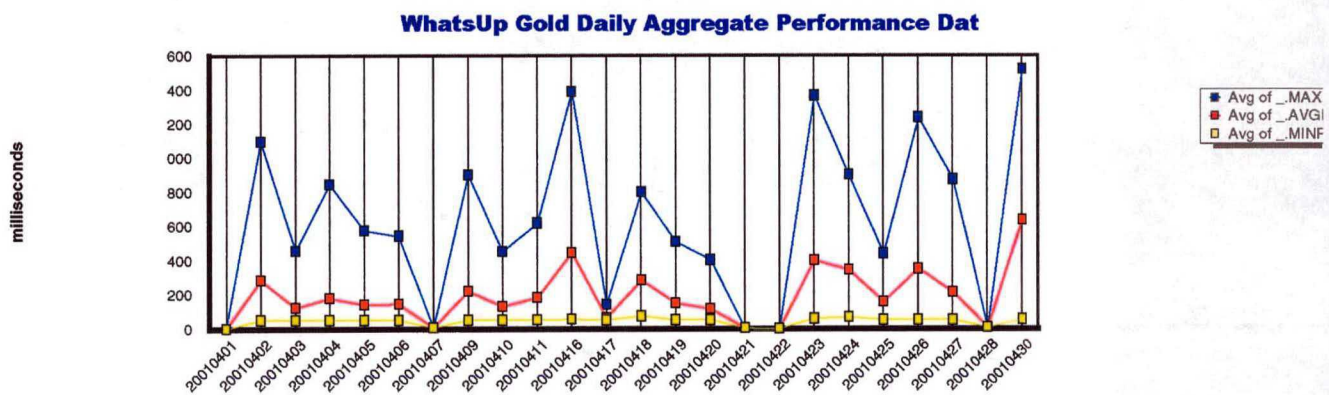


Figura 5.9 – Média diária de RTT do circuito de São Paulo no mês de abril/2001



5.7.3.4 Tamanho dos pacotes

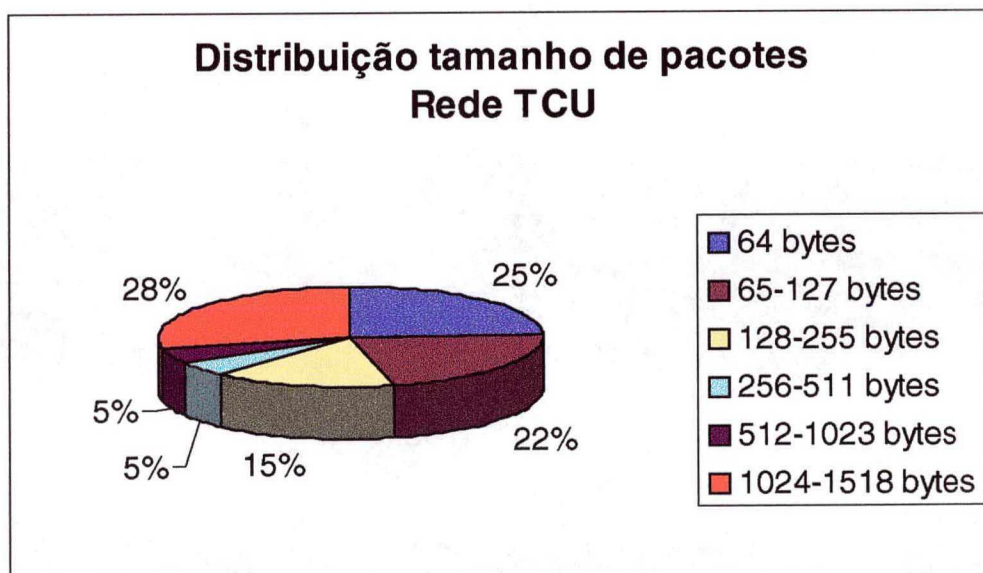
Para análise da distribuição de pacotes por tamanho foram utilizadas as variáveis relativas a quantidade de pacotes por tamanho em cada porta do *switch* central, por onde passam todos os pacotes da rede local. Foi programado que duas vezes ao dia (12:00h e 20:00h), em dias úteis, um micro com linux coletasse estas informações. Estes horários foram escolhidos pois neste período certamente os procedimentos de cópia de segurança não estão sendo executados e também por ser o período em que se concentra o maior volume de tráfego da rede local, obtendo-se, desta forma, um retrato mais fiel do comportamento do tráfego das aplicações de rede. Para obtenção destas informações utilizou-se o *script* `snmpwalk` para o ramo da MIB Lannet que disponibiliza estas

informações, gerando a saída em um arquivo. Antes da execução do comando executou-se o comando `date` simplesmente para saber a data e hora correta de geração das informações. Os comandos utilizados foram:

```
Date >> arquivo_saida  
Snmpwalk endereço_ip community .1.3.6.1.4.1.81.28.2.1.1.1 >> arquivo_saida
```

Posteriormente, as informações obtidas a partir do arquivo gerado no passo anterior foram transportadas para uma planilha Excel, possibilitando a geração de gráficos indicando a distribuição dos pacotes por tamanho, conforme mostra a figura 5.10. A partir desta planilha gerou-se também gráficos representando a distribuição dos pacotes por tamanho em cada tipo de aplicação, uma vez que as aplicações diferentes são implementadas por servidores de redes diferentes e, portanto, em diferentes portas do *switch* central. Os gráficos de distribuição de tamanho de pacotes por aplicação estão listados no Anexo II.

Figura 5.10 – Distribuição dos pacotes por tamanho



5.7.4 Análise da banda consumida no processo de gerenciamento

A banda consumida no processo de gerenciamento, ou volume de tráfego de gerenciamento em determinado período, não deve afetar significativamente a rede que está sendo monitorada. O volume de tráfego depende basicamente dos seguintes fatores:

- ✓ da quantidade de dispositivos sendo monitorados;
- ✓ do número de requisições (*get*) feitas para estes dispositivos e da quantidade de variáveis retornadas por solicitação;
- ✓ do intervalo de tempo entre solicitações, ou seja, o tempo gasto para processar a resposta recebida e efetuar nova solicitação;
- ✓ do tempo gasto para que a solicitação chegue ao dispositivo, seja processada e retorne ao solicitante.

A melhor maneira para levantar estes valores é utilizando-se analisadores de protocolo para capturar todo o tráfego de gerenciamento na rede. Isto foi feito utilizando-se o *software* Sniffer, fazendo com que todo o tráfego direcionado ao servidor de gerenciamento fosse copiado para outra porta do *switch* e capturando todo o tráfego SNMP. Essa medida foi feita em momentos que a rede estava praticamente sem tráfego e os dispositivos estavam com utilização mínima. Dessa forma, o tempo de resposta das solicitações, de retardo da rede, de tratamento da resposta pelo gerente e geração de nova solicitação seria o menor possível. Como o tempo de geração e resposta de solicitações é o menor possível e o volume de informações permanece inalterado, esta seria a situação com maior utilização de banda pelo processo de gerenciamento.

Verificou-se que, para cada gráfico gerado pelo MRTG, uma solicitação SNMP, contendo quatro variáveis, é efetuada para o dispositivo gerenciado. Como estão sendo gerados os gráficos nas quantidades expressas no quadro 5.2, observa-se que a quantidade total de solicitações seria de 365 acompanhadas do mesmo número de respostas.

Quadro 5.2 – Quantidade de gráficos para monitoração

	Router 254	Router 251	M770	LET36
Utilização	Por interface = 3 Por Sub-interface = 27 CPU = 1 Memória = 2	Por interface = 2 CPU = 1 Memória = 2	Por porta = 52	Por porta = 17 Do barramento = 1
Quantidade de pacotes	Por interface = 3	Por interfaces = 2	Por porta = 52	Junto com utilização = 0
Erros	Por interface = 3	Por interface = 2	Por porta = 52	Por porta = 17 No barramento = 1
Taxa de pacotes não <i>unicast</i>	Por interface = 3	Por interface = 2	Por porta = 52	No barramento = 1
Taxa de descartes	Por interface = 3	Por interface = 2		No barramento = 1
Reinicializações de interface	Por interface = 3	Por interface = 2		
Colisões	Interfaces eth = 1	Interfaces eth = 1		
Quadros recebidos	Por DLCI = 27			
Taxa de congestionamento	Por DLCI = 27			
Total	103 gráficos	16 gráficos	208 gráficos	38 gráficos

Observou-se que o menor tempo para receber uma solicitação seria de 7 milissegundos, que foi a resposta do *switch* conectado diretamente ao computador que estava coletando as informações. Observou-se, também, um intervalo de 5 milissegundos entre o recebimento de uma resposta e a geração de uma nova solicitação, totalizando um tempo mínimo de 12 milissegundos para completar um ciclo de solicitação, recebimento e tratamento da informação. Desta forma, em 1 segundo seria possível a geração de 83 solicitações ($1000/12$) em 1 segundo. Como o tamanho máximo observado para os pacotes de solicitação foi de 140 bytes e o tamanho máximo dos pacotes de resposta foi de 200 bytes, tem-se que o tráfego de gerência máximo seria de

225.760 bps (num. de bytes por solicitação * num. bits por byte * num. de solicitações = $340 * 8 * 83$). Este tráfego, que seria o pior caso, ocorre somente entre o computador que solicita o tráfego e o *switch* M770, consumindo somente 0,23% da banda (225.760 bps / 100 Mbps), o que é um consumo muito abaixo de 5%, definido por Oppenheimer (2000, p.48) como limite aceitável para tráfego de gerenciamento.

No caso da banda consumida para acesso aos dados dos roteadores esse cálculo deve ser feito uma vez que os mesmos utilizam um canal de 10Mbps. Verificando o pior caso que é o do roteador utilizado para interligar Sede e Regionais, a banda utilizada para gerenciamento deve ser multiplicada por 10 (relação de 10:1 entre *fast-ethernet* e *ethernet*). Mesmo assim, a banda consumida seria somente de 2,3% do canal. Levando-se em consideração que os valores foram levantados para o pior caso e que as solicitações são periódicas e não constantes, conclui-se que o tráfego de gerenciamento será sempre inferior a este valor e que só se aproximará dele em momentos de pico. Deve-se observar também que a solução adotada é de ter computadores efetuando localmente a coleta de informações, não sendo consumida, portanto, a banda da rede WAN, caso em que o consumo poderia comprometer a utilização dos *links* de comunicação e o processo de medição estaria influenciando bastante nos resultados obtidos.

5.8 Fase 8 – Revisão dos Resultados

Os dados obtidos a partir da monitoração contínua ou coleta durante períodos significativos levou a algumas conclusões interessantes:

- ✓ Em termos de utilização de CPU, memória e barramentos todos os equipamentos monitorados apresentavam folga considerável, não sendo necessário pensar em nenhum tipo de *upgrade* em pouco tempo;
- ✓ Em termos de utilização de interfaces e *links* de comunicação, constatou-se, conforme previsto, saturação em *links* de acesso Frame Relay de algumas regionais e também da internet. Para solução dos problemas das regionais recomendou-se o aumento da capacidade dos circuitos congestionados, para o acesso à internet recomendou-se, além do aumento da capacidade do *link*, a adoção de *cache* Web que, além de diminuir o tráfego naquele circuito, traria melhorias significativas no tempo de resposta para sites muito acessados;
- ✓ Embora tenha sido verificado que nenhuma das portas dos *switches* encontrava-se com utilização em níveis preocupantes, observou-se em uma porta específica (servidor de intranet), tráfego fora do padrão de normalidade para a aplicação. Isto levou a uma análise mais apurada do problema utilizando *port mirror* e captura de tráfego para identificação do problema e posterior solução.
- ✓ Verificou-se também que algumas aplicações de grande vazão poderiam aproveitar melhor a capacidade das portas do *switch*, diminuindo assim o tempo necessário para seu processamento. Como a vazão máxima de um *link* pode ser obtida pelo produto de banda * rtt, e como, para obter-se tráfego próximo desta vazão máxima o valor da janela TCP deve ser maior ou igual a este valor. Neste caso identificou-se que o problema era o tamanho da janela TCP configurada nos servidores; aumentou-se a janela e observou-se um aumento significativo na vazão;
- ✓ As taxas de erros de todas as conexões estavam em níveis aceitáveis, com exceção do elevado nível de colisões observado na porta *ethernet* de um dos roteadores, o

que levou a uma segmentação da rede. Esse problema não era esperado, uma vez que o tráfego de saída era muito inferior aos 10 Mbps do segmento compartilhado. Como dois roteadores compartilhavam o mesmo segmento, optou-se por ligar o roteador de maior tráfego diretamente em uma porta do *switch* central;

- ✓ A análise dos *links* Wan em termos de tempo de resposta correspondeu às expectativas, entretanto a vazão de alguns circuitos apresentou-se inferior ao esperado, o que levou à conversações com a prestadora de serviço de comunicações para que revisasse a configuração do CIR para estes PVCs.
- ✓ A taxa de utilização por protocolo identificou um tráfego internet superior ao esperado. Entretanto este problema está diretamente relacionado ao problema de tamanho médio de pacotes pequeno para o tráfego de acesso ao banco de dados pelas aplicações cliente servidor. Este problema deve ser investigado em conjunto pela equipe de banco de dados e de desenvolvimento de sistemas, a fim de obter-se maior eficiência nos aplicativos;
- ✓ Por fim, observou-se que a implementação do gerenciamento não sobrecarregou os equipamentos de rede e nem gerou tráfego excessivo, ficando dentro do previsto e muito abaixo do limite aceitável.

CAPÍTULO VI – CONCLUSÕES

6.1 Considerações e Contribuições

Este trabalho apresentou os conceitos básicos relativos a sistemas de gerenciamento de redes de computadores, destacando a problemática de implementação destes sistemas onde a rede já está em pleno funcionamento e algumas ferramentas de monitoração e controle já tinham sido adquiridas. O foco principal foi nas áreas funcionais de gerenciamento de desempenho e de falhas, muito embora em alguns momentos aborde aspectos de gerenciamento de segurança e contabilização.

A partir do estudo de trabalhos existentes e, considerando o ambiente do TCU, foi proposta uma estratégia para implantação de sistemas de gerenciamento. A questão da seleção das informações que deveriam ser coletadas facilitou a tarefa de monitoração, evitando desperdício de tempo e de banda passante, tornando o sistema ágil e útil.

A implantação do sistema de gerenciamento propiciou o conhecimento de muitas situações que não haviam sido identificadas no dia a dia de operação da rede. A utilização de ferramentas automatizadas para a coleta de informações relativas aos componentes principais da rede facilitou a tomada de decisão quanto aos aspectos de configuração da rede e identificação de causas para problemas relativos ao desempenho da rede. A implantação do sistema de gerenciamento de acordo com a estratégia

proposta neste trabalho mostrou ser eficiente e o resultado pode ser considerado plenamente satisfatório para os objetivos pretendidos inicialmente.

A solução implementada baseou-se ou em ferramentas de gerência que o TCU já possuía ou em ferramentas de domínio público, demonstrando a viabilidade de implementação de gerenciamento e de disponibilização de informações a custo extremamente baixo. Se por um lado o custo é bastante baixo, por outro lado a precariedade da documentação de algumas destas ferramentas e a falta de suporte técnico pode dificultar o processo de implementação.

Uma vez que um dos objetivos do trabalho era o de propor uma solução de gerenciamento de rede para a realidade do TCU, era essencial a identificação das informações de gerenciamento disponibilizada pelos equipamentos. A dificuldade de encontrar documentação sobre informações de gerenciamento disponibilizadas pelos equipamentos e a identificação de quais informações eram realmente mantidas foi o maior obstáculo encontrado. Além disso, em determinado momento foi necessária a atualização do software de todos os módulos do switch M770 para permitir o *port mirror*, que era necessário para a captura do tráfego de determinados servidores. Esta alteração influenciou nas variáveis mantidas, o que implicou em reavaliação da informação disponibilizada por todos os módulos daquele equipamento.

Muito embora o SNMP e RMON já sejam soluções bem definidas e padronizadas, a realidade mostra que a maioria dos equipamentos não implementa suas versões mais recentes (SNMPv3 e RMON2), e que mesmo a implementação do RMON por parte dos equipamentos normalmente ocorre somente para alguns grupos. Por outro

lado, o SMON que é implementado nos switches não possui ampla documentação e pouco se fala dele como padrão de gerenciamento.

A rede de computadores é altamente mutável, ocorrendo acréscimos constantes de novos micros, equipamentos ativos, sistemas e serviços o que implica em mudanças constantes em seu comportamento. Este fato implica na necessidade de revisões periódicas do *baseline* e da verificação de como as mudanças implementadas afetam o funcionamento da rede. Uma boa oportunidade para verificar esta mudança é a iminente implementação da utilização de rede Frame Relay para disponibilização de serviços de *stream* de áudio.

6.2 Trabalhos Futuros

Como trabalho futuro, sugere-se o aprimoramento das ferramentas de coleta de informações e a expansão do monitoramento. Tal aprimoramento pode envolver os seguintes aspectos:

- ✓ Expansão do monitoramento aos demais equipamentos de rede;
- ✓ Implementação de monitoramento sobre servidores e aplicações críticas;
- ✓ Modificações da ferramenta visando melhoria de performance;
- ✓ Implementação de QoS e DiffServ na rede do TCU para permitir a videoconferência e unificação dos serviços de voz e dados na rede WAN;
- ✓ Implementação de um DataWarehouse com as informações coletadas;
- ✓ Utilização de ferramentas que utilizam inteligência artificial para análise dos dados e tomada de decisão.

7. BIBLIOGRAFIA

- ARNETT, Matthew Flint; DULANEY Emmett, et al. **Desvendando o TCP/IP**. Rio de Janeiro: Campus, 1997. 543p.
- BLACK, Darryl P. **Managing Switched Local Area Networks: A Practical Guide**. Massachusetts: Addison Wesley Longman, 1998. 356p.
- BLUMENTHAL, U.; WIJNEN, Bert. **RFC2574 – User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)**. Disponível em: < <http://www.ietf.org/rfc/rfc2574.txt?number=2574>>. Acesso em: 4 de novembro de 2000.
- BRASIL. Tribunal de Contas da União. **Boletim do Tribunal de Contas da União – Edição Especial: O Tribunal de Contas da União e sua Lei Orgânica**. n. 35. Brasília, 12 de junho de 2000. 57p.
- BRASIL. Tribunal de Contas da União. **Plano Estratégico do TCU**. Brasília, 1999. 20p.
- BRASIL. Tribunal de Contas da União. **Projeto da Rede de Comunicação de Dados do Tribunal de Contas da União**. Brasília, 1994. 121p.
- BRASIL. Tribunal de Contas da União. **União – Caderno Especial: Informatização do TCU**. n. 6. Brasília, agosto de 1997. 32p.
- BROWN, Caralyn; BAKER, Fred. **RFC2115 – Management Information Base for Frame Relay DTEs using SMIV2**. Disponível em: <<http://www.ietf.org/rfc/rfc2115.txt?number=2115>>. Acesso em: 17 de abril de 2001.
- CARVALHO, Ernesto; BELCHIOR, Arnaldo Dias; SOUZA, José Newman. **Gerenciamento Pró-ativo Distribuído Baseado em Lógica Difusa**. In: Simpósio Brasileiro de Redes de Computadores, 17, Salvador, 1999. **Anais...** Salvador: SBRC, 1999. p. 649-664.
- CASE, Jeffrey D.; FEDOR, Mark S.; SCHOFFSTALL, Martin L.; DAVIN, James R. **RFC1157 – A Simple Network Management Protocol (SNMP)**. Disponível em: <

<http://www.ietf.org/rfc/rfc1157.txt?number=1157>>. Acesso em: 19 de setembro de 2000.

CASE, Jeffrey D.; MCCLOGHRIE, Keith; ROSE, Marshall.T.; WALDBUSSER, Steven. **RFC1441 – Introduction to version 2 of the Internet-standard Network Management Framework.** Disponível em: < <http://www.ietf.org/rfc/rfc1441.txt?number=1441>>. Acesso em: 21 de outubro de 2000.

CASE, Jeffrey D.; MCCLOGHRIE, Keith; ROSE, Marshall.T.; WALDBUSSER, Steven. **RFC1905 – Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)** . Disponível em: < <http://www.ietf.org/rfc/rfc1905.txt?number=1905>>. Acesso em: 21 de outubro de 2000.

CASE, Jeffrey D.; MCCLOGHRIE, Keith; ROSE, Marshall.T.; WALDBUSSER, Steven. **RFC1907 – Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)** . Disponível em: < <http://www.ietf.org/rfc/rfc1907.txt?number=1907>>. Acesso em: 21 de outubro de 2000.

CASE, Jeffrey D.; MUNDY, Russ; PARTAIN, David; STEWART, Bob. **RFC2570 – Introduction to Version 3 of Internet-standard Network Management Framework** . Disponível em: < <http://www.ietf.org/rfc/rfc2570.txt?number=2570>>. Acesso em: 21 de outubro de 2000.

CLEMENTI, Sérgio; CARVALHO, Tereza Cristina M. B. **Metodologia para Especificação e Implementação de Solução de Gerenciamento.** In: Simpósio Brasileiro de Redes de Computadores, 17, Salvador, 1999. **Anais...** Salvador: SBRC, 1999. p. 633-648.

COMER, Douglas E. **Internetworking with TCP/IP: principles, protocols and architecture.** 3.ed. Upper Saddle River/New Jersey: Prentice Hall, 1995. v1. 613p.

COMER, Douglas E; STEVENS, David L. **Internetworking with TCP/IP: Design, Implementation and Internals.** 2.ed. Upper Saddle River/New Jersey: Prentice Hall, 1994. v2. 612p.

DAVIN, James R.; GALVIN, James M.; MCCLOGHRIE, Keith. **RFC1351 – SNMP Administrative Model.** Disponível em:

<<http://www.ietf.org/rfc/rfc1351.txt?number=1351>>. Acesso em: 20 de setembro de 2000.

DERFLER, Frank J. **Guia de Conectividade**. 3.ed. Rio de Janeiro: Editora Campus, 199x. 564p.

DERFLER, Frank J. **Guia para a Interligação de Redes Locais**. Rio de Janeiro: Editora Campus, 1993. 235p.

DUARTE, Celso Damasceno. **A Constituição Explicada ao Cidadão e ao Estudante**. 5.ed. Belo Horizonte: Editora Lê, 1990. 262p.

FORD, Merilee; LEW, Kim; SPANIER, Steve, et. al. **Internetworking Technologies Handbook**. Indianapolis: Cisco Press, 1997. 717p.

FYRE, Rob; et. al. **RFC2576 – Coexistence Between Version 1, Version 2 and Version 3 of the Internet-standard Network Management Framework**. Disponível em: <<http://www.ietf.org/rfc/rfc2576.txt?number=2576>>. Acesso em: 4 novembro de 2000.

HAUGDAHL, Scott J. **Network Analysis and Troubleshooting**. Massachusetts: Addison Wesley, 2000. 357p.

HARDENY, Sean. **Total SNMP: Exploring the Simple Network Management Protocol**. 2.ed New Jersey: Prentice Hall, 1997. 642p.

IPSWITCH. **WhatsUp Gold – The Network Monitoring Tool for Windows – User’s Guide**. 5. ed. Ipswitch, 2000.

ITU-T. **Recommendation M.3000 – Overview of TMN Recommendations**. Disponível em: <<http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-M.3000-200002-I>>. Acesso em: 6 de agosto de 2001.

ITU-T. **Recommendation M.3010 – Principles for a Telecommunications Management Network**. Disponível em: <<http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-M.3010-200002-I>>. Acesso em: 6 de agosto de 2001.

ITU-T. **Recommendation M.3013 – Considerations for a Telecommunications Management Network**. Disponível em: <<http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-M.3013-200002-I>>. Acesso em: 8 de agosto de 2001.

ITU-T. **Recommendation M.3020 – TMN Interface Specification Methodology.**

Disponível em: <<http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-M.3020-200002-I>>. Acesso em: 8 de agosto de 2001.

JOHNSON, Dale S. **RFC1297 - NOC Internal Integrated Trouble Ticket System:**

Functional Specification Wishlist. Disponível em: <<http://rfc.fh-koeln.de/rfc/html/rfc1297.html>>. Acesso em: 8 de dezembro de 2000.

JOHNSON, Jeffrey T. **RFC1757 – Remote Network Monitoring MIB.** Disponível

em: <<http://rfc.fh-koeln.de/rfc/html/rfc1757.html>>. Acesso em: 15 de setembro de 2000.

LAMBERT, Michael. **RFC1857 – A Model for Common Operational Statistics.**

Disponível em: <<http://rfc.fh-koeln.de/rfc/html/rfc1857.html>>. Acesso em: 6 de dezembro de 2000.

MADRUGA, Ewerton Longoni. **Ferramentas de Apoio à Gerência de Falhas e**

Desempenho em Contexto Distribuído. Porto Alegre, 1994. 135p. Dissertação (Mestrado em Ciência da Computação) Universidade Federal do Rio Grande do Sul.

MAXWELL, Steve. **Red Hat Linux Network Management Tools.** New York:

McGraw-Hill, 2000. 683 p.

MCCLOGHRIE, Keith; ROSE, Marshall.T. **RFC1213 – Management Information**

Base for Network Management of TCP/IP-based internets: MIB II. Disponível em: <<http://www.ietf.org/rfc/rfc1213.txt?number=1213>>. Acesso em: 20 de setembro de 2000.

MCCLOGHRIE, Keith; ROSE, Marshall.T. **RFC1156 – Management Information**

Base for Network Management of TCP/IP-based internets. Disponível em: <<http://www.ietf.org/rfc/rfc1156.txt?number=1156>>. Acesso em: 19 de setembro de 2000.

MCCLOGHRIE, Keith. **RFC1909 – An Administrative Infrastructure for SNMPv2.**

Disponível em: <<http://www.ietf.org/rfc/rfc1909.txt?number=1909>>. Acesso em: 19 de setembro de 2000.

MEIRELLES, Luiz Fernando Tavares. **Uma Proposta para o Gerenciamento de**

Aplicações em Rede. Florianópolis, 1997. 115p. Dissertação (Mestrado em Ciência da Computação) Universidade Federal de Santa Catarina.

- MELCHIORS, Cristina. **Raciocínio Baseado em Casos Aplicado ao Gerenciamento de Falhas em Redes de Computadores**. Porto Alegre, 1999. 151p. Dissertação (Mestrado em Ciência da Computação) Universidade Federal do Rio Grande do Sul.
- MILLER, Mark A. **Managing Internetworks with SNMP**. 2.ed. New York: M&T Books, 1997. 709 p.
- MURRAY, James D. **Windows NT SNMP**. Sebastopol: O'Reilly & Associates, 1998. 446p.
- NASSAR, Daniel J. **Network Performance Baselining**. Indianapolis: Macmillan Technical Publishing, 2000. 715p.
- NASSIF, Lílían Noronha. **Planejamento de Capacidade para a WAN da Rede Municipal de Informática**. Belo Horizonte, 1997. 122p. Dissertação (Mestrado em Administração Pública – Área de concentração: tecnologias da informação) Universidade Federal de Minas Gerais.
- NETWORK ASSOCIATES. **Creating High-Performance Networks and Cutting Downtime With Proactive Management Tools**.
- NETWORK ASSOCIATES. **How to Manage Switched LANs and ATM Switches for Maximum Performance**
- NETWORK ASSOCIATES. **Demonstrating How Your Network Meets Business Objectives and User Expectations**
- OPPENHEIMER, Priscilla. **Projeto de Redes Top-Down: Um enfoque de análise de sistemas para o projeto de redes empresariais**. Rio de Janeiro: Editora Campus, 1999. 492p.
- PARNELL, Terè. **Guide to Wide Área Networks**. Berkeley: McGraw-Hill, 1997. 528p.
- PARNELL, Terè; NULL, Christopher. **Network Administrator's Reference**. Berkeley: McGraw-Hill, 1999. 740p.
- REITER, Cláudio César. **Uma Proposta de Gerenciamento para a Rede Catarinense de Ciência e Tecnologia**. Florianópolis, 1997. 136p. Dissertação (Mestrado em Ciência da Computação) Universidade Federal de Santa Catarina.
- RHODES, Peter D. **Building a Network: how to specify, design, procure and install a corporate LAN**. New York: McGraw-Hill, 1996. 222p.

- ROCHA, Marco Antônio da. **Uma Estratégia para Implementar a Gerência Prática em Redes com a Utilização de Sistemas Baseados em Conhecimento**. Porto Alegre, 1996. 134p. Dissertação (Mestrado em Ciência da Computação) Universidade Federal do Rio Grande do Sul.
- ROSE, Marshall.T.; MCCLOGHRIE, Keith. **RFC1155 – Structure and identification of management information for TCP/IP-based internets**. Disponível em: <<http://www.ietf.org/rfc/rfc1155.txt?number=1155>>. Acesso em: 19 de setembro de 2000.
- ROSE, Marshall.T.; MCCLOGHRIE, Keith. **RFC1212 – Concise MIB Definitions**. Disponível em: <<http://www.ietf.org/rfc/rfc1212.txt?number=1212>>. Acesso em: 19 de setembro de 2000.
- SCHWARTZ, Randal; CHRISTIANSEN, Tom. **Learning Perl**. 2.ed. Sebastopol: O'Reilly & Associates, 1997. 269p.
- SILVA, Edna Lúcia; MENEZES, Estera Muszkat. **Metodologia da Pesquisa e Elaboração de Dissertação**. Florianópolis: Laboratório de Ensino à Distância da UFSC, 2000. 118p.
- SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de Computadores: das LANs, MANs e WANs às Redes ATM**. Rio de Janeiro: Campus, 1995. 576p.
- SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, voz e imagem**. 2.ed. São Paulo: Editora Érica, 1999. 496p.
- SPECIALSKI, Elizabeth S. **Apostila de Gerência de Redes de Computadores e Telecomunicações**. CPGCC: Florianópolis, 2000.
- STALLINGS Willian. **SNMP, SNMPv2, SNMPv3 and RMON1 and 2**. 3. ed. Massachusetts: Addison Wesley, 1999. 617p.
- SUBRAMANIAN, Mani. **Network Management: An Introduction to Principles and Practice**. Massachusetts: Addison Wesley, 2000. 644p.
- TANENBAUM, Andrew S. **Redes de Computadores**. 3.ed. Rio de Janeiro: Campus, 1997. 923p.
- TAYLOR, Ed. **The Network Troubleshooting Handbook**. New York: McGraw-Hill, 1999. 907p.

TECHNET, Microsoft. **Chapter 6 – TCP/IP Implementation Details** Disponível em: <http://www.Microsoft.com/technet/winnt/reskit/sur_tcp2.asp>. Acesso em: 11 de maio de 2001.

TECHNET, Microsoft. **Network Traffic Analysis and Optimization (Windows NT 4.0 and Windows 95)**. Disponível em: <<http://www.Microsoft.com/technet/winnt/winntas/tips/net405ef.asp>>. Acesso em: 11 de maio de 2001.

TEIXEIRA JÚNIOR, José Helvécio; SUAVÉ, Jacques Philippe, et al. **Redes de Computadores: Serviços, Administração e Segurança**. São Paulo: Makron Books, 1999. 493p.

THOMAS, Robert M.. **Introduction to Local Area Networks**. 2.ed. San Francisco: Network Press, 1997. 488p.

WALDBUSSER, Steven. **RFC2021 – Remote Network Monitoring Management Information Base Version 2 using SMIV2**. Disponível em: <<http://www.ietf.org/rfc/rfc2021.txt?number=2021>>. Acesso em: 17 de abril de 2001.

WALDBUSSER, Steven. **RFC2819 – Remote Network Monitoring Management Information Base**. Disponível em: <<http://www.ietf.org/rfc/rfc2819.txt?number=2819>>. Acesso em: 17 de abril de 2001.

WATERMAN, Richard; et. al. **RFC2613 – Remote Monitoring MIB Extensions for Switched Networks**. Disponível em: <<http://www.ietf.org/rfc/rfc2613.txt?number=2613>>. Acesso em: 17 de abril de 2001.

WATERS, Glenn W. **RFC1910 – User-based Security Model for SNMPv2**. Disponível em: <<http://www.ietf.org/rfc/rfc1910.txt?number=1910>>. Acesso em: 17 de abril de 2001.

WIJNEN, Bert; PRESUHN, Randy; MCCLOGHRIE, Keith.. **RFC2575 – View-based Access Control Model (VCAM) for the Simple Network Management Protocol (SNMP)**. Disponível em: <<http://www.ietf.org/rfc/rfc2575.txt?number=2575>>. Acesso em: 4 de novembro de 2000.

8. ANEXO I – Variáveis Passíveis de Monitoração

Variável OID (1.3.6.1.)	MIB	Significado
IfSpeed 2.1.2.2.1.5	MIB II RFC 1158	Velocidade da interface
IfAdminStatus 2.1.2.2.1.7	MIB II RFC 1158	Estado desejado da interface: up(1), down(2), testing(3)
IfOperStatus 2.1.2.2.1.8	MIB II RFC 1158	Estado operacional corrente da interface: up(1), down(2), testing(3)
IfInOctets 2.1.2.2.1.10	MIB II RFC 1158	Número total de octetos recebidos na interface
IfInUcastPkts 2.1.2.2.1.11	MIB II RFC 1158	Número de pacotes unicast recebidos pela interface
IfInNUcastPkts 2.1.2.2.1.12	MIB II RFC 1158	Número de pacotes não unicast (multicast e broadcast) recebidos pela interface
IfInDiscards 2.1.2.2.1.13	MIB II RFC 1158	Número de pacotes entrantes na interface que não continham erros mas que foram descartados
IfInErrors 2.1.2.2.1.14	MIB II RFC 1158	Número de pacotes entrantes na interface em que foram detectados erros
IfOutOctets 2.1.2.2.1.16	MIB II RFC 1158	Número total de octetos enviados pela interface
IfOutUcastPkts 2.1.2.2.1.17	MIB II RFC 1158	Número de pacotes unicast enviados pela interface
IfOutNUcastPkts 2.1.2.2.1.18	MIB II RFC 1158	Número de pacotes não unicast (multicast e broadcast) enviados pela interface
IfOutDiscards 2.1.2.2.1.19	MIB II RFC 1158	Número de pacotes que saíram pela interface mas que foram descartados
IfOutErrors 2.1.2.2.1.20	MIB II RFC 1158	Número de pacotes que deixaram de ser enviados pela interface devido à existência de erros
IfOutQlen 2.1.2.2.1.21	MIB II RFC 1158	Tamanho da fila de saída em número de pacotes
IcmpInDestUnreachs 2.1.5.3	MIB II RFC 1158	Número de mensagens icmp recebidas informando que o destino não estava alcançável
IcmpInSrcQuenchs 2.1.5.3	MIB II RFC 1158	Número de mensagens icmp recebidas solicitando que seja reduzida a qtde de informação transmitida
IcmpOutDestUnreachs 2.1.5.3	MIB II RFC 1158	Número de mensagens icmp enviadas informando que o destino não estava alcançável
IcmpOutSrcQuenchs 2.1.5.3	MIB II RFC 1158	Número de mensagens icmp enviadas solicitando que seja reduzida a qtde de informação transmitida
TcpAttempFails 2.1.6.7	MIB II RFC 1158	Número de tentativas de estabelecimento de conexão tcp que não tiveram êxito
TcpEstabResets 2.1.6.8	MIB II RFC 1158	Número de conexões tcp estabelecidas que foram reinicializadas

TcpInSegs 2.1.6.10	MIB II RFC 1158	Número de segmentos tcp recebidos, inclusive aqueles com erros
TcpOutSegs 2.1.6.11	MIB II RFC 1158	Número de segmentos tcp enviados, excluindo as retransmissões de segmentos
TcpRetransSegs 2.1.6.7	MIB II RFC 1158	Número total de segmentos tcp retransmitidos
SnmpInBadCommunityNames 2.1.11.4	MIB II RFC 1158	Número de mensagens snmp recebidas com nome de comunidade inválido
SnmpInBadCommunityUses 2.1.11.5	MIB II RFC 1158	Número de mensagens snmp recebidas cuja operação requerida não era permitida para a comunidade
Dot3StatsFCSErros 2.1.10.7.2.1.3	Ether-Like RFC 1643	Número de quadros recebidos na interface com erro de FCS
Dot3StatsSingleCollisionFrames 2.1.10.7.2.1.4	Ether-Like RFC 1643	Número de frames transmitidos com sucesso e que experimentaram uma colisão
Dot3StatsMultipleCollisionFrames 2.1.10.7.2.1.5	Ether-Like RFC 1643	Número de frames transmitidos com sucesso e que experimentaram mais que uma colisão
Dot3StatsDeferredTransmissions 2.1.10.7.2.1.6	Ether-Like RFC 1643	Número de frames que sofreram atraso na transmissão pois o meio estava ocupado
Dot3StatsExcessiveCollisions 2.1.10.7.2.1.9	Ether-Like RFC 1643	Número de frames que deixaram de ser transmitidos em função de excessivo número de colisões
FrCircuitState 2.1.10.32.2.1.3	FR DTEs RFC 1315	Estado do circuito virtual referente ao DLCI: Inválido(1), ativo(2), inativo(3)
FrCircuitRecievedFECNs 2.1.10.32.2.1.4	FR DTEs RFC 1315	Número de quadros recebidos que tinham flag de FECN marcado
FrCircuitRecievedBECNs 2.1.10.32.2.1.5	FR DTEs RFC 1315	Número de quadros recebidos que tinham flag de BECN marcado
FrCircuitSentFrames 2.1.10.32.2.1.6	FR DTEs RFC 1315	Número de frames enviados no circuito virtual desde sua criação
FrCircuitSentOctets 2.1.10.32.2.1.7	FR DTEs RFC 1315	Número de bytes enviados no circuito virtual desde sua criação
FrCircuitReceivedFrames 2.1.10.32.2.1.8	FR DTEs RFC 1315	Número de frames recebidos no circuito virtual desde sua criação
FrCircuitReceivedOctets 2.1.10.32.2.1.9	FR DTEs RFC 1315	Número de bytes recebidos no circuito virtual desde sua criação
FrCircuitCreationTime 2.1.10.32.2.1.10	FR DTEs RFC 1315	Valor do sysuptime quando o circuito virtual foi criado
FrCircuitLastTimeChange 2.1.10.32.2.1.11	FR DTEs RFC 1315	Valor do sysuptime na última vez que houve alteração do valor do estado do circuito
LocIfLineProt 4.1.9.2.2.1.1.2	Cisco Interfaces	Estado do protocolo na interface: Up(1), down(0)
LocIfInBitsSec 4.1.9.2.2.1.1.6	Cisco Interfaces	Média de bits por segundo que entraram na interface nos últimos cinco minutos
LocIfInPktsSec 4.1.9.2.2.1.1.7	Cisco Interfaces	Média de pacotes por segundo que entraram na interface nos últimos cinco minutos
LocIfOutBitsSec 4.1.9.2.2.1.1.8	Cisco Interfaces	Média de bits por segundo que saíram da interface nos últimos cinco minutos
LocIfOutPktsSec 4.1.9.2.2.1.1.9	Cisco Interfaces	Média de pacotes por segundo que saíram da interface nos últimos cinco minutos

LocIfInCrc 4.1.9.2.2.1.1.12	Cisco Interfaces	Número de pacotes que entraram na interface e que apresentaram erro de CRC
LocIfInOverrun 4.1.9.2.2.1.1.14	Cisco Interfaces	Número de pacotes que chegaram mais rápido do que a capacidade de processamento do hardware
LocIfInIgnored 4.1.9.2.2.1.1.15	Cisco Interfaces	Número de pacotes recebidos e ignorados por insuficiência de buffers internos
LocIfResets 4.1.9.2.2.1.1.17	Cisco Interfaces	Número de vezes que a interface foi reinicializada internamente
LocIfLoad 4.1.9.2.2.1.1.24	Cisco Interfaces	Fator de carga da interface
LocIfCollisions 4.1.9.2.2.1.1.25	Cisco Interfaces	Número de colisões ocorridas na interface
LocIfInputQueueDrops 4.1.9.2.2.1.1.26	Cisco Interfaces	Número de pacotes entrantes descartados porque a fila de entrada estava cheia
LocIfOutputQueueDrops 4.1.9.2.2.1.1.27	Cisco Interfaces	Número de pacotes saíntes descartados porque a fila de saída estava cheia
LocIfSlowInPkts 4.1.9.2.2.1.1.30	Cisco Interfaces	Número de pacotes entrantes na interface roteados com slow switching
LocIfSlowOutPkts 4.1.9.2.2.1.1.31	Cisco Interfaces	Número de pacotes saíntes da interface roteados com slow switching
LocIfFastInPkts 4.1.9.2.2.1.1.34	Cisco Interfaces	Número de pacotes entrantes na interface roteados com <i>fast</i> switching
LocIfFastOutPkts 4.1.9.2.2.1.1.35	Cisco Interfaces	Número de pacotes saíntes da interface roteados com <i>fast</i> switching
ProcessorRam 4.1.9.3.6.6	Cisco Chassis	Número de bytes de memória RAM disponíveis para a CPU
nvRAMSize 4.1.9.3.6.7	Cisco Chassis	Tamanho em bytes da memória NV-RAM
NvRAMUsed 4.1.9.3.6.8	Cisco Chassis	Espaço utilizado da memória NV-RAM
CiscoMemoryPoolType 4.1.9.9.48.1.1.1.1	Cisco MemoryPool	Tipo de pool de memória analisado, utilizado como índice
CiscoMemoryPoolName 4.1.9.9.48.1.1.1.2	Cisco MemoryPool	Nome do pool referente àquele índice
CiscoMemoryPoolUsed 4.1.9.9.48.1.1.1.5	Cisco MemoryPool	Quantidade de bytes utilizado no pool de memória
CiscoMemoryPoolFree 4.1.9.9.48.1.1.1.6	Cisco MemoryPool	Quantidade de bytes livres no pool de memória
CfrCircuitDEins 4.1.9.9.49.1.2.1.1.1	Cisco Frame-Relay	Número de pacotes recebidos com flag DE ativado
CfrCircuitDEouts 4.1.9.9.49.1.2.1.1.2	Cisco Frame-Relay	Número de pacotes enviados com flag DE ativado
CfrCircuitDropPktsOuts 4.1.9.9.49.1.2.1.1.3	Cisco Frame-Relay	Número de pacotes descartados
CpmCPUTotal5sec 4.1.9.9.109.1.1.1.1.3	Cisco Process	Percentual de utilização da CPU nos últimos 5 segundos
CpmCPUTotal1min 4.1.9.9.109.1.1.1.1.4	Cisco Process	Percentual de utilização da CPU no último minuto
CpmCPUTotal5min	Cisco	Percentual de utilização da CPU nos últimos 5

4.1.9.9.109.1.1.1.5	Process	minutos
EthPortTraffic 4.1.81.12.3.1.1.14	Lannet Moduls	Número de bits recebidos na porta em frames sem erros
EthPortFramesReceivedOK 4.1.81.12.3.1.1.15	Lannet Moduls	Número de quadros recebidos sem erro na porta
EthPortPacketErrors 4.1.81.12.3.1.1.17	Lannet Moduls	Número de quadros recebidos na porta em que foi detectada a presença de erro
EthPortCollisions 4.1.81.12.3.1.1.19	Lannet Moduls	Número de colisões que detectadas na porta
EthPortOperStatus 4.1.81.12.3.1.1.35	Lannet Moduls	Indica o estado operacional da interface: Operac(1), não operac(2), não suportado(255)
EthPortBroadcastPkts 4.1.81.12.3.1.1.36	Lannet Moduls	Número de pacotes de broadcast recebidos na porta
EthPortMulticastPkts 4.1.81.12.3.1.1.37	Lannet Moduls	Número de pacotes recebidos na porta com endereço de multicast
EthBusTotalCollisions 4.1.81.12.5.1.1.6	Lannet Moduls	Número total de colisões detectadas no barramento
EthBusTotalPackets 4.1.81.12.5.1.1.7	Lannet Moduls	Número total de pacotes detectados no barramento
EthBusTotalErrors 4.1.81.12.5.1.1.8	Lannet Moduls	Número de pacotes com erro detectado no barramento
EthBusUtilization 4.1.81.12.5.1.1.10	Lannet Moduls	Utilização percentual do barramento na última amostragem
EthBusPeakUtilization 4.1.81.12.5.1.1.11	Lannet Moduls	Valor máximo do tráfego desde a última inicialização do equipamento
EthBusThresholdStatus 4.1.81.12.5.1.1.12	Lannet Moduls	Valor de limiar de utilização do barramento, acima do qual é gerado um trap
LsBusStatsDropEvents 4.1.81.19.3.2.1	Lannet Applic	Número total de pacotes descartados devido à falta de recursos
LsBusStatsPkts 4.1.81.19.3.2.2	Lannet Applic	Número total de pacotes recebidos no barramento do switch
LsBusStatsOctets 4.1.81.19.3.2.3	Lannet Applic	Número total de octetos recebidos no barramento do switch
LsBusStatsUtilization 4.1.81.19.3.2.4	Lannet Applic	Utilização do barramento do switch expressa em percentual
LsBusStatsEthBroadcastPkts 4.1.81.19.3.2.5	Lannet Applic	Número total de pacotes recebidos no barramento com endereço de broadcast
LsBusStatsMulticastPkts 4.1.81.19.3.2.6	Lannet Applic	Número total de pacotes recebidos no barramento do switch com endereço multicast
LsBusStatsGoodEthPkts 4.1.81.19.3.2.7	Lannet Applic	Número de pacotes recebidos no barramento sem erros
LsBusStatsGoodEthOctets 4.1.81.19.3.2.8	Lannet Applic	Número de bytes sem erro recebidos no barramento do switch
LsBusStatsBadEthPkts 4.1.81.19.3.2.9	Lannet Applic	Número de pacotes com erro recebidos no barramento do switch
LsPortNumber 4.1.81.19.3.3.4.1.1	Lannet Applic	Número da porta, calculado a partir do número da porta e do slot
LsPortInPkts 4.1.81.19.3.3.4.1.2	Lannet Applic	Número de pacotes sem erros recebidos na porta
LsPortInOctets	Lannet	Número de bytes sem erros transmitidos por esta

4.1.81.19.3.3.4.1.5	Applic	porta para o barramento do switch
LsPortInTotalErrors 4.1.81.19.3.3.4.1.6	Lannet Applic	Número de pacotes com erros recebidos na porta
LsPortInCollisions 4.1.81.19.3.3.4.1.7	Lannet Applic	Número de colisões detectadas na porta
ScGenMonDropEvents 4.1.81.28.1.2.1.1.2	Lannet Applic	Número de descartes que ocorreram devido à falta de recursos do switch
ScGenMonGoodBroadcastPkts 4.1.81.28.1.2.1.1.5	Lannet Applic	Número de pacotes de broadcast recebidos no domínio do switch
scGenMonGoodMulticastPkts 4.1.81.28.1.2.1.1.6	Lannet Xswtch	Número de pacotes de multicast recebidos no domínio do switch
ScGenMonGoodPkts 4.1.81.28.1.2.1.1.7	Lannet Xswtch	Número de pacotes sem erro recebidos no domínio do switch
ScGenMonBadPkts 4.1.81.28.1.2.1.1.8	Lannet Xswtch	Número de pacotes com erro recebidos no domínio do switch
ScGenMonGoodOctets 4.1.81.28.1.2.1.1.9	Lannet Xswtch	Número de octetos bons que trafegaram no domínio do switch
ScGenMonBadOctets 4.1.81.28.1.2.1.1.10	Lannet Xswtch	Número de octetos com erro que trafegaram no domínio do switch
ScEthPortGoodBroadcastPktsRec 4.1.81.28.2.1.1.1.5	Lannet Xswtch	Quantidade de pacotes de broadcast recebidos na porta
ScEthPortGoodMulticastPktsRec 4.1.81.28.2.1.1.1.6	Lannet Xswtch	Quantidade de pacotes de multicast recebidos na porta
ScEthPortCollisions 4.1.81.28.2.1.1.1.11	Lannet Xswtch	Quantidade de colisões que ocorreram na porta
ScEthPortPkts64Octets 4.1.81.28.2.1.1.1.12	Lannet Xswtch	Quantidade de pacotes de 64 bytes recebidos na porta
ScEthPortPkts65to127Octets 4.1.81.28.2.1.1.1.13	Lannet Xswtch	Quantidade de pacotes entre 65 e 127 bytes recebidos na porta
ScEthPortPkts128to255Octets 4.1.81.28.2.1.1.1.14	Lannet Xswtch	Quantidade de pacotes entre 128 e 255 bytes recebidos na porta
ScEthPortPkts256to511Octets 4.1.81.28.2.1.1.1.15	Lannet Xswtch	Quantidade de pacotes entre 256 e 511 bytes recebidos na porta
ScEthPortPkts512to1023Octets 4.1.81.28.2.1.1.1.16	Lannet Xswtch	Quantidade de pacotes entre 512 e 1023 bytes recebidos na porta
ScEthPortPkts1024to1518Octets 4.1.81.28.2.1.1.1.17	Lannet Xswtch	Quantidade de pacotes entre 1024 e 1518 bytes recebidos na porta
ScEthPortGoodPktsRec 4.1.81.28.2.1.1.1.18	Lannet Xswtch	Quantidade de pacotes sem erros recebidos na porta
ScEthPortBadPkts 4.1.81.28.2.1.1.1.19	Lannet Xswtch	Quantidade de pacotes com erro recebidos na porta
ScEthPortGoodOctetsRec 4.1.81.28.2.1.1.1.20	Lannet Xswtch	Quantidade total de bytes sem erros recebidos na porta
ScEthPortGoodOctetsSent 4.1.81.28.2.1.1.1.24	Lannet Xswtch	Quantidade de bytes sem erros enviados para a porta
ScEthPortGoodPktsSent 4.1.81.28.2.1.1.1.25	Lannet Xswtch	Quantidade de pacotes sem erro enviados para a porta

9. ANEXO II – Tamanho de Pacotes por Aplicação

Além do levantamento de tamanho médio de pacotes efetuado no item 5.7.3.4, é importante a análise da distribuição de tamanhos de pacote por aplicação. Como no caso do TCU aplicações diferentes são disponibilizadas por diferentes servidores foi feito o levantamento da distribuição de tamanhos de pacote para os principais servidores de rede, o que indica o comportamento das diferentes aplicações.

Figura 9.1 – Distribuição de tamanho de pacotes – Servidor de Arquivos

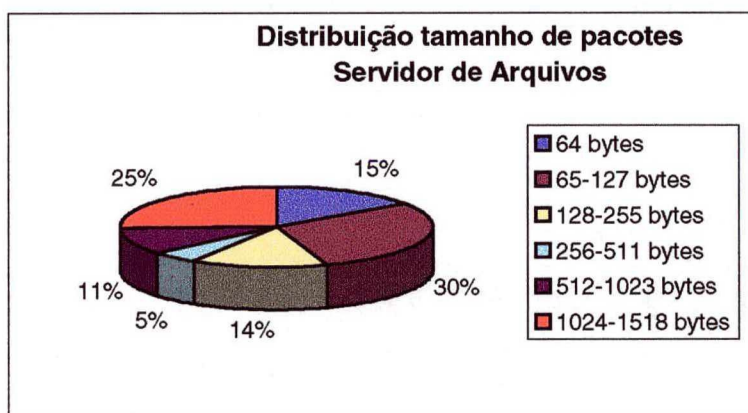


Figura 9.2 – Distribuição de tamanho de pacotes – Servidor de Impressão

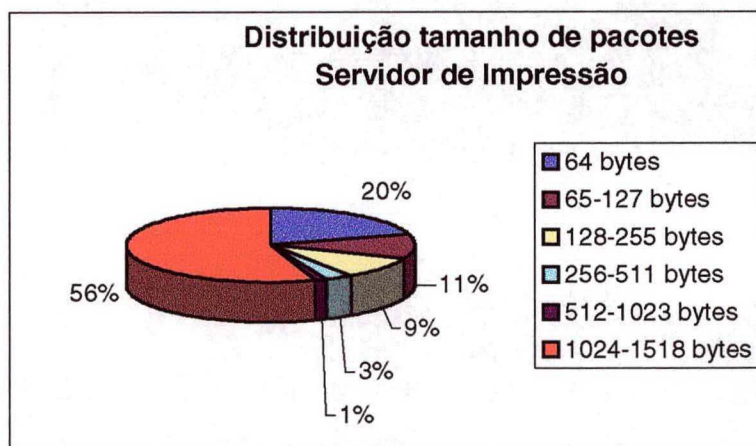


Figura 9.3 – Distribuição de tamanho de pacotes – Banco de dados textual

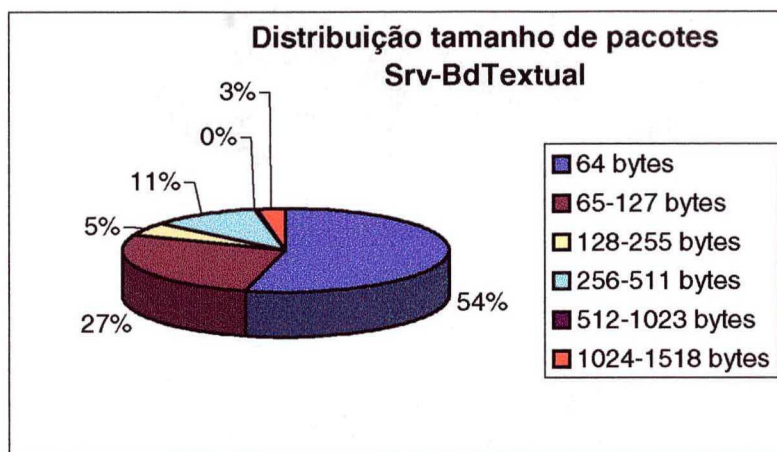


Figura 9.4 – Distribuição de tamanho de pacotes – Servidor de Banco de Dados Relacional

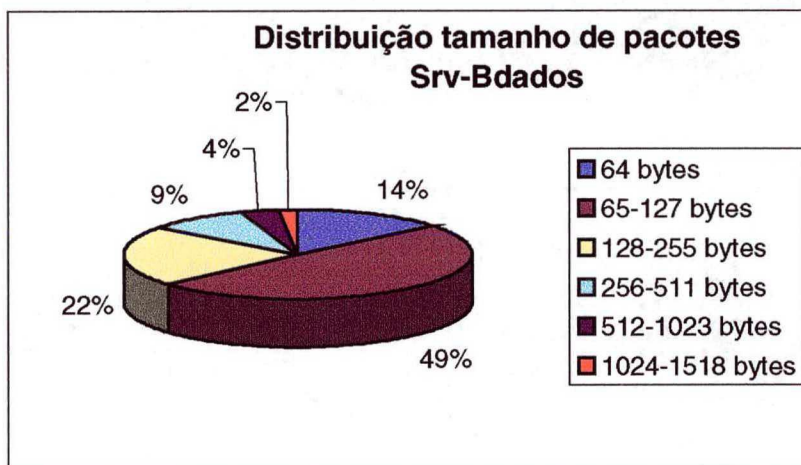


Figura 9.5 – Distribuição de tamanho de pacotes – Servidor de Comunicação

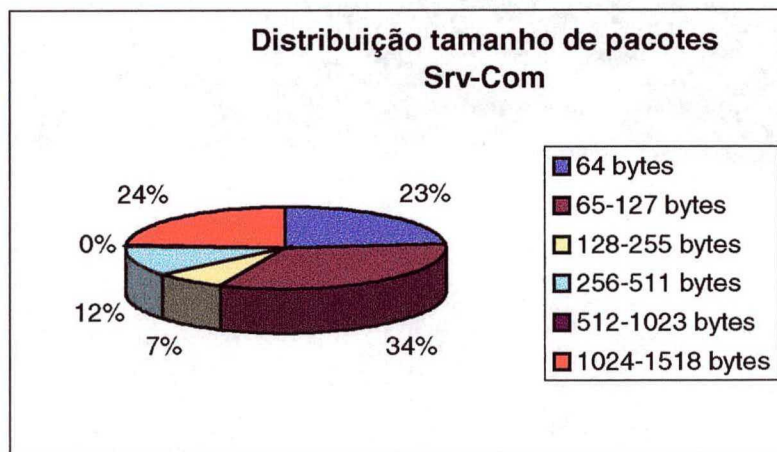


Figura 9.6 – Distribuição de tamanho de pacotes – Web Server Internet

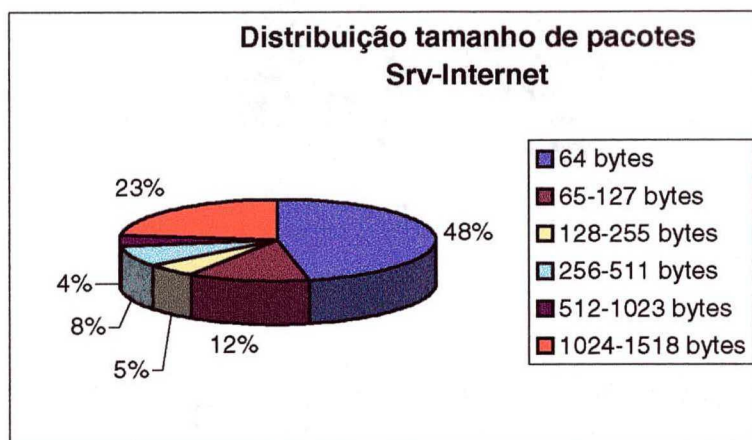


Figura 9.7 – Distribuição de tamanho de pacotes – Web Server Intranet

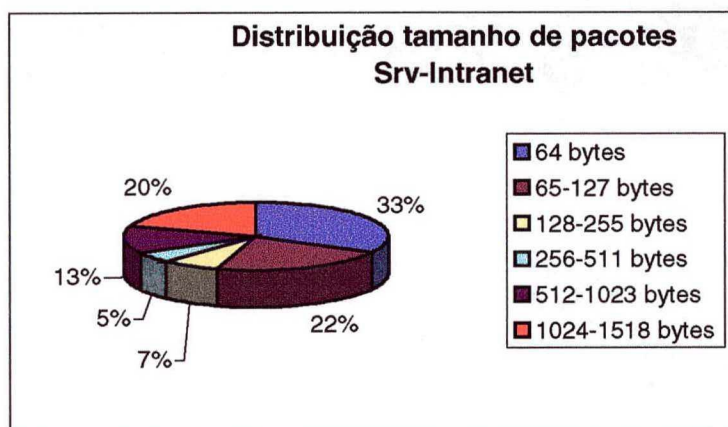


Figura 9.8 – Distribuição de tamanho de pacotes – Web Server Sisac

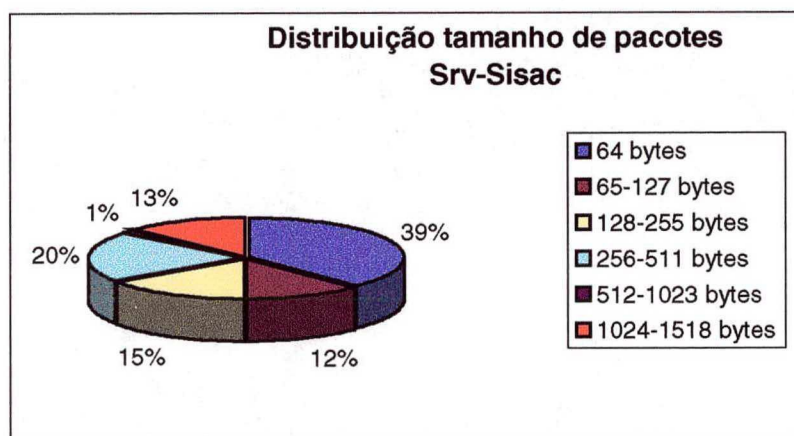


Figura 9.9 – Distribuição de tamanho de pacotes – Servidor de Correio 1

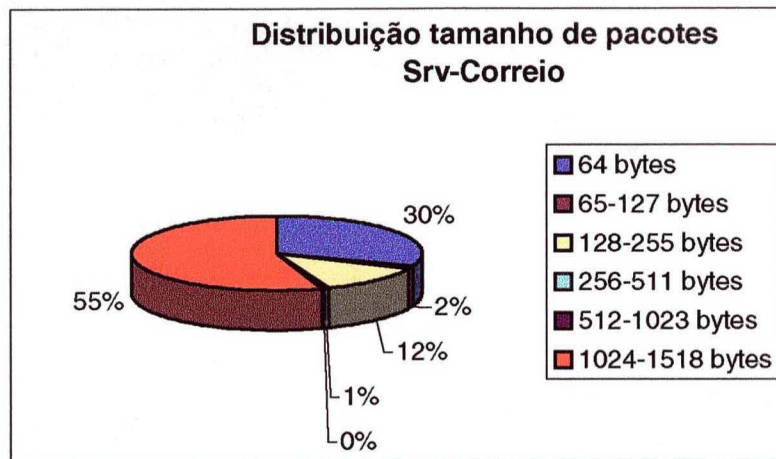
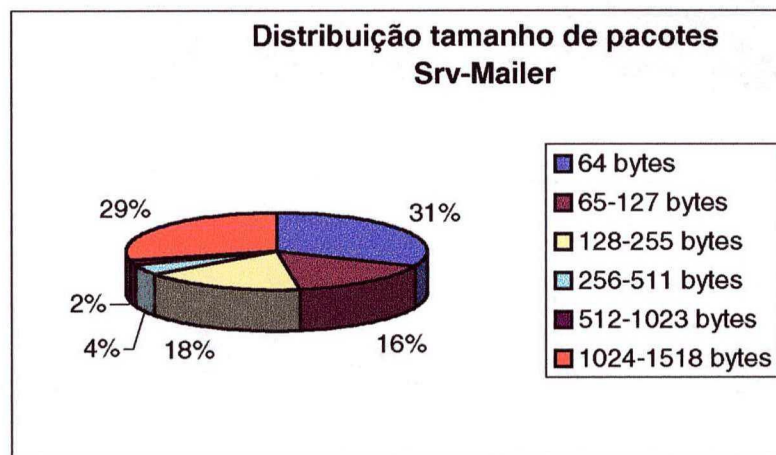


Figura 9.9 – Distribuição de tamanho de pacotes – Servidor de Correio 2



10. ANEXO III – Arquivos de Configuração do MRTG

A fim de gerar gráficos pela ferramenta MRTG é necessário primeiramente montar os arquivos de configuração que especificam quais interfaces ou OIDs devem ser monitoradas. Cada monitoração é definida em um Target, onde são passadas duas variáveis. É possível também fazer a chamada de um programa externo que devolva o valor das variáveis a serem plotadas nos gráficos. O arquivo de configuração deve ser chamado em intervalos de tempos regulares. No caso do TCU foram instaladas versões para Linux e Windows NT, no primeiro caso a periodicidade de execução é definida no arquivo Crontab, no NT é instalado um serviço e configurada a periodicidade de execução, pode-se utilizar também o comando AT. É apresentado a seguir o arquivo de configuração utilizado para levantar informações do roteador que interliga o ISC à Sede do TCU.

10.1. Arquivo .cfg - Roteador que interliga rede da Sede à Rede do ISC

```
# Add a WorkDir: /some/path line to this file

WorkDir:      d:\mrtg\graficos\router-251
Language:     brazilian
Options[_]:   bits,unknaszero,growright
WithPeak[_]: ymw
YLegend[_]:   Bits/s

# opcoes default      - Geraldo
# Options bits        - faz medicao em bits em lugar de bytes
# Options unknaszero - plota zero quando nao obtem resposta
# Options growright   - plota gráfico da esquerda para a direita
# WithPeak            - utiliza o pico nos graficos anuais, mensais e
semanais

#####
```



```
# Description: Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-IS56I-M), Version 12.0(5)T1, RELEASE SOFTWARE
(fc1) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Tue 17-
Aug-99 14:47 by cmong
# Contact:
# System Name: router_251
# Location:
#.....
```

```
Target[roteador-251-eth0]: 1:scx_TCU@10.1.255.251
MaxBytes[roteador-251-eth0]: 1250000
Title[roteador-251-eth0]: router_251 (roteador-251.tcu.gov.br):
Ethernet0
PageTop[roteador-251-eth0]: <H1>Ethernet0
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Maintainer:</TD><TD></TD></TR>
  <TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>
  <TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>
  <TR><TD>Max Speed:</TD>
  <TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>
```

```
#-----
Target[roteador-251-ISC]: 2:scx_TCU@10.1.255.251
MaxBytes[roteador-251-ISC]: 250000
Title[roteador-251-ISC]: router_251 (): Serial0
PageTop[roteador-251-ISC]: <H1>ISC Serial0
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Maintainer:</TD><TD></TD></TR>
  <TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>
  <TR><TD>IP:</TD><TD> (</TD></TR>
  <TR><TD>Max Speed:</TD>
  <TD>2Mbps - ppp</TD></TR>
</TABLE>
```

```
#-----
Target[roteador-251-cpu]:
1.3.6.1.4.1.9.2.1.58.0&1.3.6.1.4.1.9.2.1.58.0:scx_TCU@10.1.255.251
MaxBytes[roteador-251-cpu]: 100
Options[roteador-251-cpu]: gauge,unknaszero,growright
Unscaled[roteador-251-cpu]: ymwd
YLegend[roteador-251-cpu]: CPU (%)
Title[roteador-251-cpu]: router_251 (): CPU (%)
PageTop[roteador-251-cpu]: <H1>CPU (%)
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
</TABLE>
```

```
#-----
```

```

Target [roteador-251-mem] :
1.3.6.1.4.1.9.9.48.1.1.1.5.1&1.3.6.1.4.1.9.9.48.1.1.1.5.1:scx_TCU@10.1
.255.251
MaxBytes [roteador-251-mem] : 7522564
Options [roteador-251-mem] : gauge,unknaszero,growright
Unscaled [roteador-251-mem] : ymwd
YLegend [roteador-251-mem] : Memoria
Title [roteador-251-mem] : router_251 () : Memória utilizada
PageTop [roteador-251-mem] : <H1>Memória
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
</TABLE>

```

```
#-----
```

```

Target [roteador-251-io] :
1.3.6.1.4.1.9.9.48.1.1.1.5.2&1.3.6.1.4.1.9.9.48.1.1.1.5.2:scx_TCU@10.1
.255.251
MaxBytes [roteador-251-io] : 6291456
Options [roteador-251-io] : gauge,unknaszero,growright
Unscaled [roteador-251-io] : ymwd
YLegend [roteador-251-io] : Memoria IO
Title [roteador-251-io] : router_251 () : Memória IO utilizada
PageTop [roteador-251-io] : <H1>Memória IO
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
</TABLE>

```

```
#-----
```

```
# Utilização das interfaces locIfInBitsSec x locIfOutBitsSec
#-----
```

```

Target [roteador-251-eth0-bitsec] :
1.3.6.1.4.1.9.2.2.1.1.6.1&1.3.6.1.4.1.9.2.2.1.1.8.1:scx_TCU@10.1.255.2
51
MaxBytes [roteador-251-eth0-bitsec] : 10000000
Options [roteador-251-eth0-bitsec] : gauge,unknaszero,growright
Title [roteador-251-eth0-bitsec] : router_251 (roteador-251.tcu.gov.br) :
Ethernet0
PageTop [roteador-251-eth0-bitsec] : <H1>Rede Local Sede - Ethernet0 -
Utilização
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>
  <TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>
  <TR><TD>Max Speed:</TD>
  <TD>10 Mbps (ethernetCsmacd)</TD></TR>
</TABLE>

```

```
#-----
```

```

Target [roteador-251-ser0-bitsec] :
1.3.6.1.4.1.9.2.2.1.1.6.2&1.3.6.1.4.1.9.2.2.1.1.8.2:scx_TCU@10.1.255.2
51
MaxBytes [roteador-251-ser0-bitsec] : 2000000

```

```

Options[roteador-251-ser0-bitsec]: gauge,unknaszero,growright
Title[roteador-251-ser0-bitsec]: router_251 (): Serial0
PageTop[roteador-251-ser0-bitsec]: <H1>ISC Serial0 - Utilização
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>
  <TR><TD>IP:</TD><TD>() </TD></TR>
  <TR><TD>Max Speed:</TD>
    <TD>2 Mbps (PPP)</TD></TR>
</TABLE>

#-----
# Pacotes por segundo nas interfaces locIfInPktsSec x locIfOutPktsSec
#-----

Target[roteador-251-eth0-pktsec]:
1.3.6.1.4.1.9.2.2.1.1.7.1&1.3.6.1.4.1.9.2.2.1.1.9.1:scx_TCU@10.1.255.2
51
MaxBytes[roteador-251-eth0-pktsec]: 10000000
Options[roteador-251-eth0-pktsec]: gauge,unknaszero,growright
YLegend[roteador-251-eth0-pktsec]: Pacotes/seg
Title[roteador-251-eth0-pktsec]: router_251 (roteador-251.tcu.gov.br):
Ethernet0
PageTop[roteador-251-eth0-pktsec]: <H1>Rede Local Sede - Ethernet0 -
Pacotes/seg
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>
  <TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>
</TABLE>

#-----

Target[roteador-251-ser0-pktsec]:
1.3.6.1.4.1.9.2.2.1.1.7.2&1.3.6.1.4.1.9.2.2.1.1.9.2:scx_TCU@10.1.255.2
51
MaxBytes[roteador-251-ser0-pktsec]: 20000000
YLegend[roteador-251-ser0-pktsec]: Pacotes/seg
Options[roteador-251-ser0-pktsec]: gauge,unknaszero,growright
Title[roteador-251-ser0-pktsec]: router_251 (): Serial0
PageTop[roteador-251-ser0-pktsec]: <H1>ISC Serial0 - Pacotes/seg
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>
  <TR><TD>IP:</TD><TD>() </TD></TR>
</TABLE>

#-----
# Erros in e out nas interfaces - ifInErrors x ifOutErrors
#-----

Target[roteador-251-eth0-erros]:
ifInErrors.1&ifOutErrors.1:scx_TCU@10.1.255.251
MaxBytes[roteador-251-eth0-erros]: 1000000
YLegend[roteador-251-eth0-erros]: Num. Erros

```

Title[roteador-251-eth0-erros]: router_251 (roteador-251.tcu.gov.br):
Ethernet0

PageTop[roteador-251-eth0-erros]: <H1>Rede Local Sede - Ethernet0 -
Número de Erros

</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>

<TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>

</TABLE>

#-----

Target [roteador-251-ser0-erros]:

ifInErrors.2&ifOutErrors.2:scx_TCU@10.1.255.251

MaxBytes[roteador-251-ser0-erros]: 1000000

YLegend[roteador-251-ser0-erros]: Num. Erros

Title[roteador-251-ser0-erros]: router_251 (): Serial0

PageTop[roteador-251-ser0-erros]: <H1>ISC Serial0 - Número de Erros
</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>

<TR><TD>IP:</TD><TD>()</TD></TR>

</TABLE>

#-----

Quantidade de pacotes Unicast x não unicast - ifInUcastPkts x

ifInNUcastPkts

#-----

Target [roteador-251-eth0-nucast]:

ifInUcastPkts.1&ifInNUcastPkts.1:scx_TCU@10.1.255.251

MaxBytes[roteador-251-eth0-nucast]: 1000000

YLegend[roteador-251-eth0-nucast]: UcastPkts x NUcastPkts

Title[roteador-251-eth0-nucast]: router_251 (roteador-251.tcu.gov.br):
Ethernet0

PageTop[roteador-251-eth0-nucast]: <H1>Rede Local Sede - Ethernet0 -
Pacotes Ucast x NUcast

</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>

<TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>

</TABLE>

#-----

Target [roteador-251-ser0-nucast]:

ifInUcastPkts.2&ifInNUcastPkts.2:scx_TCU@10.1.255.251

MaxBytes[roteador-251-ser0-nucast]: 1000000

YLegend[roteador-251-ser0-nucast]: Num. Erros

Title[roteador-251-ser0-nucast]: router_251 (): Serial0

PageTop[roteador-251-ser0-nucast]: <H1>ISC Serial0 - Pacotes Ucast x
NUcast

```

</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>
  <TR><TD>IP:</TD><TD>()</TD></TR>
</TABLE>

#-----
# Pacotes descartados nas filas - locIfInputQueueDrops x
locIfOutputQueueDrops
#-----

Target [roteador-251-eth0-qdrop]:
1.3.6.1.4.1.9.2.2.1.1.26.1&1.3.6.1.4.1.9.2.2.1.1.27.1:scx_TCU@10.1.255
.251
MaxBytes [roteador-251-eth0-qdrop]: 10000000
YLegend [roteador-251-eth0-qdrop]: Pacotes descartados
Title [roteador-251-eth0-qdrop]: router_251 (roteador-251.tcu.gov.br):
Ethernet0
PageTop [roteador-251-eth0-qdrop]: <H1>Rede Local Sede - Ethernet0 -
Pacotes descartados
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>
  <TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>
</TABLE>

#-----

Target [roteador-251-ser0-qdrop]:
1.3.6.1.4.1.9.2.2.1.1.26.2&1.3.6.1.4.1.9.2.2.1.1.27.2:scx_TCU@10.1.255
.251
MaxBytes [roteador-251-ser0-qdrop]: 2000000
YLegend [roteador-251-ser0-qdrop]: Pacotes descartados
Title [roteador-251-ser0-qdrop]: router_251 (): Serial0
PageTop [roteador-251-ser0-qdrop]: <H1>ISC Serial0 - Pacotes
descartados
</H1>
<TABLE>
  <TR><TD>System:</TD><TD>router_251 in </TD></TR>
  <TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>
  <TR><TD>IP:</TD><TD>()</TD></TR>
</TABLE>

#-----

# Resets de interface - locIfResets
#-----

Target [roteador-251-eth0-ifrst]:
1.3.6.1.4.1.9.2.2.1.1.17.1&1.3.6.1.4.1.9.2.2.1.1.17.1:scx_TCU@10.1.255
.251
MaxBytes [roteador-251-eth0-ifrst]: 10000000
YLegend [roteador-251-eth0-ifrst]: Int Reset

```

Title[roteador-251-eth0-ifrst]: router_251 (roteador-251.tcu.gov.br):
Ethernet0

PageTop[roteador-251-eth0-ifrst]: <H1>Rede Local Sede - Ethernet0 -
Resets de Interface

</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>

<TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>

</TABLE>

#-----

Target[roteador-251-ser0-ifrst]:

1.3.6.1.4.1.9.2.2.1.1.17.2&1.3.6.1.4.1.9.2.2.1.1.17.2:scx_TCU@10.1.255
.251

MaxBytes[roteador-251-ser0-ifrst]: 2000000

YLegend[roteador-251-ser0-ifrst]: Int Reset

Title[roteador-251-ser0-ifrst]: router_251 (): Serial0

PageTop[roteador-251-ser0-ifrst]: <H1>ISC Serial0 - Resets de
Interface

</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Serial0 (2)</TD></TR>

<TR><TD>IP:</TD><TD>()</TD></TR>

</TABLE>

#-----

Colisões nas interfaces - locIfCollisions x qtde pacotes saintes

#-----

Target[roteador-251-eth0-ifcol]:

1.3.6.1.4.1.9.2.2.1.1.25.1&ifOutUcastPkts.1:scx_TCU@10.1.255.251

MaxBytes[roteador-251-eth0-ifcol]: 10000000

YLegend[roteador-251-eth0-ifcol]: Colisões

Title[roteador-251-eth0-ifcol]: router_251 (roteador-251.tcu.gov.br):
Ethernet0

PageTop[roteador-251-eth0-ifcol]: <H1>Rede Local Sede - Ethernet0 -
Colisões x pacotes

</H1>

<TABLE>

<TR><TD>System:</TD><TD>router_251 in </TD></TR>

<TR><TD>Interface:</TD><TD>Ethernet0 (1)</TD></TR>

<TR><TD>IP:</TD><TD>roteador-251.tcu.gov.br
(10.1.255.251)</TD></TR>

</TABLE>

11. ANEXO IV – Saída do SnmpWalk

O script snmpwalk foi utilizado para verificação de todas as variáveis SNMP mantidas pelos equipamentos a serem monitorados. A seguir é mostrada parte da saída gerada pelo snmpwalk para o switch LET36. Nota-se que as variáveis conhecidas tem seu OID numérico substituído pelo seu significado, enquanto as OIDs desconhecidas permanecem com seus valores numéricos.

```

system.sysDescr.0 = NMA-RS: AGENT FOR MULTIMEDIA MULTIPROTOCOL
HUB/O.S: vxWorks/UDP.IP/SNMP-CMU
system.sysObjectID.0 = OID: enterprises.81.17.1.11
system.sysUpTime.0 = Timeticks: (181812500) 21 days, 1:02:05.00
system.sysContact.0 =
system.sysName.0 =
system.sysLocation.0 =
system.sysServices.0 = 3
interfaces.ifNumber.0 = 7
interfaces.ifTable.ifEntry.ifIndex.1 = 1
interfaces.ifTable.ifEntry.ifIndex.2 = 2
interfaces.ifTable.ifEntry.ifIndex.3 = 3
interfaces.ifTable.ifEntry.ifIndex.5 = 5
interfaces.ifTable.ifEntry.ifIndex.6 = 6
interfaces.ifTable.ifEntry.ifIndex.7 = 7
interfaces.ifTable.ifEntry.ifDescr.1 = Ethernet channel
interfaces.ifTable.ifEntry.ifDescr.2 = Ethernet channel
interfaces.ifTable.ifEntry.ifDescr.3 = Ethernet channel
interfaces.ifTable.ifEntry.ifDescr.5 = Ethernet channel
interfaces.ifTable.ifEntry.ifDescr.6 = Serial channel
interfaces.ifTable.ifEntry.ifDescr.7 = LANswitch bus
interfaces.ifTable.ifEntry.ifType.1 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.2 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.3 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.5 = ethernetCsmacd(6)
interfaces.ifTable.ifEntry.ifType.6 = slip(28)
interfaces.ifTable.ifEntry.ifType.7 = other(1)
interfaces.ifTable.ifEntry.ifMtu.1 = 1500
interfaces.ifTable.ifEntry.ifMtu.2 = 1500
interfaces.ifTable.ifEntry.ifMtu.3 = 1500
interfaces.ifTable.ifEntry.ifMtu.5 = 1500
interfaces.ifTable.ifEntry.ifMtu.6 = 1500
interfaces.ifTable.ifEntry.ifMtu.7 = 1518
interfaces.ifTable.ifEntry.ifSpeed.1 = Gauge: 10000000

```

```
interfaces.ifTable.ifEntry.ifSpeed.2 = Gauge: 10000000
interfaces.ifTable.ifEntry.ifSpeed.3 = Gauge: 10000000
interfaces.ifTable.ifEntry.ifSpeed.5 = Gauge: 10000000
interfaces.ifTable.ifEntry.ifSpeed.6 = Gauge: 9600
interfaces.ifTable.ifEntry.ifSpeed.7 = Gauge: 1280000000
interfaces.ifTable.ifEntry.ifPhysAddress.1 = 0:40:d:4e:d:9f
interfaces.ifTable.ifEntry.ifPhysAddress.2 = 0:40:d:4e:d:a0
interfaces.ifTable.ifEntry.ifPhysAddress.3 = 0:40:d:4e:d:a1
interfaces.ifTable.ifEntry.ifPhysAddress.5 = 0:40:d:4e:d:a2
interfaces.ifTable.ifEntry.ifPhysAddress.6 = 0:0:0:0:0:0
interfaces.ifTable.ifEntry.ifPhysAddress.7 = 0:0:0:0:0:0
interfaces.ifTable.ifEntry.ifAdminStatus.1 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.2 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.3 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.5 = up(1)
interfaces.ifTable.ifEntry.ifAdminStatus.6 = down(2)
interfaces.ifTable.ifEntry.ifAdminStatus.7 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.1 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.2 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.3 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.5 = up(1)
interfaces.ifTable.ifEntry.ifOperStatus.6 = down(2)
interfaces.ifTable.ifEntry.ifOperStatus.7 = up(1)
interfaces.ifTable.ifEntry.ifLastChange.1 = Timeticks: (225)
0:00:02.25
interfaces.ifTable.ifEntry.ifLastChange.2 = Timeticks: (225)
0:00:02.25
interfaces.ifTable.ifEntry.ifLastChange.3 = Timeticks: (225)
0:00:02.25
interfaces.ifTable.ifEntry.ifLastChange.5 = Timeticks: (226)
0:00:02.26
interfaces.ifTable.ifEntry.ifLastChange.6 = Timeticks: (0) 0:00:00.00
interfaces.ifTable.ifEntry.ifLastChange.7 = Timeticks: (0) 0:00:00.00
interfaces.ifTable.ifEntry.ifInOctets.1 = 0
interfaces.ifTable.ifEntry.ifInOctets.2 = 0
interfaces.ifTable.ifEntry.ifInOctets.3 = 0
interfaces.ifTable.ifEntry.ifInOctets.5 = 0
interfaces.ifTable.ifEntry.ifInOctets.6 = 0
interfaces.ifTable.ifEntry.ifInOctets.7 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.1 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.2 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.3 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.5 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.6 = 0
interfaces.ifTable.ifEntry.ifInUcastPkts.7 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.1 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.2 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.3 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.5 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.6 = 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.7 = 0
interfaces.ifTable.ifEntry.ifInDiscards.1 = 0
interfaces.ifTable.ifEntry.ifInDiscards.2 = 0
interfaces.ifTable.ifEntry.ifInDiscards.3 = 0
interfaces.ifTable.ifEntry.ifInDiscards.5 = 0
interfaces.ifTable.ifEntry.ifInDiscards.6 = 0
interfaces.ifTable.ifEntry.ifInDiscards.7 = 0
interfaces.ifTable.ifEntry.ifInErrors.1 = 0
interfaces.ifTable.ifEntry.ifInErrors.2 = 0
```



```

interfaces.ifTable.ifEntry.ifInErrors.3 = 0
interfaces.ifTable.ifEntry.ifInErrors.5 = 0
interfaces.ifTable.ifEntry.ifInErrors.6 = 0
interfaces.ifTable.ifEntry.ifInErrors.7 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.1 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.2 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.3 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.5 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.6 = 0
interfaces.ifTable.ifEntry.ifInUnknownProtos.7 = 0
interfaces.ifTable.ifEntry.ifOutOctets.1 = 0
interfaces.ifTable.ifEntry.ifOutOctets.2 = 0
interfaces.ifTable.ifEntry.ifOutOctets.3 = 0
interfaces.ifTable.ifEntry.ifOutOctets.5 = 0
interfaces.ifTable.ifEntry.ifOutOctets.6 = 0
interfaces.ifTable.ifEntry.ifOutOctets.7 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.1 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.2 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.3 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.5 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.6 = 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.7 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.1 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.2 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.3 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.5 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.6 = 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.7 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.1 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.2 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.3 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.5 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.6 = 0
interfaces.ifTable.ifEntry.ifOutDiscards.7 = 0
interfaces.ifTable.ifEntry.ifOutErrors.1 = 0
interfaces.ifTable.ifEntry.ifOutErrors.2 = 0
interfaces.ifTable.ifEntry.ifOutErrors.3 = 0
interfaces.ifTable.ifEntry.ifOutErrors.5 = 0
interfaces.ifTable.ifEntry.ifOutErrors.6 = 0
interfaces.ifTable.ifEntry.ifOutErrors.7 = 0
interfaces.ifTable.ifEntry.ifOutQLen.1 = Gauge: 0
interfaces.ifTable.ifEntry.ifOutQLen.2 = Gauge: 0
interfaces.ifTable.ifEntry.ifOutQLen.3 = Gauge: 0
interfaces.ifTable.ifEntry.ifOutQLen.5 = Gauge: 0
interfaces.ifTable.ifEntry.ifOutQLen.6 = Gauge: 0
interfaces.ifTable.ifEntry.ifOutQLen.7 = Gauge: 0
interfaces.ifTable.ifEntry.ifSpecific.1 = OID: .ccitt.nullOID
interfaces.ifTable.ifEntry.ifSpecific.2 = OID: .ccitt.nullOID
interfaces.ifTable.ifEntry.ifSpecific.3 = OID: .ccitt.nullOID
interfaces.ifTable.ifEntry.ifSpecific.5 = OID: .ccitt.nullOID
interfaces.ifTable.ifEntry.ifSpecific.6 = OID: .ccitt.nullOID
interfaces.ifTable.ifEntry.ifSpecific.7 = OID: enterprises.81.19.3
at.atTable.atEntry.atIfIndex.5.1.10.1.201.202 = 5
at.atTable.atEntry.atPhysAddress.5.1.10.1.201.202 = Hex: 00 40 0D 4E
0D A2
at.atTable.atEntry.atNetAddress.5.1.10.1.201.202 = IPAddress:
10.1.201.202
ip.ipForwarding.0 = notForwarding(2)

```

```
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.1.201.202 = IpAddress:
10.1.201.202
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.10.1.201.202 = 5
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.10.1.201.202 = IpAddress:
255.255.0.0
snmp.snmpInPkts.0 = 1131
snmp.snmpOutPkts.0 = 28836
snmp.snmpInBadVersions.0 = 0
snmp.snmpInBadCommunityNames.0 = 3
snmp.snmpInBadCommunityUses.0 = 0
snmp.snmpInASNParseErrs.0 = 0
snmp.snmpInTooBig.0 = 0
snmp.snmpInNoSuchNames.0 = 0
snmp.snmpInBadValues.0 = 0
snmp.snmpInReadOnly.0 = 0
snmp.snmpInGenErrs.0 = 0
snmp.snmpInTotalReqVars.0 = 3056
snmp.snmpInTotalSetVars.0 = 12
snmp.snmpInGetRequests.0 = 629
snmp.snmpInGetNexts.0 = 512
snmp.snmpInSetRequests.0 = 1
snmp.snmpInGetResponses.0 = 0
snmp.snmpInTraps.0 = 0
snmp.snmpOutTooBig.0 = 0
snmp.snmpOutNoSuchNames.0 = 2
snmp.snmpOutBadValues.0 = 0
snmp.snmpOutGenErrs.0 = 0
snmp.snmpOutGetRequests.0 = 0
snmp.snmpOutGetNexts.0 = 0
snmp.snmpOutSetRequests.0 = 0
snmp.snmpOutGetResponses.0 = 1152
snmp.snmpOutTraps.0 = 27708
snmp.snmpEnableAuthenTraps.0 = enabled(1)
enterprises.81.7.1.0 = 10
enterprises.81.7.2.0 = 32
enterprises.81.7.3.0 = 4
enterprises.81.7.4.0 = 2
enterprises.81.7.5.0 = 1
enterprises.81.7.6.0 = 4
enterprises.81.7.7.0 = 2
enterprises.81.7.9.1.1.1.33 = 33
enterprises.81.7.9.1.1.2.33 = 28
enterprises.81.7.9.1.1.3.33 = 6
enterprises.81.7.9.1.1.4.33 = Hex: 00 40 0D 4E 0D 9F
enterprises.81.7.9.1.1.5.33 = OID: enterprises.81.7.9.2
enterprises.81.7.9.1.1.8.33 = "1.0.0"
enterprises.81.7.9.1.1.9.33 = IpAddress: 10.1.201.202
enterprises.81.7.9.2.1.1.33 = 33
enterprises.81.7.9.2.1.2.33 = IpAddress: 0.0.0.0
enterprises.81.7.9.2.1.3.33 = "L8.3.1"
enterprises.81.7.9.2.1.4.33 = "L05.1.1"
enterprises.81.7.9.2.1.5.33 = "L007.0"
enterprises.81.7.9.2.1.6.33 = Hex: 00
enterprises.81.7.9.2.1.8.33 = 1
enterprises.81.7.9.2.1.9.33 = 2
enterprises.81.7.9.2.1.10.33 = 1
enterprises.81.7.9.2.1.11.33 = 1
enterprises.81.7.9.2.1.12.33 = 1
enterprises.81.7.9.2.1.13.33 = 1
```

```
enterprises.81.7.9.2.1.14.33 = 1
enterprises.81.7.9.2.1.16.33 = 1
enterprises.81.7.9.2.1.17.33 = OID: .ccitt.nullOID
enterprises.81.7.9.2.1.20.33 = 2
enterprises.81.7.9.2.1.21.33 = "A" Hex: 41
enterprises.81.7.9.2.1.22.33 = 27
enterprises.81.7.9.2.1.23.33 = "L002.0"
enterprises.81.7.9.2.1.28.33 = 1
enterprises.81.7.9.2.1.29.33 = "A" Hex: 41
enterprises.81.7.9.2.1.30.33 = Hex: 00
enterprises.81.7.9.2.1.31.33 = 1
enterprises.81.7.9.3.1.0 = 10
enterprises.81.7.9.3.2.1.1.1 = 1
enterprises.81.7.9.3.2.1.1.2 = 2
enterprises.81.7.9.3.2.1.2.1 = IpAddress: 10.1.0.50
enterprises.81.7.9.3.2.1.2.2 = IpAddress: 10.1.0.23
enterprises.81.7.9.3.2.1.3.1 = 1
enterprises.81.7.9.3.2.1.3.2 = 1
enterprises.81.7.9.3.6.0 = 2
enterprises.81.7.9.3.8.0 = 100
enterprises.81.7.9.4.0 = 255
enterprises.81.7.9.5.0 = Hex: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00
enterprises.81.7.11.1.1.1.1 = 1
enterprises.81.7.11.1.1.1.2 = 2
enterprises.81.7.11.1.1.2.1 = 3
enterprises.81.7.11.1.1.2.2 = 3
enterprises.81.7.11.1.1.3.1 = 6
enterprises.81.7.11.1.1.3.2 = 7
enterprises.81.7.11.1.1.4.1 = 4986
enterprises.81.7.11.1.1.4.2 = 4986
enterprises.81.7.11.1.1.5.1 = 5250
enterprises.81.7.11.1.1.5.2 = 5250
enterprises.81.7.11.1.1.6.1 = 4800
enterprises.81.7.11.1.1.6.2 = 4800
enterprises.81.7.11.2.0 = 1
enterprises.81.7.11.3.0 = 75
enterprises.81.7.11.4.0 = 49
enterprises.81.7.11.5.0 = 1
enterprises.81.7.12.0 = Timeticks: (136419728) 15 days, 18:56:37.28
enterprises.81.7.13.2.0 = 1
enterprises.81.7.13.4.0 = 0
```

12. ANEXO V – Configuração SNMP e RMON nos Equipamentos

Para permitir o gerenciamento SNMP/RMON nos equipamentos é necessário ativar estas funcionalidades e fazer algumas configurações. Alguns equipamentos já vêm com a configuração padrão de comunidade *public*, que deve ser modificada por motivos de segurança. Se não for necessário nenhum tipo de modificação de configurações através de SNMP pode-se deixar desabilitada esta funcionalidade. É interessante também definir quais endereços ip podem dar comandos SNMP para o equipamento e para quais endereços devem ser enviados os *traps* quando ocorrer alguma condição de anormalidade.

Para configurar o SNMP nos roteadores cisco é necessário que seja feita uma conexão em modo privilegiado, utilizando para este fim o comando `enable` e digitando-se a senha correspondente. Quando é feita a alteração da configuração, a mesma acontece em memória, para salvar as alterações efetuadas é necessário dar o comando `copy run start`. A seguinte seqüência de comandos foi utilizada para configurar o SNMP nos roteadores:

```
snmp-server community scx_TCU RO
snmp-server location Sala de Maquinas - Anexo 1 Terreo
snmp-server contact sesup - 7277
snmp-server enable traps snmp
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server host 10.1.0.23 scx_TCU
```

A primeira linha define a comunidade a ser utilizada e as operações permitidas para esta comunidade, no caso `read-only`. A segunda e terceira linhas definem

respectivamente as variáveis `syslocation` e `syscontact` do grupo `system` da MIB II. As três linhas seguintes definem os tipos de traps a serem enviados e a última linha define o endereço ip para onde devem ser enviados os traps e com que comunidade.

As seqüência de comandos a seguir foi utilizada para configuração de eventos e alarmes RMON nos roteadores. Na definição dos eventos, feita pelo comando `rmon event`, é necessário enumerar as ações a serem executadas quando ocorrer o evento (`log` e `trap`), qual a comunidade a ser utilizada no trap (`scx_TCU`) e a descrição do evento. Os alarmes, definidos pelo comando `rmon alarm`, indicam quais as variáveis a serem monitoradas, o intervalo de monitoração (30 segundos), o tipo de medição (`delta`), os valores de `threshold` de subida e de descida para a variável monitorada durante o período definido e qual evento está associado àquele alarme. Finalmente define-se o `owner` do alarme. No caso específico foram definidos alarmes para número de erros e resets de interface.

```
rmon event 1 log trap scx_TCU description "Elevado numero de erros" owner sesup
rmon event 2 log trap scx_TCU description "Taxa de erros normal" owner sesup
rmon event 3 log trap scx_TCU description "Reset de Interface " owner sesup
rmon event 4 log trap scx_TCU description "Interface Normal " owner sesup
rmon alarm 10 ifEntry.14.2 30 delta rising-threshold 10 1 falling-threshold 0 2 owner sesup
rmon alarm 11 ifEntry.14.4 30 delta rising-threshold 10 1 falling-threshold 0 2 owner sesup
rmon alarm 20 lifEntry.17.2 30 delta rising-threshold 1 3 falling-threshold 0 4 owner sesup
rmon alarm 21 lifEntry.17.4 30 delta rising-threshold 1 3 falling-threshold 0 4 owner sesup
```

Nos demais equipamentos de rede monitorados (switches e hubs) basta configurar a comunidade SNMP a ser utilizada e os endereços dos equipamentos que podem dar comandos e receber traps SNMP. Esta configuração também é efetuada por telnet. No caso do SMON, não é necessária nenhuma configuração, somente entrar com o número da licença nos respectivos equipamentos.

13. ANEXO VI – RFC's Relevantes

Vários RFC's foram utilizados para definição dos protocolos de gerenciamento de rede. Nos quadros a seguir os principais RFC's foram agrupados por área.

SNMPv1

RFC	Título	Status
1155	Structure and Identification of Management Information for TCP/IP-based Internets	Standard
1157	A Simple Network Management Protocol (SNMP)	Standard
1212	Concise MIB Definitions	Standard
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	Standard
1215	Convention for defining traps for use with SNMP	Informational
1418	Simple Network Monitoring Protocol over OSI	Proposed
1419	Simple Network Monitoring Protocol over AppleTalk	Proposed
1420	Simple Network Monitoring Protocol over IPX	Proposed
1573	Evolution of the Interfaces Group of MIB II	Proposed
1643	Definition of Managed Objects for the <i>Ethernet</i> -like Interface Types	Standard

RMON/SMON

RFC	Título	Status
1513	<i>Token Ring</i> Extensions to the Remote Network Monitoring MIB	Proposed
2021	Remote Network Monitoring Management Information Base II	Proposed
2074	Remote Network Monitoring MIB Protocol Identifiers	Proposed
2613	Remote Network Monitoring MIB Extensions for Switched Networks	Proposed
2819	Remote Network Monitoring Management Information Base	Standard
2895	Remote Network Monitoring MIB Protocol Identifier Reference	Proposed

SNMPv2

RFC	Título	Status
1441	Introduction to Version 2 of the Internet-standard Network Management Framework	Proposed
1901	Introduction to Community-based SNMPv2	Experimental
1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)	Draft
1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)	Draft
1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	Draft
1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework	Draft
1909	An Administrative Infrastructure for SNMPv2	Experimental
1910	User-based Security Model for SNMPv2	Experimental
2578	Structure of Management Information for Version 2 (SMIv2)	Standard
2579	Textual Conventions for SMIv2	Standard
2580	Conformance Statements for SMIv2	Standard

SNMPv3

RFC	Título	Status
2570	Introduction to Version 3 of the Internet-Standard Network Management Framework	Informational
2571	An Architecture for Describing SNMP Management Frameworks	Draft
2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	Draft
2573	SNMPv3 Applications	Draft
2574	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	Draft
2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	Draft
2576	Coexistence between Version 1, Version 2 and Version 3 of the Internet-Standard Network Management Framework	Proposed

Network

RFC	Título	Status
1315	Management Information Base for Frame Relay DTEs	Proposed
1604	Definitions of Managed Objects for Frame Relay Service	Proposed
2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2	Proposed
2012	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2	Proposed
2013	SNMPv2 Management Information Base for the User Datagram Protocol using	Proposed

	SMIv2	
2115	Management Information Base for Frame Relay DTEs Using SMIv2	Draft
2863	The Interfaces Group MIB	Draft
2954	Definitions of Managed Objects for Frame Relay Service	Proposed

Transmission

RFC	Título	Status
2108	Definitions of Managed Objects for IEEE 802.3 Repeater Devices using SMIv2	Proposed
2414	Increasing TCP's Initial Window	Experimental
2415	Simulation Studies of Increased Initial TCP Window Size	Informational
2448	Enhancing TCP over Satellite Channels using Standard Mechanisms	Informational
2581	TCP Congestion Control	Proposed
2665	Definitions of Managed Objects for the <i>Ethernet</i> -like Interface Types	Proposed
2760	Outgoing TCP Research Related to Satellites	Informational
2861	TCP Congestion Window Validation	Experimental
2863	The Interfaces Group MIB	Draft
2914	Congestion Control Principles	best current practice

Application

RFC	Título	Status
1297	NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist	Informational
2720	Traffic Flow Measurement: Meter MIB	proposed
2722	Traffic Flow Measurement: Architecture	informational
2758	Definitions of Managed Objects for Service Level Agreement. Performance Monitoring	experimental
2790	Host Resources MIB	Draft