CENTRO UNIVERSITÁRIO FACVEST
CURSO DE CIÊNCIAS DA COMPUTAÇÃO
TIAGO MACHADO DA SILVA

GERENCIAMENTO DE LINK DE DADOS E VOZ COM SIMPLE NETWORK MANAGEMENT PROTOCOL - SNMP

LAGES
2012

TIAGO MACHADO DA SILVA

GERENCIAMENTO DE LINK DE DADOS E VOZ COM SIMPLE NETWORK MANAGEMENT PROTOCOL - SNMP

Trabalho apresentado ao Centro Universitário FACVEST, como parte dos requisitos para obtenção do título de Bacharel em Ciências da Computação.

Orientador: Prof. Msc. Márcio José Sembay

Co-orientador: Prof. Msc. Cassandro Albino Devenz

LAGES

2012

TIAGO MACHADO DA SILVA

GERENCIAMENTO DE LINK DE DADOS E VOZ COM SIMPLE NETWORK MANAGEMENT PROTOCOL - SNMP

Trabalho apresentado ao Centro Universitário FACVEST, como parte dos requisitos para obtenção do título de Bacharel em Ciências da Computação.
Orientador: Prof. Msc. Márcio José Sembay
Co-orientador: Prof. Msc. Cassandro Albino Devenz

Lages, SC _____/_____/2012. Nota _____ _____

(data de aprovação) **(assinatura do orientador do trabalho)**

_____

(coordenador do curso de graduação, nome e assinatura)

LAGES

2012

AGRADECIMENTOS

Aos meus pais José Ariano da Silva e Idená Machado da Silva, as pessoas mais especiais, que me ensinaram a fazer a vida com amor, ética e justiça.

Aos Professores Márcio José Sembay e Cassandro Albino Devens pela sua paciência e inteligência, que souberam orientar e valorizar esta pesquisa.

Aos meus colegas de profissão, sem os quais o meu tempo e capacidade não seriam suficientes para o trabalho.

“O essencial é saber ver – / Mas isso (triste de nós que trazemos a alma vestida!), / Isso exige um estudo profundo, / Uma aprendizagem de desaprender... / Procuro despir-me do que aprendi, / Procuro esquecer-me do modo de lembrar que me ensinaram, / E raspar a tinta com que me pintaram os sentidos, / Desencaixotar as minhas emoções verdadeiras, / Desembrulhar-me e ser eu...” (CAEIRO, citado por SANTANA, Edilson - Filosofar é Preciso, 2007, p. 122).

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AAA	Authentication, Authorization and Accounting
ANEEL	Agência Nacional de Energia Elétrica
ANSI	American National Standards
ARIN	American Registry for Internet Numbers
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
CCITT	Consultative Committe for International Telegraph and Telephone
COT	Centro de Operação da Transmissão
DOD	Departament Of Defense
EGP	Exterior Gateway Protocol
EIA	Electronic Industries Association
FXS	Foreign eXchange Subscriber
IAB	Internet Architecture Board
IANA	The Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
Internic	Internet Network Information Center
IOS	Internetwork Operating System
IP	Internet Protocol
IRTF	Internet Research Task Force
ISO	International Standards Organization
ISOC	The Internet Society
ITU-T	International Telecommunications Union
Mbps	Megabits por Segundo
MIB	Management Information Base
MME	Ministério de Minas e Energia
MTBF	Mean Time Between Failures
NMS	Network Management Station
OID	Object IDentifier
ONS	Operador Nacional do Sistema Elétrico
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PRTG	Paessler Router Traffic Grapher
RFC	Request For Comment
RMON	Remote Monitoring
SIN	Sistema Interligado Nacional
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TBE	Transmissoras Brasileiras de Energia
TIA	Telecommunications Industry Association
UDP	User Datagram Protocol
Vac	Volts Alternating Current
VIC	Voice Interface Card

I - INTRODUÇÃO

1. APRESENTAÇÃO

Ainda que nem sempre tenhamos a capacidade total de compreensão do contexto em que estamos inseridos na sociedade atual, podemos dizer que vivemos um momento singular na história da vida humana sobre a face da terra; Esta é sem dúvida a era de maior revolução tecnológica já experimentada pelo homem, revolução a qual de certa forma foi anunciada e esperada por cientistas até então taxados como "visionários" ou "loucos".

Este momento está sendo marcado pelos grandes avanços da "Nanotecnologia" que ironicamente permitem sonhar com os armazenamentos da ordem de "Giga", "Tera", "Petabytes"; A questão é tão impressionante que mesmo baseada em lógica pura e exata, torna-se impossível analisá-la sem um olhar filosófico acompanhado de questões como "... qual será o limite?".

Algumas das maiores responsáveis por esta loucura desenfreada são as redes de computadores. Elas que hoje se entrelaçam ao redor do planeta inteiro formando uma grande teia, tornaram-se como camaleões, ora fazendo-se presentes por meio de fios metálicos, outras simplesmente por ondas eletromagnéticas navegando a curtas e médias distâncias, em muitos casos em forma de pura e simplesmente luz viajando informações mais rapidamente do que possamos piscar nossos olhos. Este misto capaz de quebrar as fronteiras geográficas e aproximar as pessoas precisa ser gerenciado em diversos níveis para que continue cumprindo sua função ilimitada de conectar o mundo.

> As redes de computadores têm aumentado explosivamente. Desde os anos 70, a comunicação de computadores tem mudado de um tópico de uma pesquisa esotérica para uma parte essencial de infraestrutura. Redes são utilizadas em cada aspecto dos negócios, incluindo publicidade, produção embarcada, faturamento e contabilidade. Consequentemente a maioria das corporações possuem múltiplas redes. Escolas, em todos os níveis de ensino desde o elementar passando pela pós-graduação, estão utilizando redes de computadores para prover estudantes e professores com Acesso instantâneo às informações online. Federal, estado e escritórios locais de governo utilizam redes como fazem as organizações militares. Em resumo, as redes de computadores estão em todos os lugares. (COMER, 2008, pág. 01, tradução nossa).

Contudo, podemos dizer que os fins de utilização das redes são os mais diversos, desde entretenimento até serviços de cunho essencial. O presente trabalho destina-se a abordar a aplicação, importância e gerenciamento de redes aplicadas ao sistema elétrico Brasileiro através do uso de protocolo específico para este fim, o Simple Network Management Protocol – SNMP. São destacados ainda alguns requisitos de confiabilidade estabelecidos pelo Operador Nacional do Sistema Elétrico – ONS e de que forma o SNMP pode auxiliar no cumprimento destes requisitos por parte dos Agentes do setor.

O estudo enfatiza especificamente o gerenciamento de um conjunto de equipamentos de rede redundantes configurados para prover disponibilidade contínua de dados e voz entre as instalações do Centro de Operação da Transmissão – COT da empresa Transmissoras Brasileiras de Energia – TBE localizada em Lages-SC e o Centro de Operação do Sistema Regional Sul – COSR-S do Operador Nacional do Sistema Elétrico – ONS localizado em Florianópolis-SC. Mais do que uma opção, o gerenciamento de infraestrutura básica é tratado aqui como uma necessidade, pois cada serviço assume papel vital em um processo mais complexo o qual forma o Sistema Elétrico Interligado Nacional - SIN, este último por sua vez localizado em posição de grande importância para o desenvolvimento do país.

Este trabalho busca analisar o funcionamento prático do SNMP sob o olhar das normas partindo do RFC1157. Aborda ainda de forma prática, a correlação existente entre agentes e gerentes, respectivamente os ativos de rede que são os servidores SNMP (um par de roteadores cisco da linha 2800 rodando o serviço snmp-server) e os gerentes de rede que são os softwares responsáveis por rodar o serviço de gerência da rede (OpManager) disponibilizando informações de monitoramento e controle de diversas funcionalidades da rede em tempo real, permitindo o supervisionamento do sistema de comunicação.

2. JUSTIFICATIVA

O gerenciamento de redes é o que pode garantir o funcionamento ininterrupto dos serviços essenciais à sociedade atual. Para aplicações domésticas de serviços baseados em redes, admite-se desempenho variável; Até mesmo breves interrupções de fornecimento por falhas em equipamentos são toleradas. Porém, quanto mais subimos o nível partindo do usuário para a infraestrutura das malhas de rede, maiores são as cobranças e responsabilidades. Através de roteadores das operadoras de Telecom trafegam tanto informações do usuário doméstico como do usuário comercial, ou ainda dados dos serviços públicos como hospitais e prefeituras, logo estes equipamentos devem possuir uma disponibilidade consideravelmente maior que os equipamentos domésticos.

O Operador Nacional do Sistema Elétrico trabalha com três classes de serviços de dados e voz. A Classe A é um serviço que deve possuir 99,98% de disponibilidade, a B deve possuir 99% e para a C admite-se até 95%. Pode-se verificar que são índices altos os quais só podem ser alcançados se a rede estiver sendo gerenciada e monitorada constantemente.

> Podemos definir **gerenciamento de redes** como o monitoramento, teste, configuração e diagnóstico de componentes de rede para atender a um conjunto de exigências definido por uma organização. Entre essas exigências, temos a operação estável e eficiente da rede que fornecem a qualidade predefinida de serviços a seus usuários. Para cumprir essa tarefa, um sistema de gerenciamento de redes utiliza hardware, software e pessoas. (FOROUZAN, 2008, pág. 873).

Na busca de relação entre o conceito e a prática, será abordado o surgimento do SNMP. Desde meados dos anos 80 diversas organizações têm envidado esforços a nível mundial no sentido de padronizar a área de redes. Na Europa o principal órgão de referência é o Internet Engineering Task Force – IETF. Este instituto possui áreas específicas para cada segmento tecnológico no âmbito das telecomunicações. Como resultado do trabalho de grupos de pesquisa, nasceram os documentos chamados Request For Comments – RFCs. O modelo criado pelo IETF para gerenciar redes baseia-se inevitavelmente na iteração hardware, software e pessoas. Conhecido como Protocolo Simples de Gerenciamento de Redes ou Simple Network Management Protocol, o SNMP que é formalizado pelo RFC1157 é o eixo desta pesquisa.

3. IMPORTÂNCIA

O constante crescimento da demanda de comunicação confiável em um setor cujo objetivo é nada menos que a matéria prima para movimentar um gigante como o Brasil, por si só, já é uma justificativa para o desenvolvimento de estudos na área, porém, ainda não é tudo.

Viabilizar trabalhos como este por mais simples que possam parecer (aos olhos de Mestres e Doutores na área) é o princípio de uma mudança de paradigma. O paradigma de que a tecnologia e a integração que importamos tem mais valor do que aquela produzida pelos filhos deste país.

Importante citar que as referências encontradas sobre o tema na literatura Internacional são vastas e devem ser valorizadas, porém há de se ter a consciência de que é preciso fomentar a produção e pesquisa interna.

Há de ser dito ainda sobre como este trabalho pode auxiliar na compreensão da aplicação do protocolo SNMP, permitindo monitorar os canais solicitados de acordo com os requisitos definidos como ideais pelo ONS para que este possa disponibilizar o fornecimento de energia confiável à população e assim justificar os investimentos na área.

Para satisfazer todas as áreas que possam ter interesse e se beneficiar dos resultados, dizer ainda que o trabalho poderá auxiliar indiretamente para aumentar os lucros do setor privado.

4. OBJETIVO DO TRABALHO

4.1. Objetivo Geral

Observar a forma como o SNMP é normatizado e como esta é aplicada pelos fabricantes propiciando ao usuário final um determinado nível de integração e usabilidade dos recursos.

4.2. Objetivo Específico

- Apresentar referencial bibliográfico sobre o protocolo simples de gerenciamento de redes utilizado pelas empresas do setor elétrico;
- Apresentar o estudo de uma aplicação de alto desempenho onde o SNMP assume papel de grande importância;

5. METODOLOGIA

Este trabalho de conclusão de curso caminhou paralelamente à aplicação dos circuitos físicos em campo e testes de laboratório. A figura abaixo pode fornecer um panorama das etapas vivenciadas.

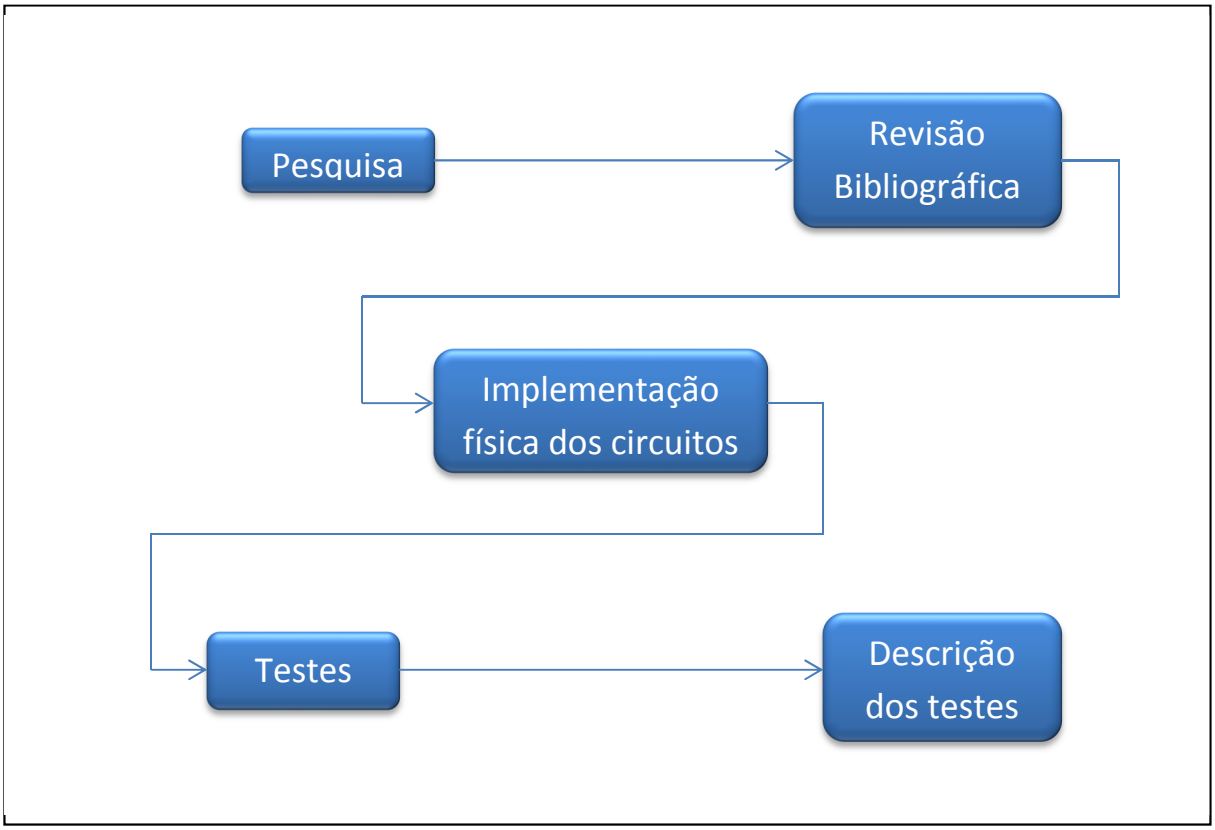

Figura 01. Etapas do desenvolvimento do TCC.
Fonte: próprio autor.

5.1. Caracterização da Pesquisa

De acordo com Richardson (1999), "existem problemas que podem ser investigados por meio de metodologia quantitativa, e há outros que exigem diferentes enfoques e, consequentemente, uma metodologia de conotação qualitativa".

Considerando que ambos os métodos de investigação foram necessários e aplicados a fim de se obter os resultados desejados, o presente trabalho apresenta caráter de pesquisa experimental quanti-qualitativa realizada nos contextos de laboratório e de campo.

> A pesquisa experimental caracteriza-se por manipular diretamente as variáveis relacionadas com o objeto em estudo. Nesta manipulação das variáveis proporciona o estudo da relação entre causas e efeitos de um determinado fenômeno. Através da criação de situações de controle, procura-se evitar a interferência de variáveis intervenientes. Interfere-se diretamente na realidade, manipulando-se a variável independente a fim de observar o que acontece com a dependente (CERVO, 1996, pág. 51).

Para atingir os resultados, o pesquisador fará uso de aparelhos e de instrumentos que a técnica moderna coloca ao seu alcance ou de procedimentos apropriados e capazes de tornar perceptíveis as relações existentes entre as variáveis envolvidas no objeto de estudo (CERVO, 1996, pág. 51).

Muitas foram as variáveis manipuladas até que fossem alcançados os resultados considerados satisfatórios para que o link de dados e voz fosse monitorado e operasse de forma plena, atendendo a procedimentos específicos definidos pelo Operador Nacional do Sistema Elétrico.

A abordagem em relação aos objetivos pode ser dita como quanti-qualitativa uma vez que se preocupa com a análise dos índices de disponibilidade de longos períodos de determinadas variáveis da rede a fim de avaliar os índices diários, semanais, mensais e anuais de disponibilidade (quantitativa), bem como, com a qualidade instantânea destes, para os casos de latência da rede e qualidade de serviço – Quality Of Service-QoS – para voz (qualitativa).

Por fim, a pesquisa abrangeu dois contextos; de laboratório, pois parte dos resultados foi alcançada durante o período dos testes laboratoriais; e de campo, onde durante a implantação observou-se pequenos desvios dos resultados esperados os quais precisaram ser corrigidos;

Uma pesquisa pode ser experimental tanto em contexto de campo quanto de laboratório (CERVO, 1996, pág. 51).

5.2. Coleta e Análise de Dados

Trata-se, em primeiro lugar, da coleta e registro de informações, da análise e interpretação dos dados reunidos e, finalmente, da classificação dos mesmos. (CERVO, 1996, pág. 73).

Para proceder à coleta dos dados foram elaborados roteiros de testes específicos com base nos manuais fornecidos pelos fabricantes do software “Manage Engine”, manuais do ativo de

rede "*Cisco" e "procedimentos de rede – Operador Nacional do Sistema Elétrico-ONS*". Os resultados foram registrados e cada etapa de testes prevista no roteiro em suas respectivas fichas anexado nesta pesquisa.

Por fim procedeu-se à classificação dos dados com referência nos procedimentos de rede – Operador Nacional do Sistema Elétrico-ONS e das regulamentações (RFCs) do Internet Engineering Task Force – IETF.

5.3. Limitação da Pesquisa

Para delimitar o assunto, pode-se fixar circunstâncias, sobretudo de tempo e espaço: trata-se de indicar o quadro histórico e geográfico, em cujos limites se localizam o assunto. (CERVO, 1996, pág. 65).

Considerando a amplitude do tema, o trabalho foi limitado à busca e descrição da forma de configuração da rede bem como do atendimento aos requisitos solicitados por meio dos procedimentos de rede estabelecidos pelo ONS. Abaixo uma síntese dos tópicos focalizados:

- Configuração dos ativos;
- Configuração do SNMP;
- Teste do SNMP;
- Resultados de desempenho e qualidade da rede por meio do SNMP;
- Relatórios dos testes;

Dispondo da ferramenta de gerência de rede ("OpManager"), a empresa TBE, passou a adotar verificações diárias nos ativos da rede visando atender os seguintes requisitos do ONS constantes no Submódulo 13.2 dos procedimentos de rede conforme Anexo A.

- Requisitos de disponibilidade;
- Requisitos de qualidade;
- Requisitos de configuração de voz e dados

6. CRONOGRAMA

Atividades	2012							
	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Determinação do tema								
Revisão Bibliográfica								
Construção Lógica do trabalho								
Testes de laboratório								
Implementação física dos circuitos								
Descrição dos testes								
Desenvolvimento do TCC								
Entrega do TCC a Banca Avaliadora								
Apresentação do TCC a Banca Avaliadora								

Quadro 1. Cronograma do TCC.
Fonte: O próprio autor

II – REVISÃO BIBLIOGRÁFICA

1. DEFININDO SISTEMA DE GERENCIAMENTO DE REDES

Podemos definir gerenciamento de redes como o monitoramento, teste, configuração e diagnóstico de componentes de rede para atender a um conjunto de exigências definido por uma organização. Entre essas exigências, temos a operação estável e eficiente da rede que fornecem a qualidade predefinida de serviços a seus usuários (FOROUZAN, 2008, pág. 873).

No caso específico desta pesquisa, os critérios mínimos de qualidade são predefinidos pelo ONS através do Submódulo 13.2 dos procedimentos de rede conforme Anexo A.

"Para atender à operação do SIN, o serviço de telecomunicações deve dispor de serviços de comunicação de voz e dados em três classes, a saber: A, B e C" (ONS SM13.2, 2010, pág. 04) conforme Anexo A.

As classes definem as características que o serviço deve apresentar. Para a classe 'A', a disponibilidade mínima deve ser de 99,98%, para a classe 'B' de 99% e para a classe 'C' superior a 95%. Considerando que o link em questão atenderá à operação do SIN em tempo real, ele está classificado como classe A.

1.1. Gerenciamento de Configuração

Uma rede de grandes proporções é constituída, normalmente, por centenas de equipamentos e entidades que são ligados entre si de forma física e lógica. Essas entidades apresentam uma configuração inicial quando a rede é ativada, mas essa configuração pode mudar com o tempo. (FOROUZAN, 2008, p. 874).

De acordo com as literaturas de referência, o gerenciamento de configuração é basicamente dividido em duas etapas distintas: de reconfiguração e de documentação.

1.1.1. Reconfiguração

Reconfiguração significa ajustar os componentes e as características da rede, pode ser algo que ocorre diariamente em uma rede grande. Existem três tipos de configuração: de hardware, de software e de conta de usuários. (FOROUZAN, 2008, pág. 874).

O gerenciamento de reconfiguração faz-se constantemente necessário na rede em questão, pois os sistemas computacionais dependentes desta infraestrutura aplicados ao gerenciamento de energia estão em franca expansão. A cada ampliação ou crescimento da rede, por exemplo, no mínimo as regras de segurança e acesso devem ser revisadas.

1.1.2. Documentação

Para que seja possível identificar falhas, intervir com segurança e corrigir defeitos com rapidez e eficácia, faz-se necessário o registro detalhado de cada alteração. Esta também é uma característica fundamental se abordada sob o aspecto da perenidade da rede.

Assim como a reconfiguração, a documentação também deve ser específica para hardware (composta por diagramas e especificações), software e usuários. A documentação de software e usuários é normalmente realizada por meio de utilitários dos sistemas operacionais. Os anexos listados abaixo mostram a documentação da rede em análise neste trabalho:

Anexo	Descrição
A	Diagrama Físico
B	Diagrama Lógico
C	Especificações dos ativos
D	Documentação de Software

Quadro 2. Documentação da rede.
Fonte: Próprio autor

1.2. Gerenciamento de Falhas

As falhas são definidas como condições anormais de funcionamento na rede, ou seja, trata-se de qualquer processo que apresente resultados diferentes do esperado.

Segundo FOROUZAN (2008), o Gerenciamento de falhas consiste em detectar, isolar, notificar e corrigir as falhas na rede. Um sistema de gerenciamento de falhas apresenta dois subsistemas: proativo e reativo.

1.2.1. Reativo

O gerenciamento dito reativo, como o próprio nome sugere, ocorre em reação às falhas detectadas na rede. Primeiramente deve ser feita a detecção do ponto exato que está causando o defeito, a seguir deve ser isolada a falha para que ela atinja o menor número possível de usuários. Depois de isolada, os usuários dos serviços devem ser notificados e informados em relação à previsão de tempo para que ocorra a sua normalização.

Cumpridas estas etapas passa-se à correção do defeito, o qual pode ser de caráter lógico ou físico. Por último deve ocorrer a documentação de todo o processo, pois esta permitirá realizar análises de ordem técnica e gerencial.

Para FOROUZAN (2008), a documentação é extremamente importante por várias razões: O problema pode ser recorrente e neste caso a documentação pode auxiliar a solucionar um problema similar agora ou no futuro. A frequência do mesmo tipo de falha é uma indicação de um problema mais sério no sistema. Dados estatísticos são úteis para outra parte da administração de redes: o gerenciamento de desempenho.

1.2.2. Proativo

O gerenciamento de falhas proativo visa atuar preventivamente na rede de forma a antecipar-se à ocorrência de problemas e assim evitar indisponibilidades. Um bom exemplo de gerenciamento proativo pode ser a intervenção planejada em equipamentos os quais atingiram a vida útil limite (ou o tempo de MTBF) definido pelo fabricante do mesmo.

Esta alternativa representa maior custo em curto prazo, porém, torna a rede mais confiável, sendo ideal para aplicações que exigem alta disponibilidade.

1.3. Gerenciamento de Desempenho

Informalmente, nós utilizamos o termo *velocidade* para descrever a performance de rede, e referir à *rede de baixa* velocidade ou *rede de alta* velocidade. (COMER, 2008, pág. 471, tradução nossa).

O desempenho pode ser definido como o uso eficiente da rede. É preciso que os recursos estejam adequados à demanda da aplicação.

O gerenciamento de desempenho tenta quantificar o desempenho de uma rede usando quantidades mensuráveis como capacidade, tráfego, Throughput ou tempo de resposta. (FOROUZAN, 2008, pág. 876).

1.3.1. Capacidade

A capacidade da rede deve constar do projeto inicial da mesma e o correto gerenciamento desta variável irá garantir que os valores limites desta rede não sejam ultrapassados, sob pena de ocorrerem reduções da taxa de dados e até mesmo interrupção dos serviços que utilizam a infraestrutura.

Os recursos que constituem a rede (número de estações x tráfego médio destas estações) são os principais fatores que determinam a capacidade da mesma. Estes valores são geralmente medidos em Megabits por segundo (Mbps).

1.3.2. Tráfego

O tráfego pode ser medido de duas maneiras: interna e externamente. O tráfego interno é medido pelo número de pacotes (ou bytes) que trafegam pela rede. O tráfego externo é medido pela troca de pacotes (ou bytes) fora da rede. (FOROUZAN, 2008, pág. 876).

1.3.3. Throughput

O Throughput pode ser definido como a taxa de transferência efetiva de um ativo, de uma rede ou ainda de parte dela. Trata-se da quantidade de dados transferida de um lugar a outro em um determinado espaço de tempo.

O gerenciamento de desempenho monitora o Throughput para se certificar de que esta não seja reduzida a níveis inaceitáveis. (FOROUZAN, 2008, pág. 876).

1.3.4. Tempo médio de resposta (Latência)

Refere-se ao tempo médio transcorrido entre o instante em que um usuário solicita um serviço até o momento em que o serviço é atendido. O tempo de resposta pode ser afetado por outros fatores como a capacidade e o tráfego da rede.

O gerenciamento de desempenho monitora o tempo médio de resposta e o tempo de resposta em horários de pico. Qualquer aumento no tempo de resposta é uma condição muito grave, já que ele é uma indicação de que a rede está operando acima de sua capacidade. (FOROUZAN, 2008, pág. 876).

1.3.5. Jitter

> Uma Terceira medida de rede está tornando-se importante à medida que as redes estão sendo utilizadas para a transmissão de vídeo e áudio em tempo real. A medida, a qual é conhecida como *Jitter de rede*, avalia a variação em atraso. Duas redes podem ter a mesma a mesma média de atraso, mas valores diferentes de Jitter. Em particular, se todos os pacotes que atravessam uma dada rede possuem exatamente o mesmo Atraso, D, a rede não possui Jitter. Entretanto, se os pacotes alternam entre um atraso de D+Ɛ e D-Ɛ, a rede possui o mesmo atraso médio, porém, possuem Jitter diferente de zero.
> Para entender porque o Jitter é importante, considere o envio de voz sobre uma rede. No lado do emissor, o sinal analógico é amostrado e digitalizado e após um valor digital de oito bits á emitido a cada 125μ segundos. As amostragens são coletadas dentro dos pacotes, os quais são então transferidos através da rede. No lado receptor, os valores digitais são extraídos e convertidos de volta para saída analógica. Se a rede possui Jitter zero (por exemplo, cada pacote demora exatamente o mesmo tempo para transitar a rede), a saída de áudio irá coincidir com a entrada original; de outra forma, a saída será falha. (COMER, 2008, pág. 476, tradução nossa).

A variação dos tempos de resposta da rede ou *Jitter* podem inviabilizar a utilização de voz sobre uma infraestrutura IP, logo, este deve ser um dos parâmetros a ser medido para garantir o desempenho ideal da aplicação.

1.4. Gerenciamento de Segurança

Esta variável do gerenciamento de desempenho é comumente aplicada a redes mistas com diversos perfis de usuários, onde costumam ocorrer constantes autenticações destes para acesso a arquivos em servidores distribuídos ou mesmo à internet.

O gerenciamento de segurança é responsável pelo controle de acesso à rede tomando como base uma política predefinida. (FOROUZAN, 2008, pág. 876).

Para o caso da presente análise, o gerenciamento de segurança é voltado para o recurso de firewall dos roteadores da rede. Os roteadores deverão permitir tráfego de pacotes somente dos endereços IP definidos nas Access List negando todos os demais. Tentativas de acesso fora da faixa pré-ajustada deverão ser classificadas como 'não autorizados' e ter suas requisições ignoradas.

1.5. Gerenciamento de Contabilização

Gerenciamento de contabilização é a quantificação do acesso e uso dos recursos de rede por seus usuários para fins de tarifação. No gerenciamento de contabilização, usuários individuais, departamentos, divisões ou até mesmo projetos são cobrados pelos serviços que a rede os proporciona; (FOROUZAN, 2008, pág. 877).

O gerenciamento de contabilização em geral é utilizado para verificar o quanto cada usuário, grupo ou projeto utiliza de recurso da rede para suas atividades, com isso ele impede que sejam monopolizados tais recursos, evitam o uso ineficiente deles e permitem que os administradores elaborem planos de curto e longo prazo com base na demanda de uso da rede a fim de estimarem seu crescimento.

Neste projeto há a intenção de utilizar o gerenciamento de contabilização para verificar o quanto cada uma das aplicações que rodam nos servidores da empresa consome da capacidade da rede e com base nestes dados quantificar com maior precisão o custo efetivo que as ampliações nos sistemas de telesupervisão representam.

2. PROCESSOS DO GERENCIAMENTO NA APLICAÇÂO DA TBE

O propósito de gerenciar este link foi reduzir ao mínimo os índices de indisponibilidade dos serviços utilizados pela empresa TBE para com o ONS através da adoção de regras claras visando manter o sistema de rede de acordo com os procedimentos que regem o setor. Para garantir o sucesso desta aplicação foram definidos alguns processos básicos que merecem atenção.

2.1. Gestores da Rede

Os gestores ou administradores da rede possuem a responsabilidade de projetá-la e mantê-la em adequado funcionamento. Algumas das atribuições levantadas como essenciais para esta implantação foram:

- Participar das definições de objetivos do projeto.
- Participar da implantação da rede.
- Acompanhar o processo de compra dos materiais e dispositivos necessários para a aplicação.
- Configurar os equipamentos para operarem conforme a topologia definida no anexo A.
- Disponibilizar e instalar a estação de gerência SNMP.
- Controlar e acompanhar o desempenho do link e demais serviços.
- Divulgar informações periódicas do desempenho dos serviços;

2.2. Procedimentos para Monitoramento

Foi estabelecida a sistemática abaixo listada para a verificação diária dos processos da rede:

- Visualização geral dos alarmes do sistema;
- Visualização específica.
- Emissão de relatórios.
- Divulgação de relatórios.
- Testes.
- Documentação dos testes.

2.3. Planejamento

Os relatórios do link apresentam características quanti-qualitativas e permitirão desta forma que sejam realizadas estimativas de longo prazo sobre uma eventual ampliação ou redução da banda dos canais utilizados em função de:

- Desempenho
- Throughput
- Escalabilidade
- Custo
- Latência

A rede gerenciada permitirá avaliar ainda a respeito da necessidade ou não do estabelecimento de novas rotas extras a fim de garantir a disponibilidade exigida dos serviços.

2.4. Segurança

A segurança é abordada aqui sob dois pontos de vista: O primeiro refere-se a garantir a inviolabilidade dos dados de configurações dos equipamentos uma vez que estes roteadores terão habilitados os serviços de "Telnet" a fim de permitir configuração remota. O segundo ponto que foi observado é referente a permitir o acesso somente de endereços IP conhecidos pela aplicação.

> A utilização da proteção de senha para controlar ou restringir o acesso à interface por linha de comando do roteador é um dos elementos fundamentais de um plano de segurança completo.
> Proteger o roteador de acesso remoto não autorizado, geralmente Telnet, é o aspecto de segurança mais comum que se necessita configurar, porém, proteger o roteador de acesso local não autorizado não pode ser bloqueado. Proteção de senha é somente um dos muitos passos que necessita ser configurado em um regime de segurança efetivo. Firewalls, access-lists, e controle de acesso físico ao equipamento são outros elementos que precisam ser considerados quando da implementação do plano de segurança. (CISCO, 2012, pág. 1, tradução nossa).

Optou-se por senhas criptografadas para acesso aos roteadores, pois desta forma as mesmas não poderão ser identificadas por usuários não autorizados. O firewall foi aplicado de forma a permitir acesso à rede apenas da faixa estabelecida para uso, bem como somente dos

endereços IP definidos para os hosts da aplicação. Foram utilizados os recursos de firewall e access-lists disponíveis no Cisco IOS.

3. NORMATIZAÇÃO

> Produtos que apresentam restrições de compatibilidade e aplicação praticamente perderam seu espaço no mercado... No mundo das redes nada é diferente. Para que uma tecnologia alcance grande sucesso, a padronização deve ser realizada em consenso e com cautela. O mundo globalizado exige produtos que funcionem tanto no Japão quanto no Brasil. Isso só é possível graças à padronização. (MENDES, 2007, pág. 33).

A normatização ou criação de normas permite principalmente que pessoas em diversas partes do mundo possam implementar suas aplicações e que elas possam ser compatíveis.

A normatização permite que diversas tecnologias possam convergir em termos de aplicação. Esta característica é também chamada 'Interoperabilidade', pois uma vez que os equipamentos de fabricantes diferentes produzidos para um mesmo fim possam ser utilizados em conjunto, logo, há um ganho para fabricantes e clientes.

No Brasil, grande parte dos produtos e processos tem suas normas e padrões técnicos regidos pela ABNT (Associação Brasileira de Normas Técnicas), seguindo modelos internacionais. As tecnologias de redes são padronizadas por entidades estabelecidas pelo mundo. (MENDES, 2007, pág. 34).

A lista a seguir das principais entidades utilizadas como referência para padronização internacional podem auxiliar a compreender a importância destas organizações para o sucesso das tecnologias:

- ISO – International Standards Organization.
- ANSI – American National Standards, EUA.
- IEEE – Institute of Electrical and Electronics Engineers.
- ITU-T – International Telecommunications Union.
- EIA – Electronic Industries Association.
- TIA – Telecommunications Industry Association.
- IAB – Internet Architecture Board.
- IETF – Internet Engineering Task Force.
- IRTF – Internet Research Task Force.

- IESG – Internet Engineering Steering Group.
- Internic – Internet Network Information Center.
- ARIN – American Registry for Internet Numbers.
- IANA – The Internet Assigned Numbers Authority.
- ISOC – The Internet Society.

3.1. Internet Engineering Task Force

O instituto Internet Engineering Task Force é uma grande comunidade internacional de designers de rede, operadores, representantes e pesquisadores preocupados com a evolução da arquitetura de internet. A organização é livre de interesses individuais.

Grupo de trabalho que identifica, prioriza e endereça assuntos considerados de curto prazo, incluindo protocolos, arquitetura e operações de serviços. Os padrões propostos são publicados na Internet por meio de RFC (Request for Comment). (MENDES, 2007, pág. 36).

A organização possui grupos de trabalho organizados por tópicos em diversas áreas como roteamento, transporte, segurança, etc. Como documentação destes esforços coletivos, são geradas as Request For Comments que podem ser consultadas gratuitamente em um repositório atualizado que o instituto mantém em sua página oficial na web através do endereço http://www.ietf.org/rfc.html.

3.2. Request for comments

> O termo RFC refere-se aos documentos que especificam padrões e serviços para a Internet e para a arquitetura TCP/IP. É importante observar que, antes de ser concluída e aprovada a RFC é chamada de Internet Draft. As RFCs são numeradas sequencialmente na ordem cronológica em que são escritas. Quando um padrão é revisado, as alterações são escritas numa RFC com um novo número. (MENDES, 2007, pág. 36).

A seguir são destacados os RFCs que estão relacionados ao protocolo SNMP, foco deste trabalho.

RFC	TÍTULO	ÚLTIMA REVISÃO
RFC 1056	PCMAIL: A distributed mail system for personal computers	1988-06

RFC 1058	Routing Information Protocol	1988-06
RFC 1155	Structure and identification of management information for TCP/IP-based internets	1990-05
RFC 1157	Simple Network Management Protocol (SNMP)	1990-05
RFC 1202	Directory Assistance service	1991-02
RFC 1212	Concise MIB definitions	1991-03
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets:MIB-II	1991-03
RFC 1229	Extensions to the generic-interface MIB	1991-05
RFC 1231	IEEE 802.5 Token Ring MIB	1991-05
RFC 1239	Reassignment of experimental MIBs to standard MIBs	1991-06
RFC 1243	AppleTalk Management Information Base	1991-07
RFC 1284	Definitions of Managed Objects for the Ethernet-like Interface Types	1991-12
RFC 1351	SNMP Administrative Model	1992-07
RFC 1352	SNMP Security Protocols	1992-07
RFC 1354	IP Forwarding Table MIB	1992-07
RFC 1389	RIP Version 2 MIB Extensions	1993-01
RFC 1398	Definitions of Managed Objects for the Ethernet-Like Interface Types	1993-01
RFC 1414	Identification MIB	1993-02
RFC 1441	Introduction to version 2 of the Internet-standard Network Management Framework	1993-04
RFC 1445	Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)	1993-04
RFC 1446	Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)	1993-04
RFC 1447	Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)	1993-04
RFC 1448	Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)	1993-04
RFC 1451	Manager-to-Manager Management Information Base	1993-04

RFC 1452	Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework	1993-04
RFC 1461	SNMP MIB extension for Multiprotocol Interconnect over X.25	1993-05
RFC 1472	The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol	1993-06
RFC 1474	The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol	1993-06
RFC 1537	Common DNS Data File Configuration Errors	1993-10
RFC 1623	Definitions of Managed Objects for the Ethernet-like Interface Types	1994-05
RFC 1650	Definitions of Managed Objects for the Ethernet-like Interface Types using SMIv2	1994-08
RFC 1666	Definitions of Managed Objects for SNA NAUs using SMIv2	1994-08
RFC 1696	Modem Management Information Base (MIB) using SMIv2	1994-08

Quadro 3. RFCs relacionadas ao tema.
Fonte: Próprio autor

4. SIMPLE NETWORK MANAGEMENT PROTOCOL – SNMP

No princípio dos anos 80, o gerenciamento de redes era realizado de forma mais simples, pois os ativos em geral estavam fisicamente próximos. Esta característica permitia que os técnicos visualizassem “em loco” o status destes componentes e os mantivessem em boas condições de operação, porém, à medida que as redes foram crescendo percebeu-se a necessidade de criar novos métodos para tal tarefa.

Desenvolvido a mais de 30 anos, o SNMP vem sendo aprimorado de tal forma que continua sendo o protocolo de referência quando o assunto é gerenciamento de rede.

O protocolo simples de Gerenciamento de rede faz parte do conjunto de protocolos TCP/IP e foi desenvolvido nos anos 80 como uma solução para os requisitos de gerenciamento de rede que apareceram devido ao crescimento das infraestruturas de rede. (BARRET; KING, 2010, pág. 271).

O SNMP tem como documentação histórica para referência o RFC 1157 com data de maio de 1990.

4.1. Conceito

Atuando na camada de aplicação do padrão OSI, o SNMP utiliza o conceito de Agente/Gerente para trocar mensagens entre os dispositivos de rede e desta forma prover o gerenciamento da infraestrutura.

4.1.1. Gerentes e Agentes

Para BARRET & KING (2010), a infraestrutura de Gerenciamento do SNMP consiste em três componentes principais: **Nó gerenciado SNMP, Agente SNMP e Estação de gerenciamento de rede (Network Management Station – NMS) SNMP**.

Uma estação gerenciadora, denominada **gerente**, é um host que roda o programa-cliente SNMP. Uma estação gerenciada, denominada **agente**, é um roteador (ou um host) que executa o programa-servidor SNMP. O gerenciamento é obtido pela interação entre gerente e agente. (FOROUZAN, 2008, pág. 878).

A óptica de exposição de BARRET e KING difere da óptica de FOROUZAN no momento em que define uma "estação agente" como uma junção de "Nó gerenciado" com "Agente SNMP". O conceito "agente" de FOROUZAN é a própria junção de "Nó gerenciado SNMP" com o serviço snmp-server do "Agente SNMP".

Quanto ao outro item da definição, (Gerente SNMP ou Estação de gerenciamento de rede - NMS) pode-se perceber que há certa convergência em relação à sua conceptualização, porém, ainda com sútil diferença. Seguindo a ideia lógica de FOROUZAN, aqui podemos entender o conceito "gerente" como a junção do "host" responsável pela hospedagem do serviço com o próprio serviço "Gerente SNMP", fato este que não está claro pela ideia de BARRET e KING quando cita somente a "Estação de Gerenciamento de Rede" como item de definição básico do protocolo.

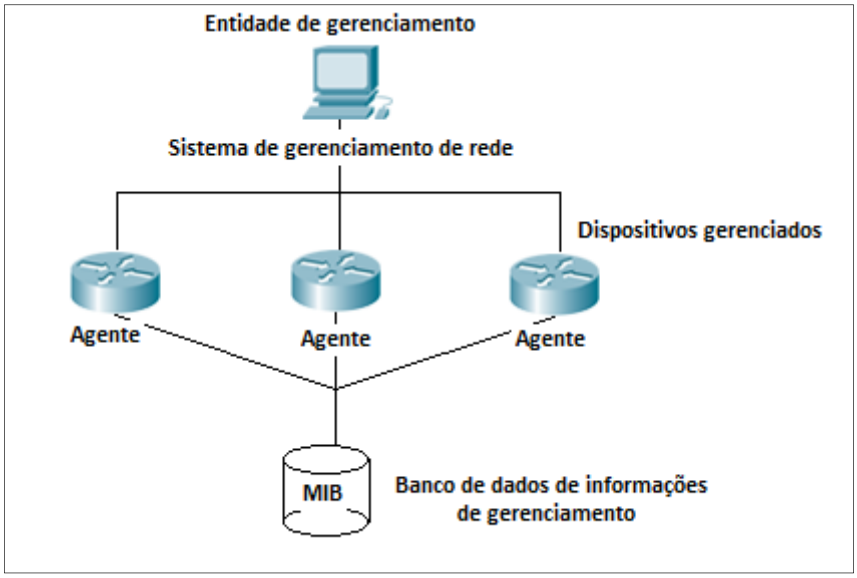

Figura 02. Rede gerenciada por SNMP
Fonte: Barrett; King, 2010.

Para esta etapa, foi adotado como referência o conceito de FOROUZAN por considerar-se que “gerentes” e ”agentes” formam uma ideia mais didática e completa sobre o tema.

O agente mantem suas informações em um banco de dados chamado “Base de Informação de Gerenciamento” o qual está sempre disponível para que o gerente realize consultas e escreva valores nas variáveis. Em alguns casos o agente também pode enviar valores (mensagens de alerta) espontaneamente para o gerente.

A partir desta base de interação gerente x agente surgem três conceitos sobre os quais se pode fundamentar o gerenciamento por meio do SNMP:

- Um gerente solicita informações ao agente;
- Um gerente escreve informações no agente;
- Um agente envia informações espontaneamente ao gerente;

4.2. Componentes do Gerenciamento

Cada agente possui a sua base de informação de gerenciamento (Management Information Base – MIB) o qual toma forma a partir de certas regras contidas na “Estrutura de Informação de Gerenciamento” (Structure of Management Information – SMI).

“... o gerenciamento na internet é realizado por meio da cooperação de três protocolos: SNMP, SMI e MIB...” (FOROUZAN, 2008, pág. 878).

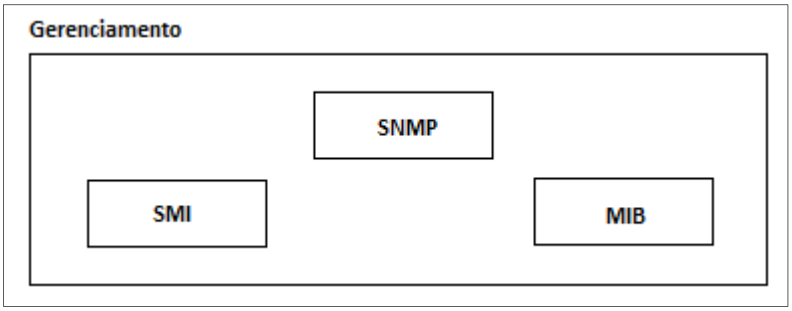

Figura 03. Componentes do gerenciamento de redes na Internet.
Fonte: Forouzan, 2008.

4.2.1. Papel do SNMP

O SNMP é um framework para gerenciamento de dispositivos de rede que utilizam TCP/IP, ou seja, é um conjunto de classes que colaboram para o gerenciamento de dispositivos que utilizam a tecnologia TCP/IP.

O SNMP define o formato dos pacotes trocados entre um gerente e um agente. Ele lê e altera o estado (valores) dos objetos (variáveis) por intermédio de pacotes SNMP. (FOROUZAN, 2008, pág. 879).

4.2.2. Papel do SMI

As regras que determinam o nome, o tipo e como são codificados os objetos no SNMP estão definidas no protocolo auxiliar "Structure of Management Information". Estas regras são universais e, portanto, independem da arquitetura do computador.

O SMI define regras de atribuição de nomes a objetos, estabelece tipos de objeto e mostra como codificar objetos e valores. O SMI não define o número de objetos que uma entidade pode gerenciar, não dá nomes aos objetos a serem gerenciados nem define a associação entre objetos e seus valores. (FOROUZAN, 2008, pág. 879).

Podemos resumir as seguintes funções para o SMI:

- Define a regra de como montar os nomes, porém, não é ele quem dá o nome.
- Lista os tipos de objetos, porém, não é ele quem diz qual o tipo que o objeto deve utilizar.

- Mostra como codificar objetos e valores, porém, não é ele quem define a associação entre objetos e valores.

4.2.3. Papel da MIB

O "Management Information Base" vem a complementar esta lacuna não preenchida pelo SMI. Este é o protocolo responsável por definir o número de objetos, dar nome a eles e fazer a associação de cada tipo a um objeto. Estas tarefas são cumpridas seguindo-se as regras contidas no SMI, é como se o SMI tivesse o papel da linguagem em programação e a MIB o papel do código escrito, onde são definidas quais variáveis existirão e quais seus valores.

A MIB cria um conjunto de objetos com nomes, tipos e relações entre si para uma entidade a ser gerenciada. (FOROUZAN, 2008, pág. 879).

Este conjunto de objetos criados pela MIB para cada entidade apresenta forma semelhante a um banco de dados, por este motivo é assim representada nos diagramas.

4.3. Structure of Management Information – SMI

O SMI é uma diretriz para o SNMP. Ele enfatiza três atributos que identificam um objeto: nome, tipo de dados e método de codificação. (FOROUZAN, 2008, pág. 881).

Este protocolo está na versão 3. Ele é referenciado e definido pelo IETF por meio das RFCs 2578, 2579 e 2580.

4.3.1. Nome

Para Forouzan (2008), "o SMI requer que cada objeto gerenciado tenha um nome exclusivo e para atribuir estes nomes de forma global ele utiliza um identificador hierárquico com base em uma estrutura na forma de árvore".

Para BARRET & KING (2010), o SMI é definido como "Um padrão OSI que controla como as estruturas de dados devem ser organizadas".

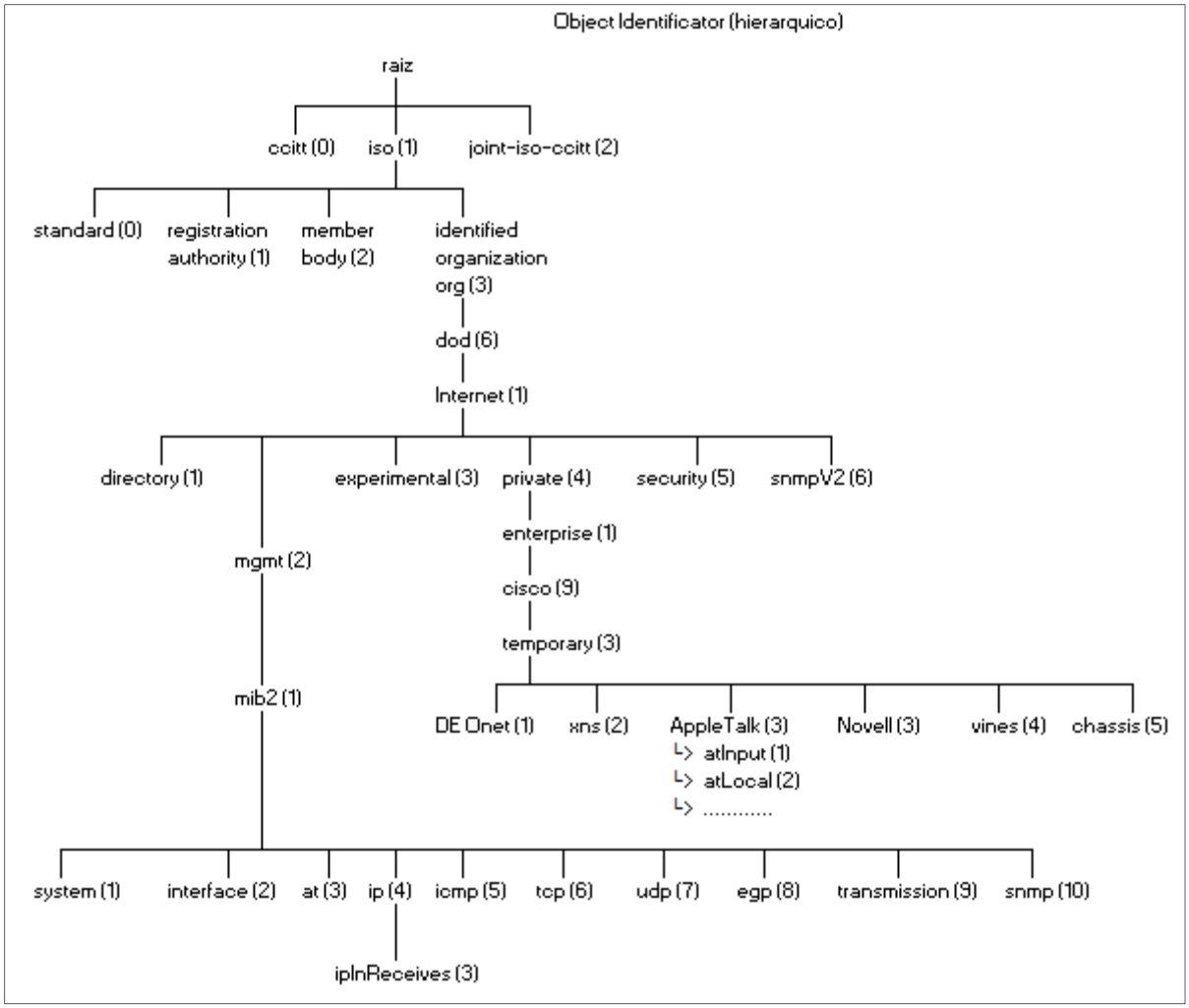

Figura 04. Árvore dos Identificadores de Objetos.
Fonte: próprio autor.

Alguns itens desta estrutura foram investigados com mais detalhes a fim de se adquirir uma compreensão mais ampla de sua aplicação, são eles:

- ccitt (0) - Nó zero da arvore hierárquica definida pela ISO. Representa a estrutura lógica da MIB. Administrado pela Consultative Committe for International Telegraph and telefone.
- iso (1) - Nó um da árvore hierárquica. Administrado pela International Organization for Standardization - ISO.
- joint-iso-ccitt (2) - Nó dois. Administrado em conjunto pela CCITT e pela ISO.
- org (3) - Sub-árvore designada pela ISO para outras organizações.
- dod (6) - USA, Department of Defense. O dod não diz como gerencia sua árvore, assim, assume-se que ele aloca um nó para a comunidade Internet para ser administrada pela Internet Activities Board - IAB.

- directory (1) - Reservada para o uso do diretório OSI na Internet.
- mgmt (2) - Management, utilizada para identificar objetos que estão definidos em documentos aprovados pela IAB. A administração da sub-árvore é delegada para a Internet Assigned Numbers Authority - IANA.
- experimental (3) - Utilizada para identificar objetos usados por experiências da Internet. Administrada pela IANA.
- private (4) - Utilizada para identificar objetos definidos unilateralmente (para Indústria). Sub-árvore administrada pela IANA.
- enterprises (1) - Utilizada entre outras coisas para permitir que prováveis facções de subsistemas de redes registrem modelos de seus produtos. Recebendo uma sub-árvore, a empresa pode, por exemplo, definir novos objetos MIB na sua sub-árvore. Com isto é recomendado que ela registre também seus subsistemas de rede abaixo desta sub-árvore, de modo a evitar ambiguidade no mecanismo de identificação a serem usados pelos protocolos de gerência.

> A estrutura em forma de árvore também pode definir um objeto pela sequencia de nomes textuais separados por pontos. O SNMP utiliza a representação inteiro-ponto. A notação nome-ponto é usada por pessoas. Por exemplo, as duas formas a seguir mostram o mesmo objeto em duas notações distintas: iso.org.dod.internet.mgmt.mib-2 ➔ 1.3.6.1.2.1.
> Os objetos que são usados pelo SNMP se localizam abaixo do objeto mib-2, de modo que seus identificadores sempre sejam iniciados com 1.3.6.1.2.1. (FOROUZAN, 2008, pág. 882).

4.3.2. Tipo

Para definir o tipo de dado, o SMI usa as definições padronizadas pelo **ASN.1 (Abstract Syntax Notation 1 – Notação de sintaxe abstrata 1)** e acrescenta algumas definições novas. Em outras palavras, o SMI é tanto um subconjunto como um superconjunto do ASN.1. O SMI tem duas categorias de dados: *simples* e *estruturada.* (FOROUZAN, 2008, pág. 882).

4.3.2.1. Tipo Simples

Este tipo de dado é definido por FOROUZAN apenas como sendo um tipo de dado atômico.

Tipo	*Tamanho*	*Descrição*
INTEGER	4 bytes	Inteiro com valor entre -2^{31} a $2^{31}-1$
Integer32	4 bytes	Idem a INTEGER
Unsigned32	4 bytes	Sem sinal com valor entre 0 a $2^{32}-1$
OCTET STRING	Variable	String de bytes até 65.535 bytes de comprimento
OBJECT IDENTIFIER	Variable	Identificador de objeto
IPAddress	4 bytes	Endereço IP composto por quatro inteiros
Counter32	4 bytes	Inteiro cujo valor pode ser incrementado de 0 a 2^{32}, quando atinge seu valor máximo, recomeça do zero
Counter64	8 bytes	Contador de 64bits
Gauge32	4 bytes	Idem a Counter32, mas quando atinge seu valor máximo, ele não reinicia do zero, mas permanece nesse valor até ser reiniciado.
TimeTicks	4 bytes	Valor de contagem que registra o tempo em 1/100 s
BITS		String de bits
Opaque	Variable	String não interpretada

Quadro 04. Tipos de dados do ASN.1.
Fonte: FOROUZAN, 2008, pág. 883

4.3.2.2. Tipo Estruturado

Pela combinação de tipos de dados estruturados e simples, podemos criar novos tipos de dados estruturados. O SMI define dois **tipos de dados estruturados:** *sequence* e *sequence of*. (FOROUZAN, 2008, pág. 883).

O tipo *sequence* caracteriza-se por uma combinação de tipos de dados simples não necessariamente do mesmo tipo, enquanto *sequence of* caracteriza-se por uma combinação de tipos de dados simples, em geral todos do mesmo tipo ou uma combinação de tipos de dados sequence do mesmo tipo. FOROUZAN ainda utiliza de uma forma muito clara a analogia citada com o conceito de registro e array em linguagem C para definir respectivamente *sequence* e *sequence of*.

4.3.3. Método de Codificação

O SMI usa outro padrão, as BER (**Basic Encoding Rules – regras de codificação básicas**), para codificar dados a serem transmitidos através de uma rede. As BER especificam que cada um dos dados seja codificado em um formato de trinca: marca, comprimento e valor. (FOROUZAN, 2008, pág. 884).

4.3.3.1. Basic Encoding Rules – BER

O padrão Internacional consultado o qual especifica o grupo de regras básicas que podem ser utilizadas para codificação foi a recomendação X.690 pertencente à Série X: *Data Networks and Open System Communications* definida pelo ITU-T.

O X.690: **Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).**

Através desta recomendação, podemos perceber que existem três regras de codificação para uso em conjunto com o Abstract Syntax Notation One, dentre as quais se podem destacar o BER.

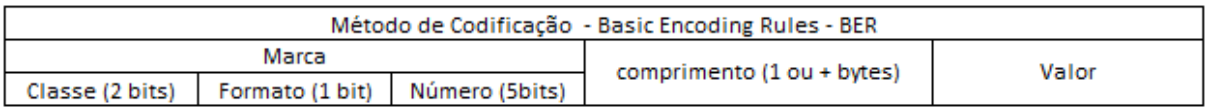

Figura 05. Componentes do BER.
Fonte: próprio autor.

O Método BER pode ser inicialmente dividido em três campos: marca, Comprimento e Valor. Sendo o primeiro responsável pela informação do tipo de dado, o segundo pela identificação do tamanho e o terceiro o próprio dado transmitido.

O campo marca por sua vez subdivide-se em outros três campos: Classe, Formato e Número. O primeiro define a abrangência dos dados, o segundo indica se se trata de dados simples (0) ou estruturado (1) e o terceiro subdivide os dados em subgrupos.

> O subcampo class define a abrangência dos dados. São definidas quatro classes: universal (00), aplicationwide (01), contexto-specific (10) e private (11). Os tipos de dados universal são extraídos do ASN.1 (INTEGER, OCTET STRING e ObjectIdentifier). Os tipos de dados applicationwide são aqueles acrescentados pelo SMI (IPAddress, Counter, Gauge e TimeTicks). Os cinco tipos de dados contexto-specific apresentam significados que podem variar de protocolo para protocolo. Os tipos de dados private são específicos de cada fornecedor. (FOROUZAN, 2008, pág. 884).

Tipo de dados	*Classe*	*Formato*	*Número*	*Marca (Binária)*	*Marca (Hexa)*
INTEGER	00	0	00010	**00000010**	**02**
OCTET STRING	00	0	00100	**00000100**	**04**
OBJECT IDENTIFIER	00	0	00110	**00000110**	**06**
NULL	00	0	00101	**00000101**	**05**
Sequence, sequence of	00	1	10000	**00110000**	**30**
IPAddress	01	0	00000	**01000000**	**40**
Counter	01	0	00001	**01000001**	**41**
Gauge	01	0	00010	**01000010**	**42**
TimeTicks	01	0	00011	**01000011**	**43**
Opaque	01	0	00100	**01000100**	**44**

Quadro 05. Tipos de dados do BER.
Fonte: FOROUZAN, 2008, pág. 885

4.4. Management Information Base – MIB

Para FOROUZAN, o MIB2 é o segundo componente-chave utilizado no gerenciamento de redes.

Cada agente tem sua própria MIB2, que é um conjunto de todos os objetos que o gerente pode administrar. Os objetos da MIB2 são classificados em 10 grupos diferentes: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission e snmp. (FOROUZAN, 2008, pág. 886).

> Objetos em uma MIB são definidos com o esquema de nomes do ASN.1, o qual designa à cada objeto um prefixo longo que irá garantir que os nomes sejam únicos. Por exemplo, uma integer que conta o número de datagramas IP que um dispositivo recebe é nomeada: *iso.org.dod.internet.mgmt.mib.ip.ipInReceives.* Quando o nome do objeto é representado em uma mensagem SNMP, cada parte do nome recebe um valor inteiro. Assim, em uma mensagem SNMP, o nome de *ipInReceives* é: 1.3.6.1.2.1.4.3. (COMER, 2008, pág. 543, tradução nossa).

A representação do objeto em valores inteiros (para encapsulamento no protocolo SNMP) separados por pontos recebe o nome de Object Identifier, ou simplesmente *OID*.

4.4.1. Objetos da MIB2

Os dez grupos de Objetos da MIB2 localizados na árvore de identificadores de objetos são representados pela figura abaixo.

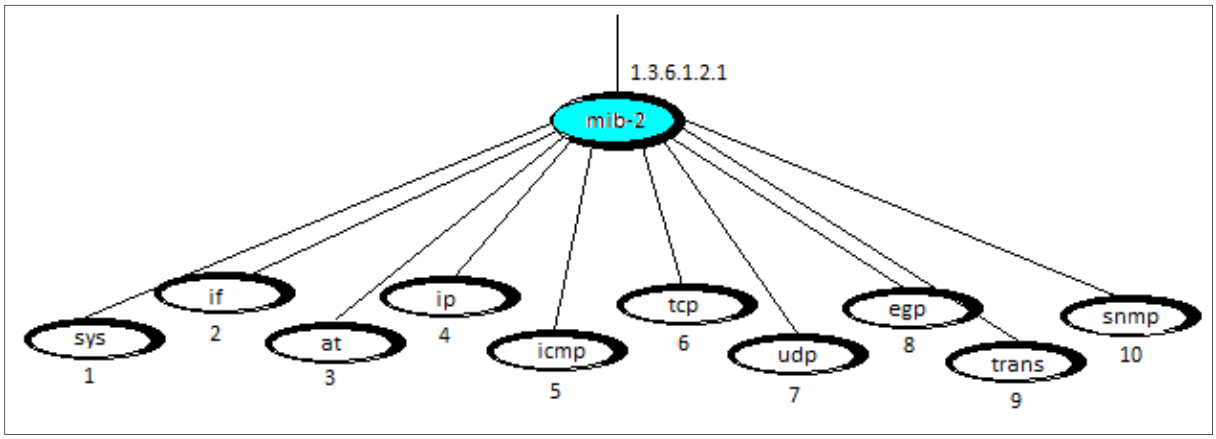

Figura 06. Componentes da sub-árvore mib-2.
Fonte: FOROUZAN, 2008.

A seguir breve síntese das funcionalidades de cada grupo de acordo com as RFCs 1066, 1213 e 2863. Dentro de cada grupo segue uma lista/amostragem de alguns objetos e respectivos OIDs. Esta lista irá variar em tamanho dependendo do fabricante do dispositivo. A forma mais confiável de consulta de um OID é por meio de sites especializados e que possuem serviço de repositório como, por exemplo, o *OID Repository* [http://oid-info.com/get], ou o *OID VIEW* [http://www.oidview.com].

- **sys (system) –** Define informações gerais sobre o nó (system), como nome, localização e vida útil.

  Fornece contato, administrativo, localização, e informações de serviços relativas ao nó gerenciado. (RFC 1213, 1991, pág. 5, tradução nossa).

system - sys - 1.3.6.1.2.1.1			
Objeto	*Descrição*	*OID*	*Rfc*
sysDecr	Descrição textual da entidade	1.3.6.1.2.1.1.1	1066
sysObjectID	Fabricante do sistema	1.3.6.1.2.1.1.2	1066
sysUpTime	O tempo em centésimos de segundo desde a última reinicialização do sistema	1.3.6.1.2.1.1.3	1066
sysContact	Identificação textual da pessoa responsável pela gerência do nó.	1.3.6.1.2.1.1.4	1213
sysName	Uma designação de nome administrativo para o nó gerenciado.	1.3.6.1.2.1.1.5	1213
sysLocation	A localização física do nó. Ex.: Piso, prédio, etc..	1.3.6.1.2.1.1.6	1213

sysServices	Um valor o qual indica o tipo de serviço primário que esta entidade oferece.	1.3.6.1.2.1.1.7	1213

Quadro 06. Componentes da MIB system.
Fonte: próprio autor

- **if (interface) –** Define informação sobre todas as interfaces instaladas no nó, inclusive número de interface, endereço físico e endereço IP.

interface - if - 1.3.6.1.2.1.2			
Objeto	*Descrição*	*OID*	*Rfc*
ifNumber	O número das interfaces de rede nas quais este sistema pode enviar e receber datagramas IP.	1.3.6.1.2.1.2.1	1066
ifTable	A lista de entradas de interface. O numero de entradas é dado pelo valor do ifNumber.	1.3.6.1.2.1.2.2	1066
ifEntry	Entrada de interface contendo objetos do link de rede e abaixo para uma interface particular.	1.3.6.1.2.1.2.2.1	1066
ifIndex	Valor único por cada interface. O range deste valor está entre 1 e o valor de ifNumber.	1.3.6.1.2.1.2.2.1.1	1066
ifDescr	String de texto contendo informações da interface. Esta string deve incluir o nome do fabricante, do produto e da versão do hardware da interface.	1.3.6.1.2.1.2.2.1.2	1066
ifType	O tipo de interface. De acordo com o protocolo do link físico imediatamente abaixo do link de rede no protocolo.	1.3.6.1.2.1.2.2.1.3	1066
ifMtu	Tamanho do maior datagrama permitido (em octetos)	1.3.6.1.2.1.2.2.1.4	1066

Quadro 07. Componentes da MIB interface.
Fonte: próprio autor

- **at (address translation) –** Define as informações sobre a tabela ARP.

address translation - at - 1.3.6.1.2.1.3			
Objeto	*Descrição*	*OID*	*Rfc*

atTable	Contêm o endereço de rede equivalente ao endereço físico. Algumas interfaces não usam tabela de tradução para determinar as equivalências.	1.3.6.1.2.1.3.1	1066
atEntry	Cada entrada contém um endereço de rede para equivalência de um físico.	1.3.6.1.2.1.3.1.1	1066
atIfIndex	A interface na qual a equivalência. desta entrada é efetiva. A interface identificada por um valor particular do índice é a mesma interface identificada pelo valor do ifIndex.	1.3.6.1.2.1.3.1.1.1	1066
atPhysAddress	O endereço físico da dependência de mídia.	1.3.6.1.2.1.3.1.1.2	1066
atNetAddress	O endereço de rede (ip) correspondente ao endereço físico da mídia.	1.3.6.1.2.1.3.1.1.3	1066

Quadro 08. Componentes da MIB address translation.
Fonte: próprio autor

- **ip (IP) –** Define informações referentes ao IP, como tabela de roteamento e endereço IP.

IP - ip			
Objeto	*Descrição*	*OID*	*Rfc*
ipForwarding	Indica se esta entidade está atuando como um IP gateway em relação ao repasse dos datagramas recebidos.	1.3.6.1.2.1.4.1	1066
ipDefaultTTL	O valor padrão inserido no campo tempo de vida do cabeçalho do datagrama.	1.3.6.1.2.1.4.2	1066
ipInReceives	O número total de datagramas de entrada recebido das interfaces.	1.3.6.1.2.1.4.3	1066
ipInHdrErrors	O número de datagramas descartados por erros em seus cabeçalhos de IP.	1.3.6.1.2.1.4.4	1066
ipInAddrErrors	O número de datagramas descartados porque o endereço de destino IP não foi um endereço considerado válido.	1.3.6.1.2.1.4.5	1066
ipForwDatagrams	O número de datagramas de entrada pelos quais esta entidade não encontrou seu destino final, como resultado uma tentativa foi feita de encontrar a rota até o destino final.	1.3.6.1.2.1.4.6	1066

ipInUnknownProtos	O número de datagramas recebidos com sucesso pelo localhost, mas descartados por causa de um protocolo desconhecido ou não suportado.	1.3.6.1.2.1.4.7	1066

Quadro 09. Componentes da MIB ip.
Fonte: próprio autor

- **icmp (ICMP) –** Define informações relacionadas à ICMP, como número de pacotes enviados e recebidos.

ICMP - icmp - 1.3.6.1.2.1.5			
Objeto	*Descrição*	*OID*	*Rfc*
icmpInMsgs	O número total de mensagens icmp as quais a entidade recebeu, incluindo as de erros.	1.3.6.1.2.1.5.1	1066
icmpInErros	O número de mensagens icmp que a entidade recebeu, mas determinou que tivessem erros.	1.3.6.1.2.1.5.2	1066
icmpInDestUnreachs	O número de destinos icmp recebidos com mensagem unreachable.	1.3.6.1.2.1.5.3	1066
icmpInTimeExceds	O número de mensagens icmp recebidas com tempo excedido.	1.3.6.1.2.1.5.4	1066
icmpInParmProbs	O número de mensagens icmp recebidas com problemas de parâmetro.	1.3.6.1.2.1.5.5	1066
icmpInSrcQuenchs	O número de mensagens icmp recebidas de fonte extinta.	1.3.6.1.2.1.5.6	1066
icmpInRedirects	O número de mensagens icmp redirecionadas recebidas.	1.3.6.1.2.1.5.7	1066

Quadro 10. Componentes da MIB icmp.
Fonte: próprio autor

- **tcp (TCP) –** Define informações gerais relacionadas ao TCP, como tabela de conexões, valor de timeout, número de portas e números de pacotes enviados e recebidos.

TCP - tcp - 1.3.6.1.2.1.6			
Objeto	*Descrição*	*OID*	*Rfc*
tcpRtoAlgorithm	O algoritmo utilizado para determinar o valor de timeout utilizado para retransmitir o octeto de reconhecimento.	1.3.6.1.2.1.6.1	1066

tcpRtoMin	O valor mínimo (medido em milissegundos) permitido por uma implementação tcp para retransmissão do timeout.	1.3.6.1.2.1.6.2	1066
tcpRtoMax	O valor máximo (medido em milissegundos) permitido por uma implementação tcp para retransmissão do timeout.	1.3.6.1.2.1.6.3	1066
tcpMaxConn	O limite do número total de conexões tcp que a entidade pode suportar.	1.3.6.1.2.1.6.4	1066
tcpActiveOpens	O número de vezes que a conexão tem feito uma transição direta para o estado SYN-SENT a partir do estado fechado.	1.3.6.1.2.1.6.5	1066
tcpPassiveOpens	O número de vezes que a conexão tem feito uma transição direta para o estado SYN-RCVD a partir do estado fechado.	1.3.6.1.2.1.6.6	1066
tcpAttemptFails	O número de vezes que a conexão tem feito uma transição direta para o estado fechado a partir dos estados SYN-SENT ou SYN-RCVD, mais o número de vezes que a conexão tcp tem feito uma transição direta do estado SYN-RCVD para o estado LISTEN.	1.3.6.1.2.1.6.7	1066

Quadro 11. Componentes da MIB tcp.
Fonte: próprio autor

- **udp (UDP) –** Define informações gerais relativas ao UDP, como número de portas e número de pacotes enviados e recebidos.

UDP - udp - 1.3.6.1.2.1.7			
Objeto	*Descrição*	*OID*	*Rfc*
udpInDatagrams	O número total de datagramas UDP entregue para o usuário UDP.	1.3.6.1.2.1.7.1	1066
udpNoPorts	O número total de datagramas UDP recebidos para os quais não há aplicação na porta de destino.	1.3.6.1.2.1.7.2	1066
udpInErrors	O número de datagramas UDP recebidos que não puderam ser entregues por razões outras que não a aplicação da porta destino.	1.3.6.1.2.1.7.3	1066
udpOutDatagrams	O número total de datagramas UDP enviados a partir desta entidade.	1.3.6.1.2.1.7.4	1066

udpTable	Uma tabela contendo informações do host ouvinte.	1.3.6.1.2.1.7.5	1213
udpEntry	Informação sobre o atual host ouvinte UDP.	1.3.6.1.2.1.7.5.1	1213
udpLocalAddress	O endereço IP local para o host ouvinte UDP.	1.3.6.1.2.1.7.5.1.1	1213

Quadro 12. Componentes da MIB udp.
Fonte: próprio autor

- **egp (EGP) –** A implementação do grupo EGP é obrigatória para todos os sistemas que implementam o protocolo EGP. (RFC 1066, 1988, pág. 63, tradução nossa).

EGP - egp - 1.3.6.1.2.1.8			
Objeto	*Descrição*	*OID*	*Rfc*
egpInMsgs	O número de mensagens egp recebidas sem erros.	1.3.6.1.2.1.8.1	1066
egpInErrors	O número de mensagens egp recebidas que provaram ser erros.	1.3.6.1.2.1.8.2	1066
egpOutMsgs	O número total de mensagens egp geradas localmente.	1.3.6.1.2.1.8.3	1066
egpOutErrors	O número de mensagens egp geradas localmente e não enviadas por limitação própria dentro da entidade egp.	1.3.6.1.2.1.8.4	1066
egpNeighTable	Tabela egp das entidades vizinhas.	1.3.6.1.2.1.8.5	1066
egpAs	O sistema autônomo de números da entidade egp.	1.3.6.1.2.1.8.6	1213
egpNeighEntry	Informação sobre o relacionamento desta entidade egp com uma egp vizinha.	1.3.6.1.2.1.8.5.1	1066

Quadro 13. Componentes da MIB egp.
Fonte: próprio autor

- **trans (transmission) –** A MIB-1 era falha à medida que não distinguia entre diferentes tipos de meios de transmissão. (RFC 1213, 1991, pág. 8, tradução nossa).
- **snmp (SNMP) –** Define informações gerais relativas ao SNMP.

  Para o SNMP é útil ter informações estatísticas. Um novo grupo, o grupo snmp é alocado para este propósito. (RFC 1213, 1991, pág. 8, tradução nossa).

SNMP - snmp - 1.3.6.1.2.1.10			
Objeto	*Descrição*	*OID*	*Rfc*
snmpInPkts	O número total de mensagens entregue para a entidade SNMP a partir do serviço de transporte.	1.3.6.1.2.1.10.1	1213

snmpInGenErrs	O número total de PDUs SNMP que foram entregues para a entidade do protocolo e para os quais o valor do campo Status de erro é 'genErr'.	1.3.6.1.2.1.10.12	1213
snmpInGetNexts	O número total de PDUs SNMP Get-Request que foram aceitos e processados pela entidade do protocolo SNMP.	1.3.6.1.2.1.10.16	1213
snmpInTraps	O número total de PDUs Trap SNMP que foram aceitos e processados pela entidade de protocolo SNMP.	1.3.6.1.2.1.10.19	1213
snmpOutPkts	O número total de mensagens SNMP as quais passaram da entidade de protocolo SNMP para o serviço de transporte.	1.3.6.1.2.1.10.2	1213
snmpInBadVersions	O número total de mensagens SNMP que foram entregues para a entidade do protocolo SNMP e não foram suportados pela versão.	1.3.6.1.2.1.10.3	1213
snmpInTooBigs	O número total de PDUs SNMP que foram entregues para a entidade do protocolo e nos quais o valor do campo de status de erro 'sem nome'.	1.3.6.1.2.1.10.8	1213

Quadro 14. Componentes da MIB snmp.
Fonte: próprio autor

4.4.2. Acesso às Variáveis da MIB

Cada um dos dez grupos define suas próprias variáveis ou tabelas. Para acessar as variáveis, ou tabelas utiliza-se o id do grupo seguido pelo id da variável. Em seu livro FOROUZAN exemplifica à pág. 887 o acesso de quatro variáveis do grupo udp conforme relacionado abaixo, no entanto, destaca claramente que eles definem apenas a variável e não a instância (o seu conteúdo).

udpInDatagrams → 1.3.6.1.2.1.7.1
udpNoPorts → 1.3.6.1.2.1.7.2
udpInErrors → 1.3.6.1.2.1.7.3
udpOutDatagrams → 1.3.6.1.2.1.7.4

Para mostrar a instância ou o conteúdo de cada variável, temos de adicionar um sufixo de instância. O sufixo de instância para uma variável simples é um simples zero. (FOROUZAN, 2008, pág. 888).

Acesso ao conteúdo do exemplo:

udpInDatagrams	→	1.3.6.1.2.1.7.1.0
udpNoPorts	→	1.3.6.1.2.1.7.2.0
udpInErrors	→	1.3.6.1.2.1.7.3.0
udpOutDatagrams	→	1.3.6.1.2.1.7.4.0

4.4.3. Acesso às Tabelas da MIB

Para identificar uma tabela, utiliza-se o id da mesma (Ex.: udpTable → 1.3.6.1.2.1.7.5). Porém, em sua formação as tabelas são definidas por uma numeração sequencial, desta forma deve-se acrescentar o id do campo *Entry* (udpEntry → 1.3.6.1.2.1.7.5.1) e somente então se inicia o processo de acesso às entidades contidas na tabela. Analisando a figura abaixo ilustrada por FOROUZAN, é possível visualizar a estrutura de entidades individuais e tabelas.

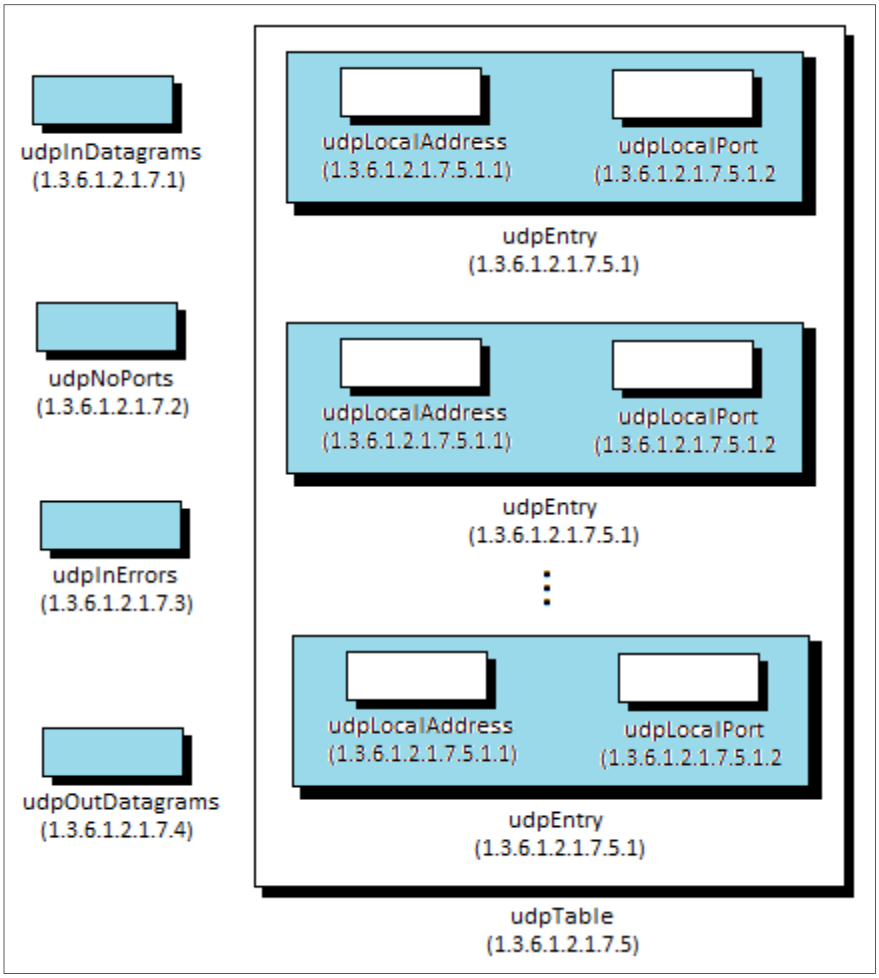

Figura 07. Acesso à Tabela da MIB.
Fonte: FOROUZAN, 2008.

4.5. PDUs

O Protocol Data Unit (PDU) é o formato de mensagem que gerentes e agentes utilizam para enviar e receber informações. Cada um dos seguintes operadores SNMP possui um formato padrão de PDU: get, getnext, getbulk (SNMPv2 e SNMPv3), set, getresponse, trap, notification (SNMPv2 e SNMPv3), inform (SNMPv2 e SNMPv3), report (SNMPv2 e SNMPv3). (MAURO; SCHIMIDT, 2005, pág. 37, tradução nossa).

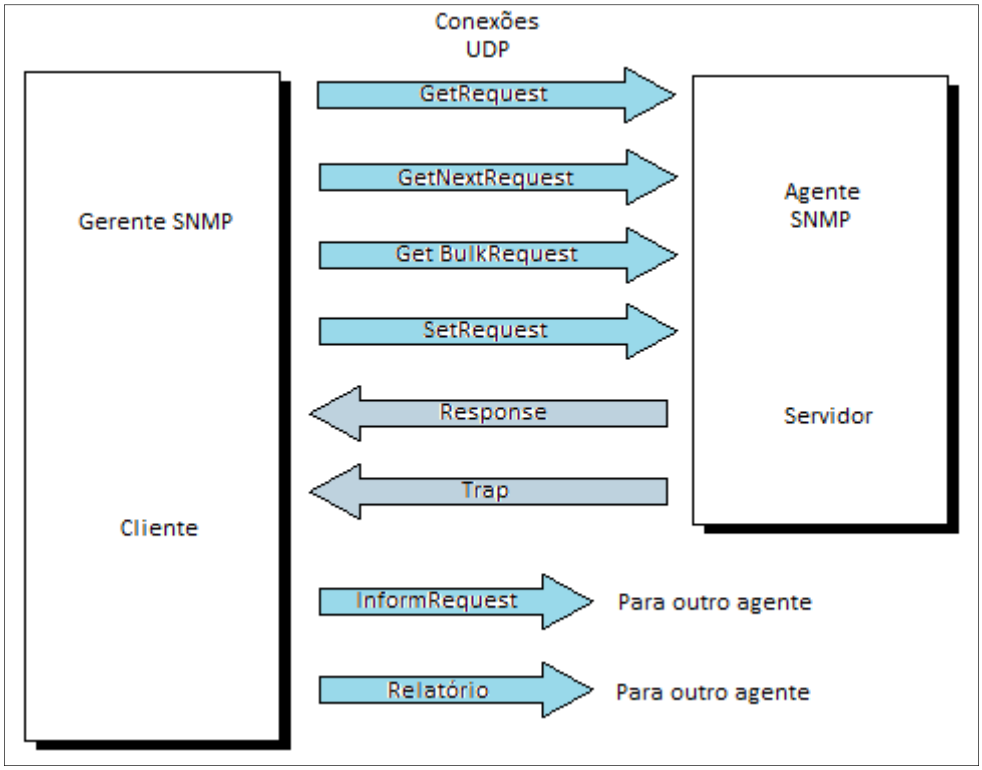

Figura 08. Troca de mensagens PDU.
Fonte: FOROUZAN, 2008.

4.5.1. GetRequest

O PDU GetRequest é enviado do gerente (cliente) para o agente (servidor) para leitura de um valor de uma variável ou um conjunto de variáveis. (FOROUZAN, 2008, pág. 891).

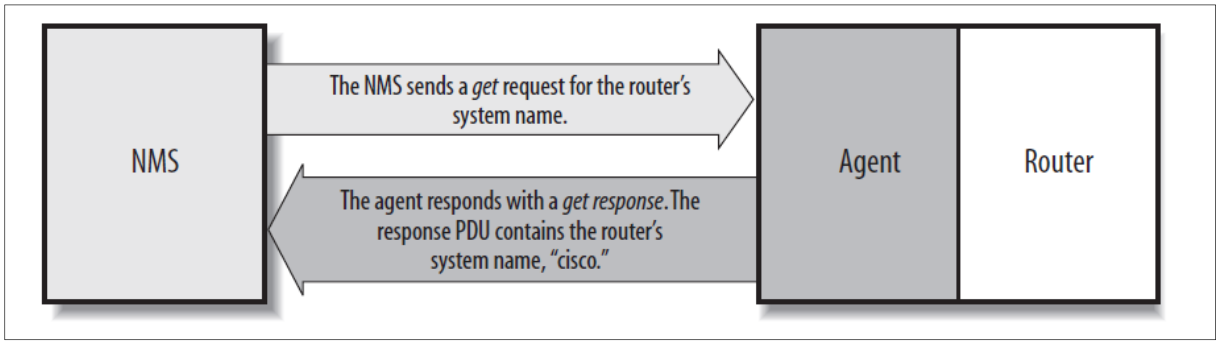

Figura 09. GetRequestSequence.
Fonte: (MAURO; SCHIMIDT, 2005, pág. 38).

Mauro & Schimidt esclarecem um pouco mais o processo ao exemplificar o seguinte processo que vem a calear com o desenvolvimento deste trabalho. No exemplo, a estação de gerência da rede (NMS) envia um GetRequest para o agente solicitando nele o nome do

dispositivo. O agente devolve um PDU chamado GetResponse e a resposta contém o nome do roteador, “cisco”.

4.5.2. GetNextRequest

O PDU GetNextRequest é enviado do gerente até o agente para leitura do valor de uma variável. O valor lido é o valor do objeto especificado pelo ObjectId definido no PDU. Ele é usado, na maioria das vezes, para leitura de valores de entrada de uma tabela. Se o gerente não conhecer os índices das entradas, não poderá ler os objetos. Entretanto, pode usar o comando GetNextRequest e definir o ObjectId da tabela. Como a primeira entrada retornará o ObjectId imediatamente após o ObjectId da tabela, então o valor retornado será o valor da primeiro entrada. O gerente pode usar esse ObjectId para obter o valor do seguinte e assim por diante. (FOROUZAN, 2008, pág. 891).

4.5.3. GetBulkRequest

O PDU GetBulkRequest é enviado do gerente até o agente para permitir a leitura de uma grande quantidade de dados. Pode ser usado no lugar de vários PDU GetRequest e GetNextRequest. (FOROUZAN, 2008, pág. 892).

4.5.4. SetRequest

O PDU SetRequest é enviado do gerente até o agente para gravar (armazenar) um valor de uma variável. (FOROUZAN, 2008, pág. 892).

4.5.5. Response

O PDU Response é enviado de um agente até o gerente em resposta a um PDU GetRequest ou GetNextRequest. Contém os valores das variáveis solicitadas pelo gerente. (FOROUZAN, 2008, pág. 893).

4.5.6. Trap

Trap (também denominado SNMPv2 Trap para diferenciá-lo do PDU SNMPv1 Trap) é enviado do agente até o gerente para notificar um evento anormal. Por exemplo, se o agente for reiniciado, ele notifica o gerente informa o horário de reinicialização. (FOROUZAN, 2008, pág. 892).

4.5.7. InformRequest

O PDU InformRequest é enviado de um gerente até outro gerente remoto para obter o valor de algumas variáveis dos agentes sob o controle do gerente remoto. O gerente remoto responde com um PDU Response. (FOROUZAN, 2008, pág. 892).

4.5.8. Report

O PDU Report foi projetado para alguns tipos de erros entre agentes. Ainda não é utilizado. (FOROUZAN, 2008, pág. 892).

4.5.9. Formato

O formato do pacote para os oito PDUs SNMP é mostrado na figura de FOROUZAN, conforme ilustrado abaixo. Nela podemos perceber ainda que o PDU GetBulkRequest apresenta características diferenciadas em relação aos demais.

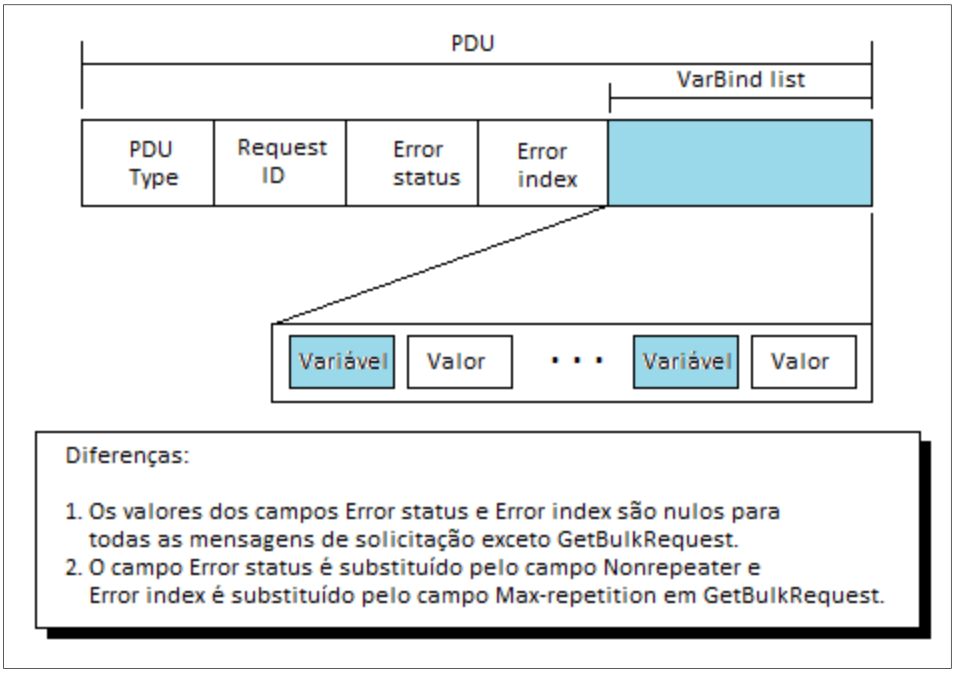

Figura 10. Formato do pacote PDU.
Fonte: FOROUZAN, 2008.

Por julgarmos este ponto importante para a compreensão do protocolo, cada um dos campos do PDU será listado no subitem a seguir juntamente com uma descrição sucinta de suas características.

4.5.9.1. PDU Type

Campo responsável pela definição do PDU. A tabela a seguir apresenta os tipos possíveis:

Dados	*Classe*	*Formato*	*Número*	*Tag Inteiro (Binário)*	*Tag Inteiro (Hexa)*
GetRequest	10	1	00000	**10100000**	**A0**
GetNextRequest	10	1	00001	**10100001**	**A1**
Response	10	1	00010	**10100010**	**A2**
SetRequest	10	1	00011	**10100011**	**A3**
GetBulkRequest	10	1	00101	**10100101**	**A5**
InformRequest	10	1	00110	**10100110**	**A6**
Trap (SNMPv2)	10	1	00111	**10100111**	**A7**
Report	10	1	01000	**10101000**	**A8**

Quadro 15. Tipos de dados do PDU.
Fonte: FOROUZAN, 2008, pág. 894

4.5.9.2. Request ID

Esse campo define um número de sequencia usado pelo gerente num PDU Request e repetido pelo agente em uma resposta. É usado para associar uma solicitação a uma resposta. (FOROUZAN, 2008, pág. 892).

4.5.9.3. Error status

Define um valor inteiro que é usado apenas nos PDUs Response para mostrar os tipos de erros notificados pelo agente. Seu valor é 0 nas PDUs Request. (FOROUZAN, 2008, pág. 893).

A tabela a seguir mostra os tipos de erros que podem ocorrer:

Estado	*Nome*	*Significado*
0	noError	Nenhum erro
1	tooBig	Resposta muito grande para caber em uma mensagem
2	noSuchName	A variável não existe
3	badValue	O valor a ser armazenado é inválido
4	readOnly	O valor não pode ser modificado
5	genErr	Outros erros

Quadro 16. Error Status do PDU.
Fonte: FOROUZAN, 2008, pág. 893

4.5.9.4. Nonrepeaters

Esse campo é usado apenas em PDUs GetBulkRequest e substitui o campo Error status, que é vazio nos PDUs Request. (FOROUZAN, 2008, pág. 893).

4.5.9.5. Error index

O campo Error index é um offset que informa ao gerente qual variável provocou o erro. (FOROUZAN, 2008, pág. 893).

4.5.9.6. Max-repetition

Esse campo também é usado apenas em PDUs GetBulkRequest e substitui o campo índice de erro, que é vazio nos PDUs Request. (FOROUZAN, 2008, pág. 893).

4.5.9.7. VarBin list

Trata-se de um conjunto de variáveis com seus valores correspondentes, que o gerente deseja ler ou gravar. Os valores são nulos em GetRequest e GetNextRequest. Em um PDU Trap, ele mostra as variáveis e valores relativos ao PDU específico. (FOROUZAN, 2008, pág. 893).

4.5.10. Mensagens

Uma mensagem SNMPv3 é constituída por quatro elementos: versão, cabeçalho, parâmetros de segurança e dados (que incluem o PDU codificado). (FOROUZAN, 2008, pág. 893).

> O cabeçalho contêm valores para a identificação das mensagens, tamanho máximo da mensagem (o tamanho máximo da resposta), flag da mensagem (um octeto cujo tipo de dados é OCTET STRING, em que cada bit define o tipo de segurança, como privacidade ou autenticação, ou outras informações) e um modelo de segurança de mensagens (definido o protocolo de segurança). Os dados estão contidos no PDU. Se forem criptografados, existem informações sobre o mecanismo de criptografia (o programa-gerente que a realizou) e o contexto da criptografia (o tipo) seguido pelo PDU criptografado. Se os dados não forem criptografados, formarão apenas o próprio PDU. Para definir o tipo de PDU, o SNMP usa um tag. A classe é sensível ao contexto (10), o formato é estruturado (1) e os números são 0,1,2,3,5,6,7 e 8. Note que o SNMPv1 definiu A4 para Traps que é obsoleto hoje em dia. (FOROUZAN, 2008, pág. 893).

4.5.11. Portas UDP

O SNMP usa serviços UDP em duas portas conhecidas, 161 e 162. A porta conhecida 161 é usada pelo servidor (agente) e a porta 162, pelo cliente (gerente). (FOROUZAN, 2008, pág. 895).

4.6. Segurança

A principal diferença entre o SNMPv3 e o SNMPv2 é a segurança reforçada. O SNMPv3 dispõe de dois tipos de segurança: geral e específica. O SNMPv3 pode utilizar mecanismos para autenticação de mensagens, privacidade e autorização do gerente. (FOROUZAN, 2008, pág. 897).

5. REMOTE MONITORNG - RMON

A especificação de monitoração remota (Remote Monitoring – RMON) pode ser considerada uma extensão do padrão SNMP. Ela foi definida no início dos anos 90 como um meio de monitorar dispositivos remotos. Ela também conta com a estrutura de informações da MIB e SMI. Sua finalidade é enviar informações de rede agrupadas em nove elementos de monitoração principais. (BARRET; KING, 2010, pág. 273).

- Grupo de alarme
- Grupo de evento
- Grupo de filtro
- Grupo de histórico
- Grupo de host
- Grupo de HostTopN
- Grupo de matriz
- Grupo de captura de pacote
- Grupo de estatísticas

Segundo Barret & King, a Cisco Systems inclui funcionalidade SNMP e RMON em seu software. O recurso será investigado ao longo do desenvolvimento do projeto.

6. SOFTWARES CLIENTES SNMP

Uma NMS utiliza um software para executar as aplicações que monitoram e controlam os dispositivos gerenciados. Este software é conhecido como “gerente”. As estações de gerência geralmente são centralizadas.

Como opção de software gerente de rede, foram analisados e apresentados três deles, os quais foram testados e apresentaram bom desempenho: OpManager, PRTG e AdRem NetCrunch.

6.1. Manage Engine OpManager

O ManageEngine OpManager é um software de monitoramento de rede que combina o monitoramento da Wan, servidores e aplicações, e pode ser integrado com o Help Desk, com gerenciamento de ativos e ainda com o analisador de tráfego de rede. O OpManager automatiza uma série de tarefas de monitoramento e remove a complexidade associada a essas tarefas.

Abaixo as telas do OpManager que merecem destaque:

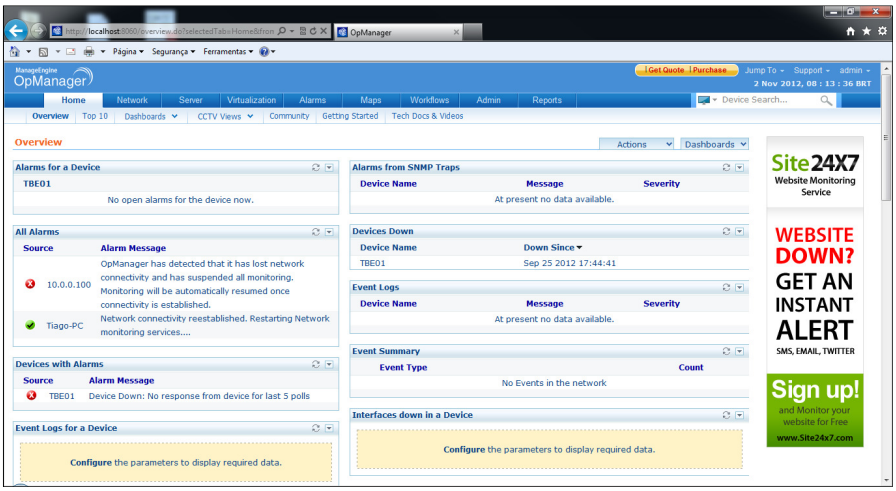

Figura 12. Tela Home
Fonte: Software OpManager

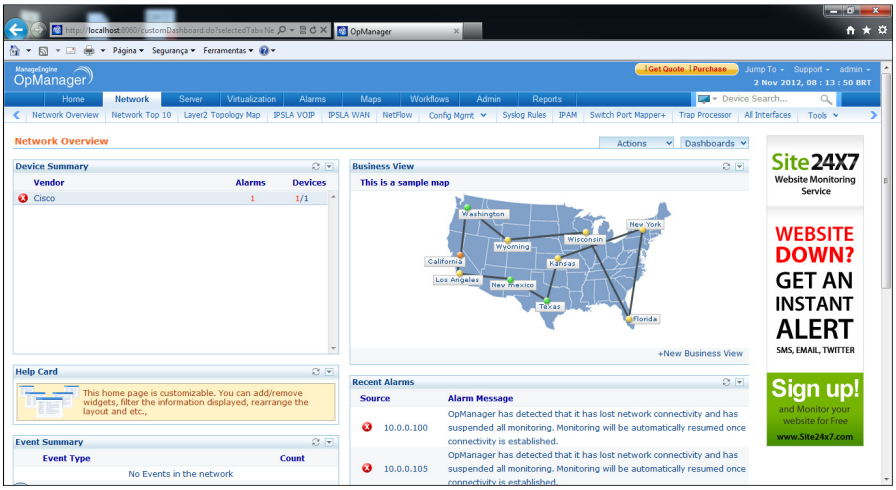

Figura 11. Tela Network Overview
Fonte: Software OpManager

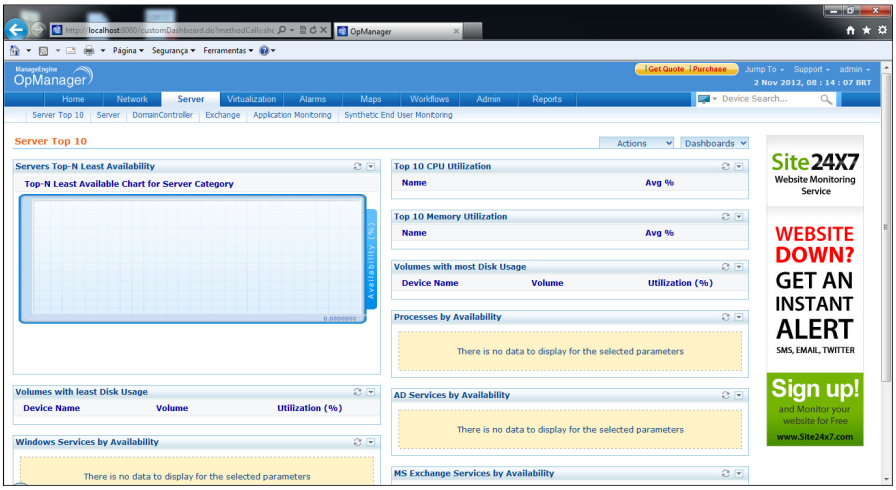

Figura 13. Tela Server
Fonte: Software OpManager

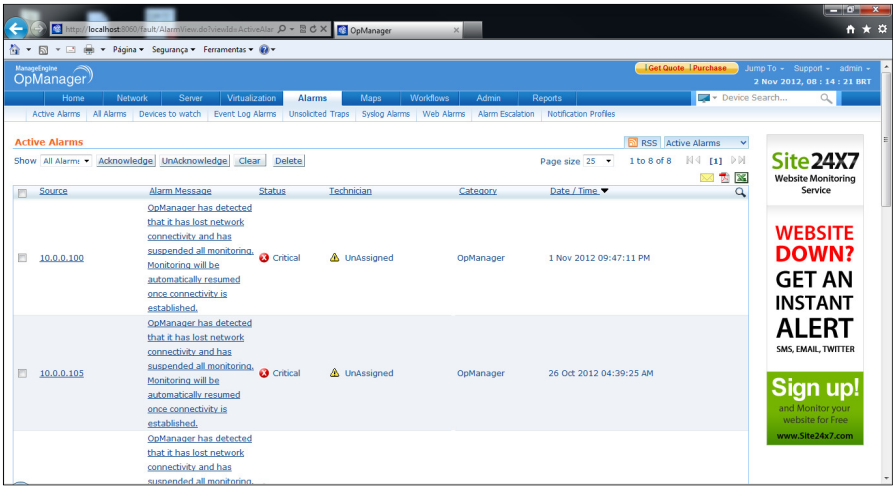

Figura 14. Tela Alarms
Fonte: Software OpManager

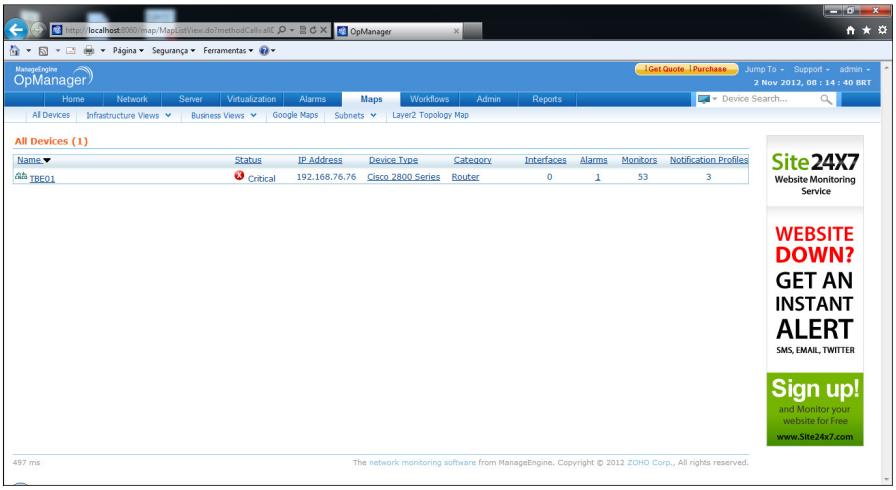

Figura 15. Tela Maps
Fonte: Software OpManager

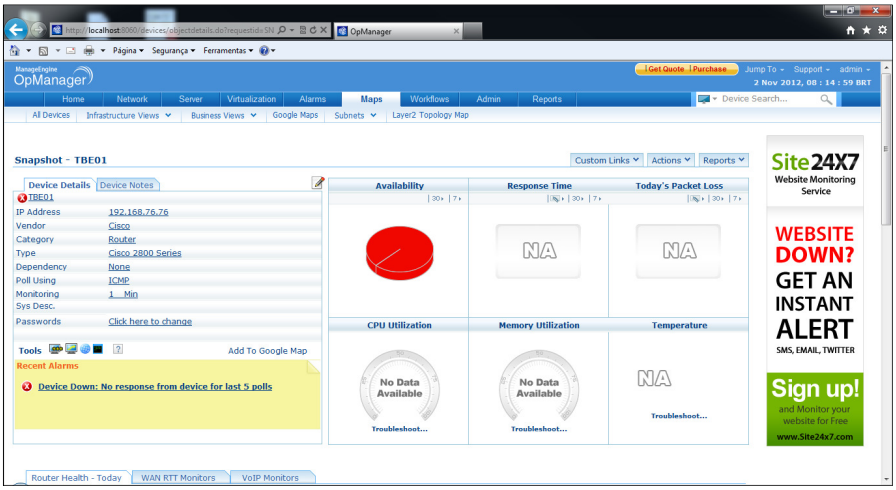

Figura 16. Tela Snapshot – TBE01
Fonte: Software OpManager

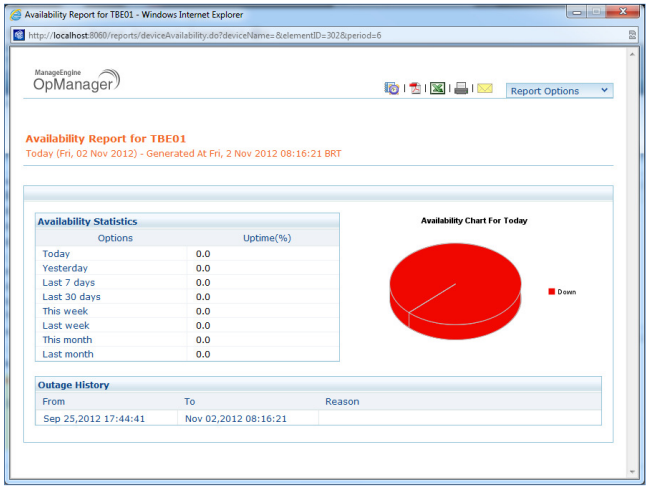

Figura 17. Tela Report de disponibilidade
Fonte: Software OpManager

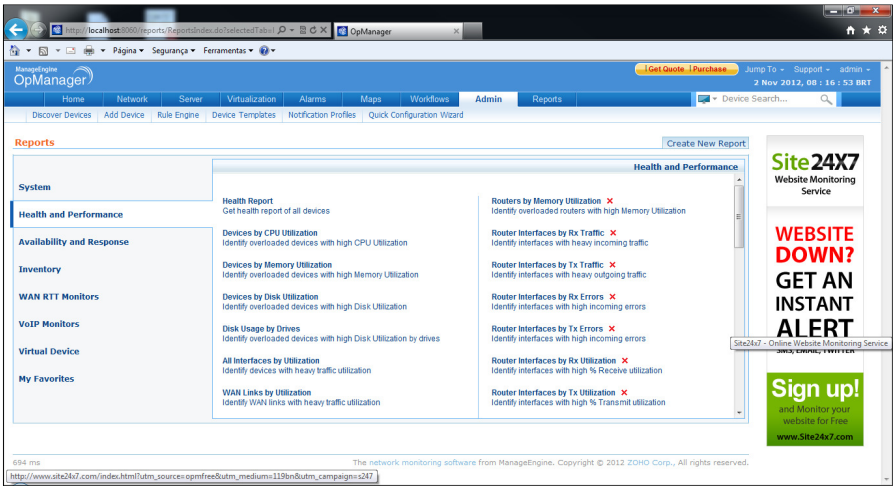

Figura 18. Tela Admin
Fonte: Software OpManager

6.2. PRTG Network Monitor

Semelhante ao OpManager, o **PRTG** roda no sistema Windows dentro da própria rede coletando estatísticas das máquinas, softwares e dispositivos.

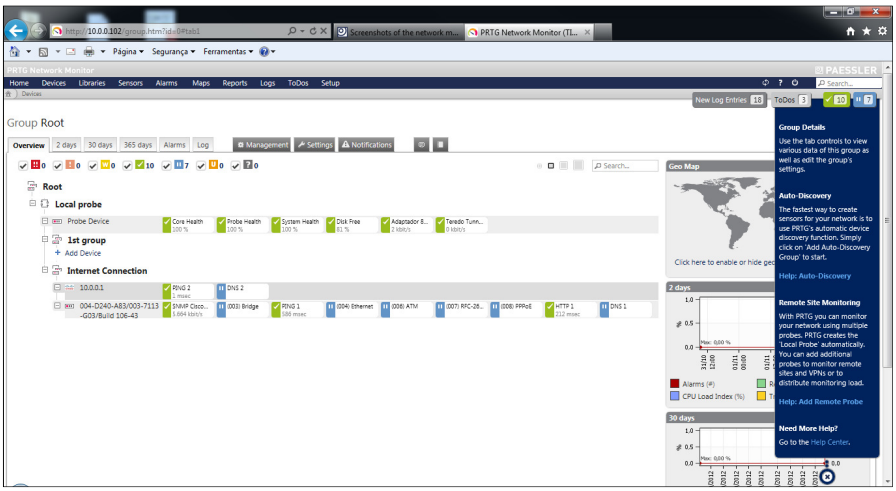

Figura 19. Tela Devices
Fonte: Software PRTG

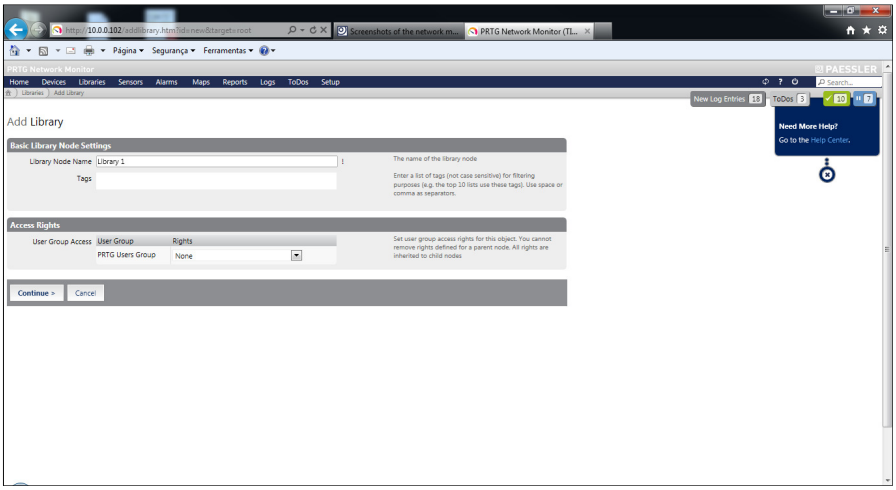

Figura 20. Tela Libraries
Fonte: Software PRTG

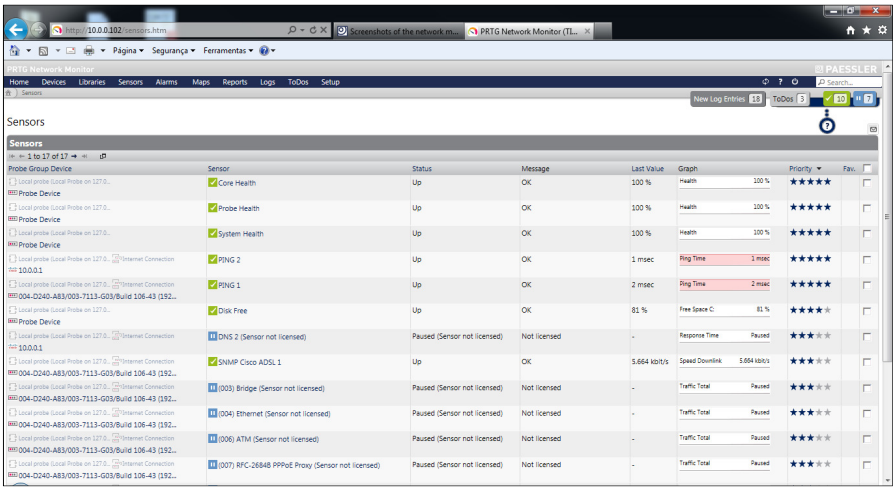

Figura 21. Tela Sensores
Fonte: Software PRTG

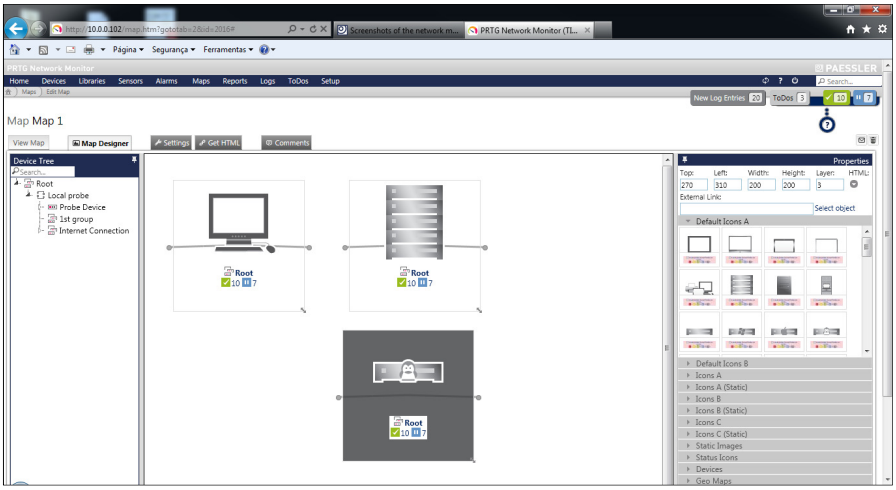

Figura 22. Tela Mapas
Fonte: Software PRTG

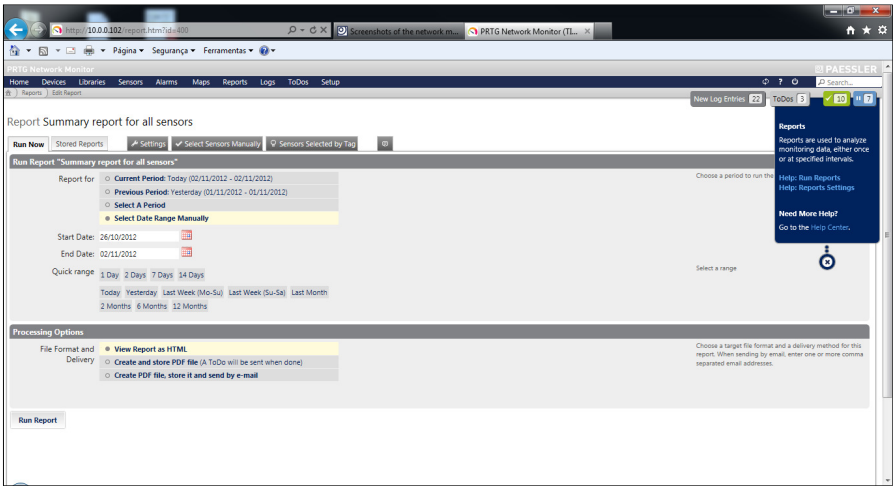

Figura 23. Tela Reports
Fonte: Software PRTG

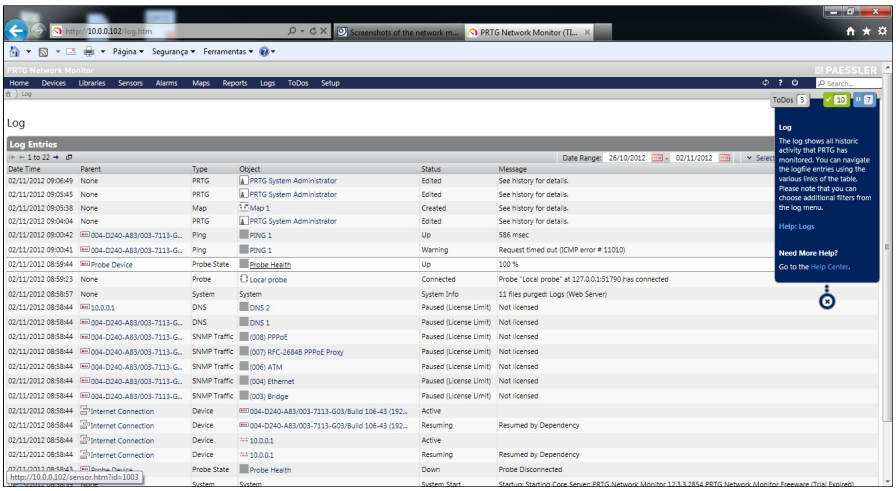

Figura 24. Tela Logs
Fonte: Software PRTG

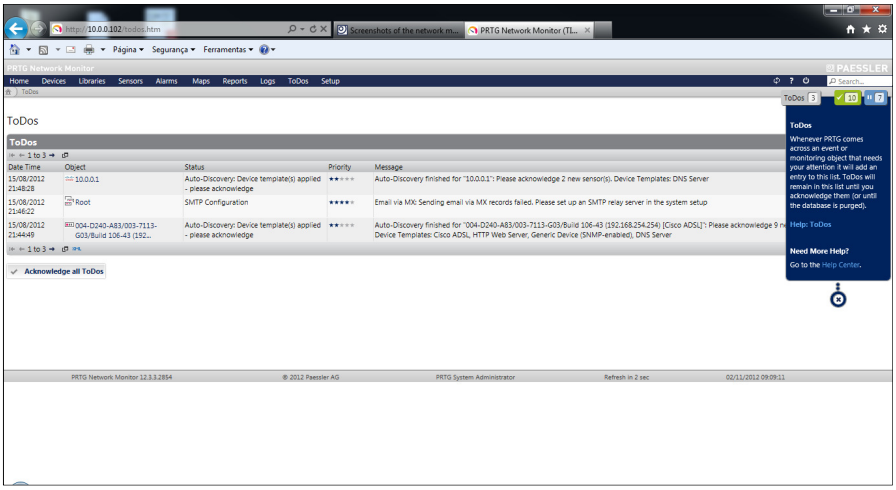

Figura 25. Tela ToDocs
Fonte: Software PRTG

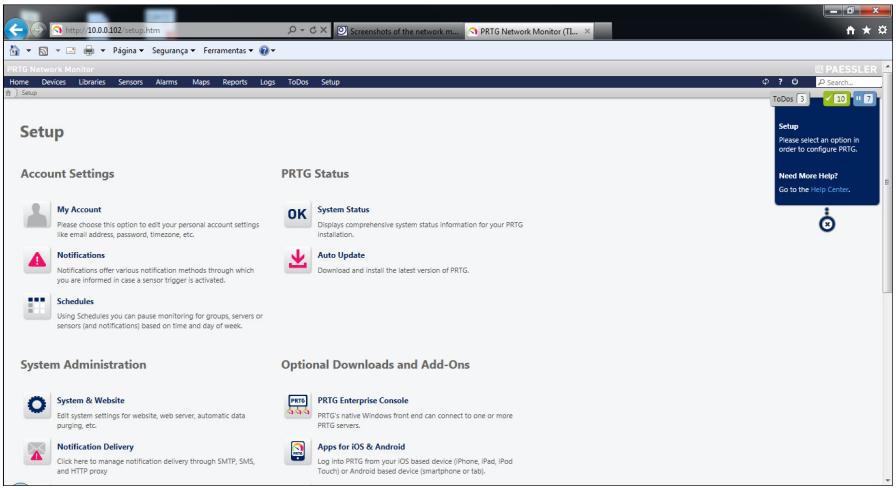

Figura 26. Tela Setup
Fonte: Software PRTG

6.3. AdRem NetCrunch

O AdRem NetCrunch possui características semelhantes aos anteriormente citados, no entanto, pode-se destacar: a realização de descoberta automática e classificação dos recursos da rede, visualização dinâmica da topologia física e lógica rede por meio de mapas gráficos, a coleta de eventos e envio de alertas quando há problemas, o monitoramento de desempenho, a análise de tendências em longo prazo, o acesso remoto e por fim o Inventário de Hardware e software.

A seguir quatro telas importantes do Console de Administração do AdRem NetCrunch:

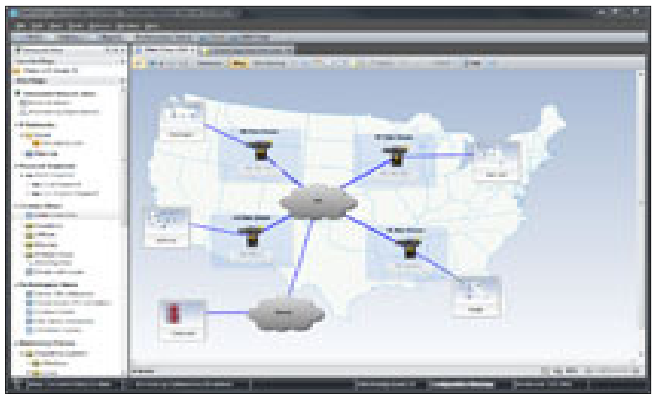

Figura 27. Tela Top Network view
Fonte: Software NetCrunch

Figura 28. Tela Real Time View
Fonte: Software NetCrunch

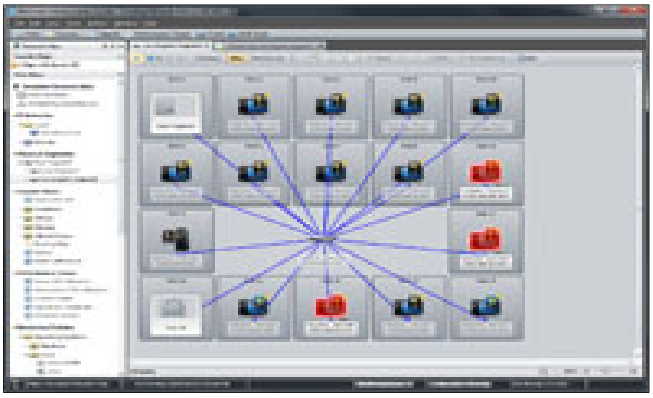

Figura 29. Tela Physical Segments View
Fonte: Software NetCrunch

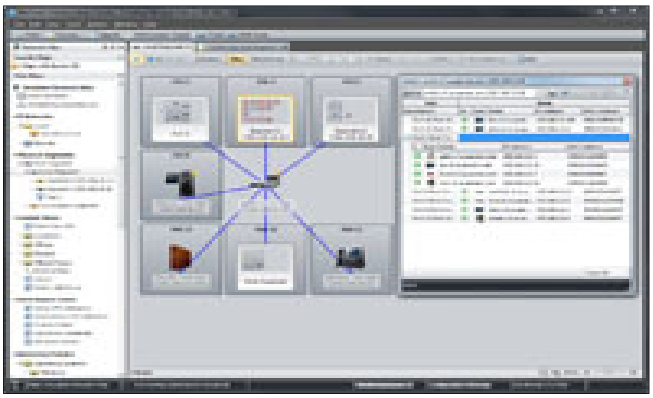

Figura 30. Tela Switch Port Mapping
Fonte: Software NetCrunch

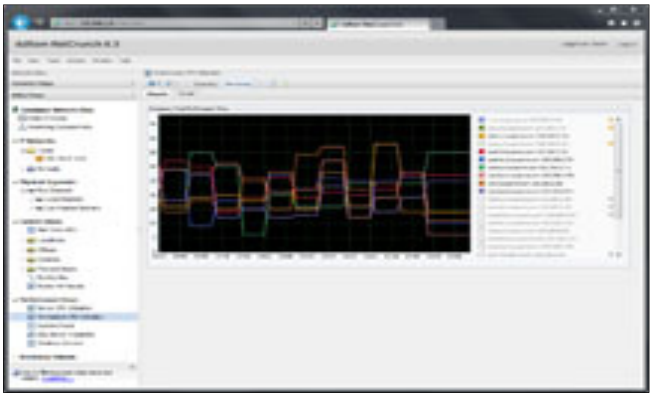

Figura 31. Tela Tempos do Processador
Fonte: Software NetCrunch

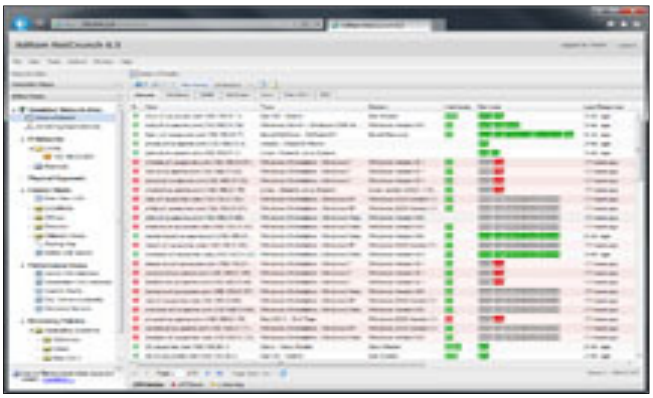

Figura 32. Tela Detalhes de todos os nós
Fonte: Software NetCrunch

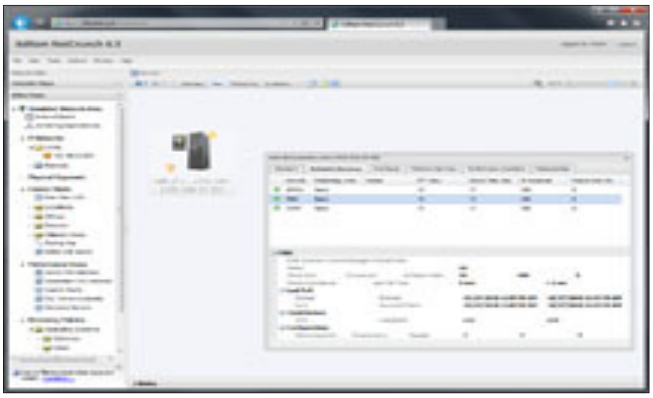

Figura 33. Tela Status do nó
Fonte: Software NetCrunch

III – DESCRIÇÃO DO ESTUDO DE CASO

1. INTRODUÇÃO

A proposta do trabalho é demonstrar a utilização do protocolo SNMP, para assim garantir o monitoramento e o desempenho dos canais de dados e voz e comprovar o atendimento aos requisitos dos procedimentos de rede.

O Desenvolvimento do trabalho consistiu em implementar a estrutura física, configuração do canal de dados/voz, aplicação do SNMP de acordo com a norma dos RFCs, desenvolvimento de plano de testes a serem utilizados pela empresa TBE-SUL e testes efetivos de desempenho.

1.1. A empresa TBE

Tendo suas atividades iniciadas em 2000, a TBE caracteriza-se hoje como um conjunto de nove concessionárias de transmissão de energia elétrica, atuando nos estados do Pará, Maranhão, Santa Catarina, Mato Grosso e Minas Gerais com instalações que totalizam 3140 km de linhas de transmissão e 27 Subestações nas tensões primárias de 230 e 500 quilovolts. As concessões foram objeto de leilão público promovido pela União através da ANEEL – Agência Nacional de Energia Elétrica, sob o novo modelo adotado pelo Setor Elétrico a partir de 1999.

A entrada em operação comercial de cada empresa ocorreu sequencialmente:

- Empresa Catarinense de Transmissão de Energia – Março de 2002
- Empresa Paraense de Transmissão de Energia – Agosto de 2002
- Empresa Amazonense de Transmissão de Energia – Março de 2003
- Empresa Regional de Transmissão de Energia – Setembro de 2004
- Empresa Norte de Transmissão de Energia – Fevereiro de 2005
- Sistema de Transmissão Catarinense – Novembro de 2007
- LUMITRANS Companhia Transmissora de Energia Elétrica – outubro de 2007
- Empresa Brasileira de Transmissão de Energia – julho de 2011
- Empresa Santos Dumont de Energia – junho/2012

1.2. Gerência Regional Sul

A Gerência Regional Sul é responsável pela operação, manutenção e administração das três companhias localizadas na região Sul do país e pela operação de outras duas sendo uma na Região Centro-Oeste e outra na Região Norte. Ligado à gerência Sul está ainda o Centro de Operação Nacional do grupo, o COT-TBE-SUL.

1.3. Centro de Operação da Transmissão Sul, COT-TBE-SUL

O Centro de Operação da Transmissão, COT-TBE-SUL fica localizado em Lages-SC e é responsável por coordenar, supervisionar e controlar em tempo real todos os processos desenvolvidos nas subestações e nas linhas de transmissão, integrando estas instalações aos demais agentes do sistema elétrico.

A operação em tempo real na TBE está centralizada na região Sul, porém é responsável pela operação de instalações distribuídas por várias regiões do Brasil. Este setor possui regras e procedimentos rígidos que são determinados pelo Operador Nacional do Sistema Elétrico e devem ser seguidos para que a totalidade do sistema elétrico Brasileiro permaneça íntegro. Parte destas normas são requisitos técnicos que devem ser atendidos pelas equipes de manutenção.

1.4. Setor de Engenharia e Manutenção

A equipe de engenharia fica situada no escritório central do Grupo TBE localizado em São Paulo Capital, enquanto que as equipes de manutenção ficam descentralizadas sob a gerência das respectivas Regionais Sul, Norte e Centro-Oeste. As equipes de engenharia e manutenção na TBE atuam em constante interação a fim de prover soluções, planejamentos e melhorias que venham a trazer benefícios ao sistema elétrico.

Atuando em conjunto, estas duas áreas da empresa funcionam ainda como integradores de tecnologias realizando constantes adequações das instalações do Grupo aos requisitos e normas do Operador Nacional do Sistema Elétrico, da Agência Nacional de Energia Elétrica e demais empresas que compõem o setor no Brasil.

1.5. Infraestrutura de Telecomunicações

A Infraestrutura de Telecomunicações é uma das quatro áreas de responsabilidade da equipe de manutenção de sistemas sob a gerência e coordenação da Gerência Regional Sul. Pode-se considerar ainda neste grupo de manutenção as áreas de Proteção do Sistema Elétrico, Sistemas de Supervisão e Controle e Suporte a TI.

2. OPERADOR NACIONAL DO SISTEMA ELÉTRICO

> O Operador Nacional do Sistema Elétrico (ONS) é o órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional (SIN), sob a fiscalização e regulação da Agência Nacional de Energia Elétrica (Aneel).
> Para o exercício de suas atribuições legais e o cumprimento de sua missão institucional, o ONS desenvolve uma série de estudos e ações a serem exercidas sobre o sistema e seus agentes para manejar o estoque de energia de forma a garantir a segurança do suprimento contínuo em todo o País. O Operador Nacional é constituído por membros associados e membros participantes, constituídos por empresas de geração, transmissão, distribuição e consumidores livres de grande porte. Também participam importadores e exportadores de energia, além do Ministério de Minas e Energia (MME).
> O ONS é uma pessoa jurídica de direito privado, sob a forma de associação civil, sem fins lucrativos, criado em 26 de agosto de 1998, pela Lei nº 9.648/98, com as alterações introduzidas pela Lei nº 10.848/04 e regulamentado pelo Decreto nº 5.081/04.

2.1. Centro de Operação do Sistema Regional Sul

Para gerenciar o Sistema Interligado Nacional, o ONS dispõe de cinco Centros de Operação, os quais são responsáveis pela coordenação, supervisão e controle de toda a rede de operação do SIN. Estes centros ficam estrategicamente dispostos da seguinte forma: o Centro Nacional de Operação do Sistema (CNOS), em Brasília (DF); o Centro Regional de Operação Norte/Centro-Oeste (COSR-NCO), também em Brasília; o Centro Regional de Operação Nordeste (COSR-NE), em Recife (PE); o Centro Regional de Operação Sudeste (COSR-SE),

no Rio de Janeiro (RJ); e o Centro Regional de Operação Sul (COSR-S), em Florianópolis (SC).

O Centro Nacional de Operação reporta-se aos Centros Regionais do ONS, que por sua vez se reportam aos centros de operação dos Agentes, e estes com as instalações de geração, transmissão e distribuição.

As Empresas da TBE estão na posição de Agente do Sistema Elétrico Brasileiro, sendo que cada concessão se reporta ao Centro de Operação do ONS responsável pelo gerenciamento da respectiva área em que está instalada a Empresa. Desta forma, as empresas instaladas na região Sul do país, reportam-se ao Centro de Operação do Sistema Regional Sul de Florianópolis e o fazem também por meio de canais de voz e dados de alto desempenho e com redundância de rotas físicas.

A Operação assistida do Sistema elétrico por parte dos Centros de Controle do ONS e dos Agentes se dá de forma ininterrupta durante as 24 horas do dia e 365 dias por ano.

2.2. Importância no cenário Nacional

Por diversos fatores, o ONS é hoje a referência para as empresas de geração, transmissão e distribuição de energia no Brasil. Cada centro regional dispõe de uma área Normativa, uma área de Operação e uma área de Infraestrutura as quais orientam e interagem com os Agentes a fim de cumprir as regras definidas em procedimentos específicos do setor.

Hierarquicamente, o ONS se reporta a Agência Nacional de Energia Elétrica, sendo este último, um órgão governamental inserido no contexto das agências reguladoras federais, caracterizada como autarquia com regime jurídico especial e vinculada ao Ministério de Minas e Energia.

> A ANEEL iniciou suas atividades em dezembro de 1997, tendo como principais atribuições:
> - Regular a produção, transmissão, distribuição e comercialização de energia elétrica;
> - Fiscalizar, diretamente ou mediante convênios com órgãos estaduais, as concessões, as permissões e os serviços de energia elétrica;
> - Implementar as políticas e diretrizes do governo federal relativas à exploração da energia elétrica e ao aproveitamento dos potenciais hidráulicos;
> - Estabelecer tarifas;
> - Mediar, na esfera administrativa, os conflitos entre os agentes e entre esses agentes e os consumidores;

- Por delegação do governo federal, promover as atividades relativas às outorgas de concessão, permissão e autorização de empreendimentos e serviços de energia elétrica.
  (ANEEL, [http://www.aneel.gov.br], Disponível em 02 de Novembro de 2012).

2.3. Os procedimentos de Rede

São documentos de caráter normativo sendo elaborados pelo ONS, com participação dos agentes, e aprovados pela ANEEL, que definem os procedimentos e os requisitos necessários à realização das atividades de planejamento da operação eletroenergética, administração da transmissão, programação e operação em tempo real no âmbito do SIN. (ONS, [http://www.ons.org.br], Disponível em 02 de Novembro de 2012).

As regras e diretrizes constantes nos procedimentos de rede devem ser plenamente atendidas pelas empresas, pois é o cumprimento destas que irá garantir a segurança das instalações, das pessoas e a continuidade da distribuição energética ao país.

3. CENÁRIO DE IMPLEMENTAÇÂO E TESTES

As empresas da TBE na região Sul foram concebidas com a utilização de canais de comunicação de dados seriais e canais de voz analógicos dedicados entre suas instalações e o COSR-S. O objetivo dos canais de dados é para que o Centro de Operação do ONS possa visualizar o status das condições elétricas das instalações do Agente, enquanto que os canais de voz do tipo '*Hot-Line*' são para manter contato único e exclusivo entre as áreas operativas de forma rápida e eficiente.

Por exigência constante nos procedimentos de rede, o Agente possui a responsabilidade de implantar e manter dois canais para cada aplicação de dados e dois canais dedicados de voz, sendo que estes canais devem ser disponibilizados por meios físicos distintos para garantir continuidade dos serviços mesmo sob condições adversas.

O estabelecimento de um link serial para transmissão de dados entre dois concentradores de dados fisicamente distantes apesar de ser uma forma bastante segura no aspecto de isolamento entre os sistemas, é ao mesmo tempo pouco eficiente, uma vez que se limita ao uso de protocolos em sua maioria descontinuados ou caindo em desuso e que oferecem

poucos recursos de gerenciamento e acesso. O mesmo pode-se dizer a respeito da telefonia convencional ou mais especificamente da transmissão de voz a longas distâncias por meio de canais analógicos. Existe hoje, no mercado de telefonia mundial um processo irreversível de conversão de canais de voz do meio puramente analógico para o meio digital. Uma vez digitalizada, a voz pode ser encapsulada e transmitida por meio do mesmo canal em que são transmitidos os dados, quem passa então a gerenciar o que é voz e o que é dado são os protocolos de rede.

Outro fator desfavorável aos links de dados seriais e fonia analógica é a impossibilidade da utilização de ferramentas automatizadas de gerenciamento destes serviços, ao passo que torná-los digitais abre espaço para que sejam aplicadas as ferramentas de gerenciamento já aplicadas às redes que operam sobre tecnologia IP.

A necessidade de monitorar o desempenho e a disponibilidade dos canais de voz e dados fez com que em meados de 2012 a ANEEL e o ONS estabelecessem novas regras determinando prazo para que os Agentes adequassem os serviços. Pelos fatores técnicos positivos já expostos somados ao crescente aumento de confiabilidade dos serviços sobre tecnologia IP e consequente redução de custos. A TBE, por sua vez, optou por realizar a adequação solicitada através da instalação de roteadores modulares capazes de fornecer os serviços desejados.

3.1. O Monitoramento dos Processos

> Apesar da tecnologia básica de Internet parecer não mudar, novas aplicações continuam a emergir e fornecer experiências aprimoradas para o interesse dos usuários. O mundo dos negócios utiliza sistemas de ponta em teleconferência para reduzir os custos. Sensores de rede, mapas e sistemas de navegação habilitam desenvolvimento de monitoramento, segurança e facilidade de tráfego. (COMER, 2008, pág. 24, tradução nossa).

O SNMP, uma tecnologia que nasceu ainda nos anos 80 e que é hoje uma solução sólida para este fim, foi a escolhida pelo ONS para atuar no monitoramento dos processos básicos que contribuem e dão origem aos links de voz e dados. O ONS optou pela utilização do software OpManager para rodar em sua NMS, e assim gerenciar os ativos de rede dos Agentes

Em um primeiro momento, a TBE utilizou também o OpManager (versão limitada) para rodar em sua NMS, e assim também gerenciar os mesmos ativos, porém, este ainda não foi ratificado como sendo o software final para gerenciar a rede.

Os processos que a equipe técnica precisa verificar a fim de manter os sistemas de supervisão e controle operando de forma eficiente, vão muito além do simples gerenciamento dos ativos próprios do seu parque de rede. Eles incluem também alguns processos-chave que rodam em servidores Windows e Linux, multiplexadores, além dos equipamentos de rede pertencentes às Operadoras de Telecom que prestam serviços complementares.

3.2. O gerenciamento de Telecom na TBE

A infraestrutura básica que permite a interconexão física dos equipamentos de rede como os roteadores é comumente chamada pelas operadoras e proprietários de 'Infraestrutura de *Telecom*'. A infra da TBE é composta em sua maioria por multiplexadores de plataforma multisserviço do fabricante Datacom. Estes dispositivos formam uma rede de equipamentos de hierarquia digital plessiócrona, ou simplesmente PDH (Plesiochronous Digital Hierarchy). Estes multiplexadores são flexíveis e permitem tanto a interconexão de meios físicos ópticos como elétricos dos mais diversos padrões.

O sistema de Telecom da TBE é gerenciado remotamente por meio do software DmView da Datacom o qual faz uso do protocolo SNMP para ler e escrever informações nos equipamentos. O tipo de gerência é denominado *'Gerência In-Band'*, pois utiliza uma pequena parte da banda de dados para acesso remoto ao equipamento.

O padrão de interface elétrica para conexão do multiplexador ao roteador é serial do tipo V.35 na extremidade do multiplexador e padrão smart serial na conexão do lado do roteador.

4. APLICAÇÃO DO ESTUDO DE CASO REFERENTE AO MONITORAMENTO E GRERENCIAMENTO DO CANAL DE DADOS E VOZ COM USO DO SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Este trabalho possui grande importância pelo contexto no qual está inserido. Ao final ele deverá agregar valores específicos de ordem técnica, prática e teórica às áreas da empresa as

quais estiveram de alguma forma envolvidas no processo, apresentando-se como um estudo que abre caminho para incentivar à busca pela pesquisa e pelo conhecimento dentro de uma instituição privada.

O legado não pode ser mensurado a partir do momento que inclui fatores abstratos como a quebra de paradigmas, a qual demonstra que interesses econômicos capitalistas e interesses acadêmicos em prol da difusão do conhecimento social podem caminhar em uma mesma direção. Neste caso, ouso dizer ainda que a percepção, de que, o mercado privado pode ser melhor estruturado e mais forte quando acredita e investe no crescimento da sociedade que lhe cerca se tornou uma verdade presente. A utilização da estrutura física de laboratórios e de equipamentos da TBE-SUL foi fundamental para o êxito da pesquisa, pois, propiciou à aplicação prática que fundamentou o trabalho.

4.1. Implantação da Infraestrutura Física

Cada extremidade do link da rota 02 pertencente à TBE foi estruturada sobre um multiplexador multisserviço, sendo, um Datacom CPU64 na localidade de Lages e um Datacom CPU32 na localidade de Florianópolis, ambos pertencentes à estrutura de Telecom da TBE.

As extremidades do link referente à rota 01 o qual pertence à operadora de Telecom contratada operam da mesma forma sobre multiplexadores multisserviço modelo CPU64 da Datacom. O gerenciamento deste sistema é realizado pela operadora de Telecom.

O caminho que interliga os multiplexadores da TBE apresenta forma mais complexa e por não ser tema foco do trabalho, será aqui representado somente por uma nuvem tanto para o caso da operadora contratada como para o caso da estrutura da TBE.

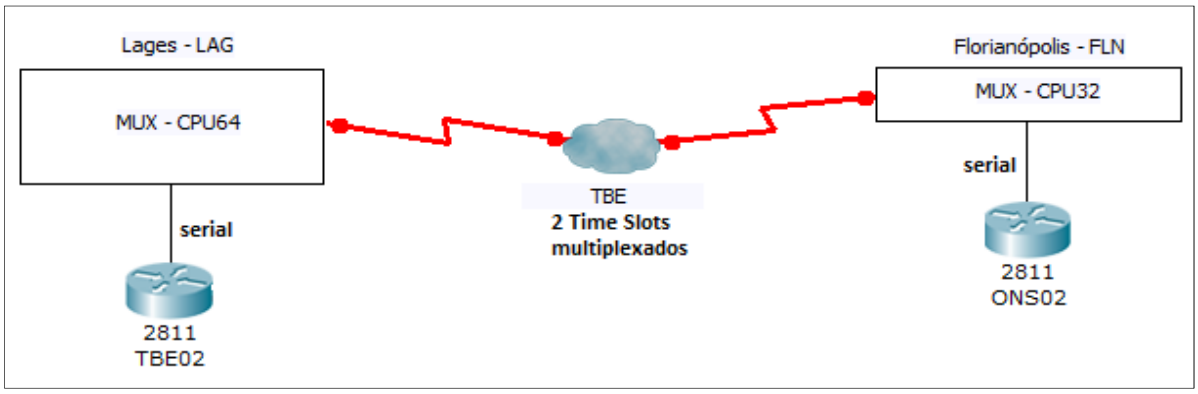

Figura 34. Topologia da rota 02.
Fonte: próprio autor.

Figura 35. Topologia da rota 01.
Fonte: próprio autor.

Diferentemente da infraestrutura da TBE a qual é composta por multiplexação PDH pura entre os equipamentos finais, a infraestrutura da operadora para além-fronteiras dos multiplexadores ópticos (os quais fornecem a ligação física até o multiplexador multisserviço) é desconhecida para a TBE, no entanto, estes dados não são relevantes para a aplicação final desde que não interfiram na qualidade do serviço contratado.

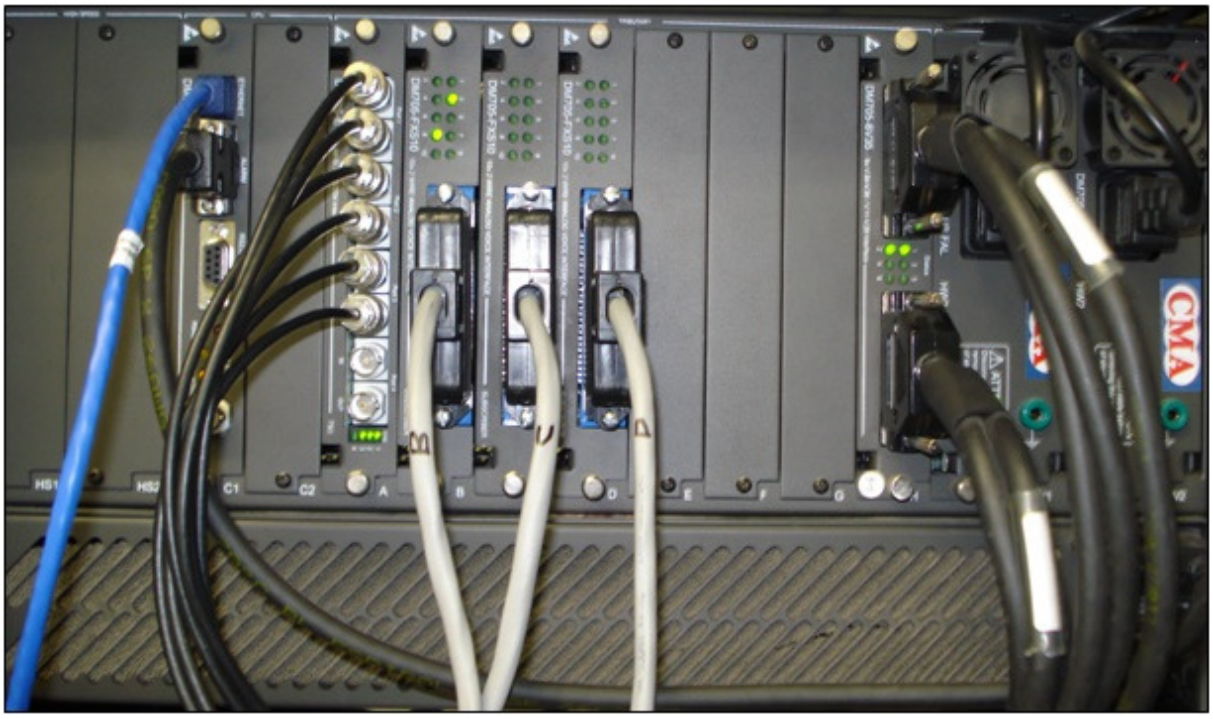

Figura 36. Multiplexador de Telecom da TBE.
Fonte: próprio autor.

Figura 37. Multiplexador de Telecom da Operadora.
Fonte: próprio autor.

Conforme verificado anteriormente, para a conexão entre multiplexador e roteador é utilizado o padrão serial V35. O multiplexador pode gerenciar placas de seis unidades seriais a qual é conhecida como 6V35, ou placas com duas unidades seriais que é conhecida como V35Dual. Na imagem a seguir o detalhe da conexão com o MUX.

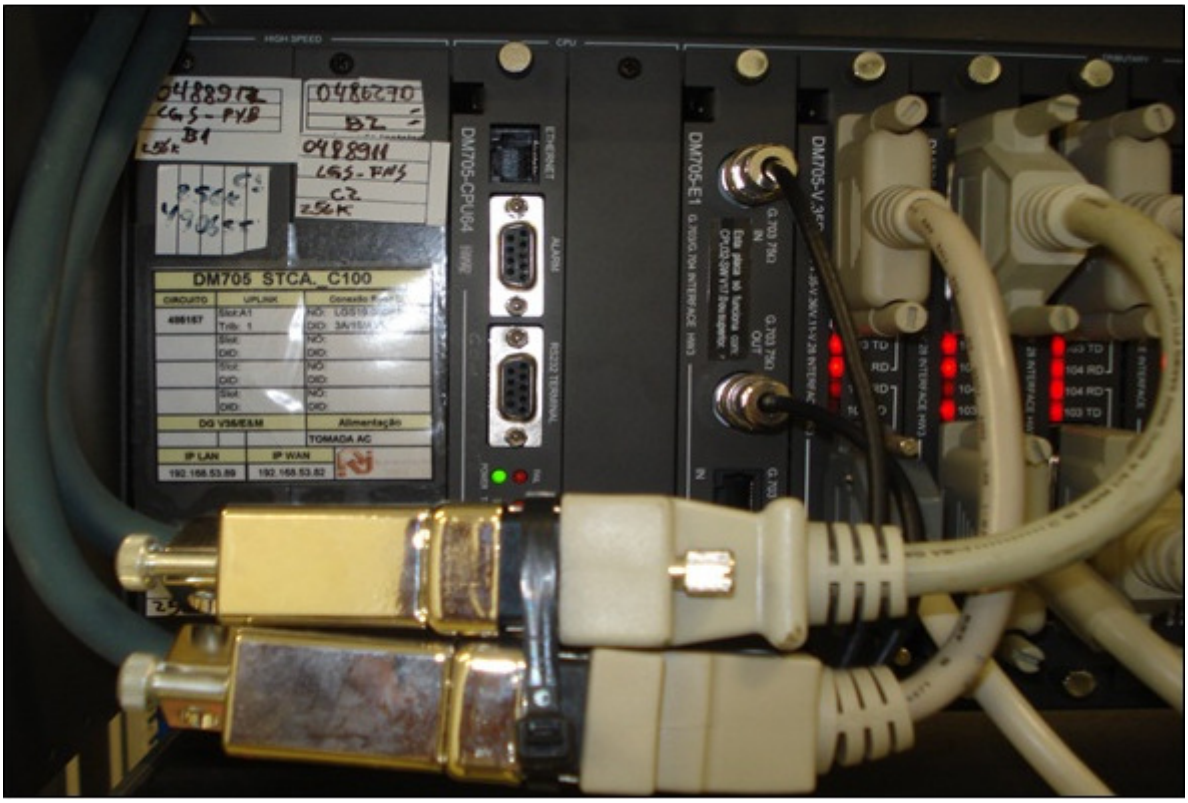

Figura 38. Multiplexador da Operadora – Detalhe da conexão serial.
Fonte: próprio autor.

A instalação de cada roteador utiliza apenas uma interface serial para interconexão com o multiplex. Sob os multiplexadores, foram implementados os roteadores da marca Cisco 2800 Series, objeto físico inicial do link. Cada unidade possui:

- Fonte automática 90 ~ 240Vac;
- Módulo de voz VIC-2FXS;
- Módulo HWIC-1T;

A seguir é apresentada a visualização frontal geral do hardware do roteador a qual contêm todas as interfaces acima mencionadas:

Figura 39. Par de roteadores em laboratório (sob teste).
Fonte: próprio autor.

As duas formas utilizadas para acesso ao equipamento foram “Console” e “Telnet”. A porta console utiliza tecnologia serial e fica localizada na parte frontal do hardware sendo acessível por meio de um conector M8V comumente chamado como RJ-45. Ela foi utilizada somente para o primeiro acesso o qual se faz necessário para a realização da configuração inicial do equipamento. O software para esta tarefa pode ser qualquer emulador de terminal, porém, neste caso utilizamos o ‘*Windows Hyper Terminal’* ajustado para as configurações abaixo listadas:

- Taxa de Transmissão: 9600bps
- Bits de Dados: 8
- Paridade: Nenhuma
- Bit de Parada: 1
- Controle de Fluxo: Nenhum

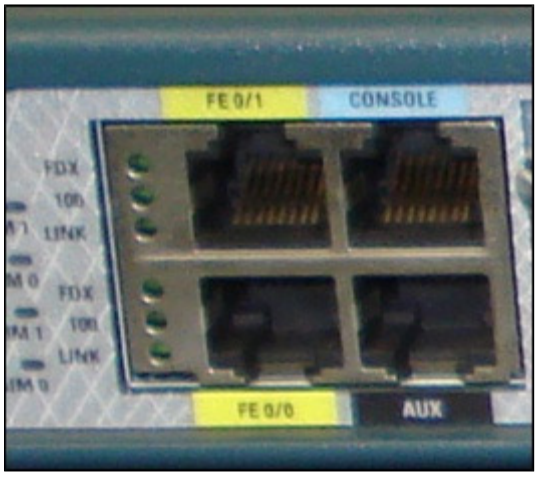

Figura 40. Interface Console (conexão superior direita).
Fonte: próprio autor.

A maior parte dos testes foram realizados em ambiente de laboratório nas instalações da TBE. Nesta etapa procurou-se replicar a condição de operação que o conjunto assumiria na sua instalação definitiva no campo em nível de roteamento, protocolo de redundância, links de voz, gerenciamento snmp, acesso remoto e firewall.

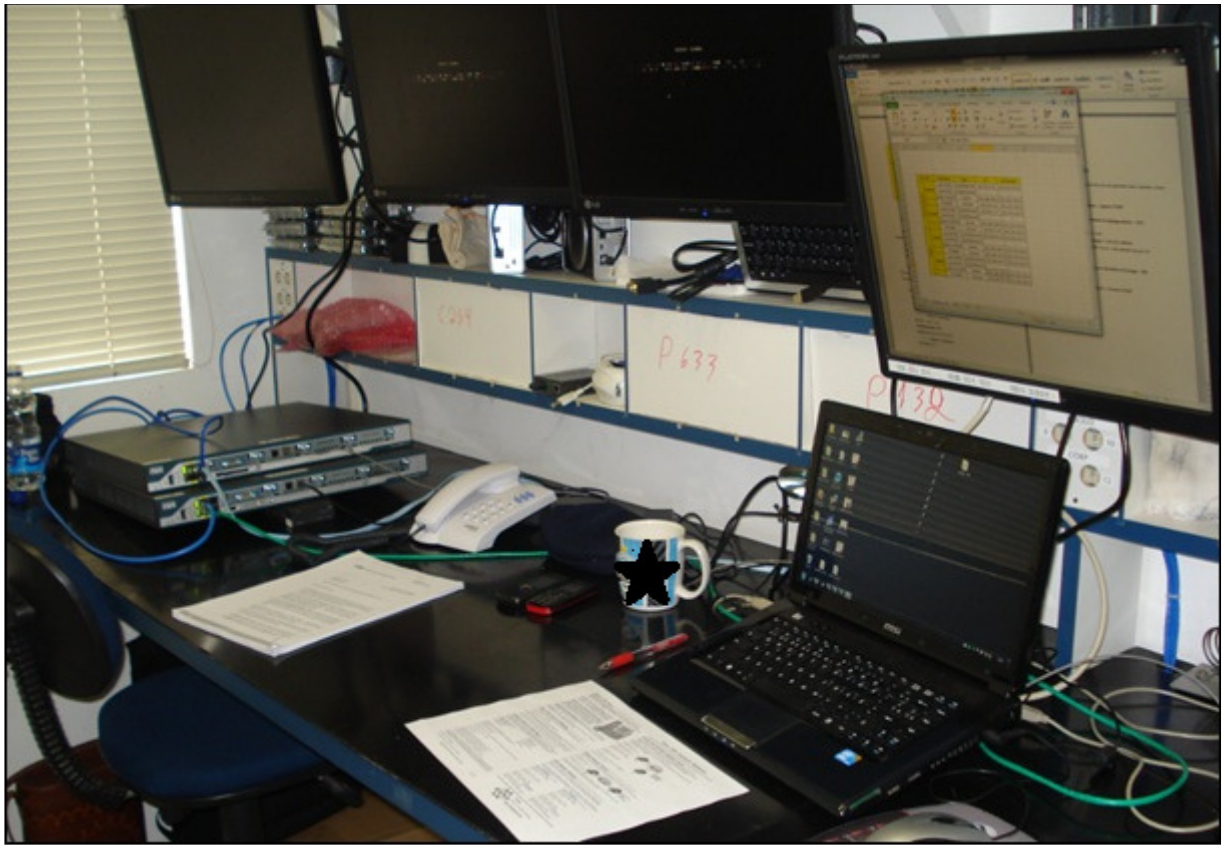
Figura 41. Roteadores em ambiente de laboratório (sob teste).
Fonte: próprio autor.

Figura 42. Roteadores em ambiente de laboratório (sob teste).
Fonte: próprio autor.

Figura 43. Roteador em instalação definitiva no campo.
Fonte: próprio autor.

4.2. Implantação da Infraestrutura Lógica

As configurações dos roteadores da rede foram realizadas por meio de linha de comando, também chamadas por Command Line Interface - CLI. O Cisco Internetwork Operating System (Cisco IOS) é o software responsável por tratar todas as informações do núcleo dos equipamentos de rede mais modernos.

A figura 45 mostrada abaixo apresenta a topologia simples da rede já contendo os nomes dos roteadores (hostname), as localidades onde serão instalados, o proprietário do meio físico da interligação e a largura da banda dos links.

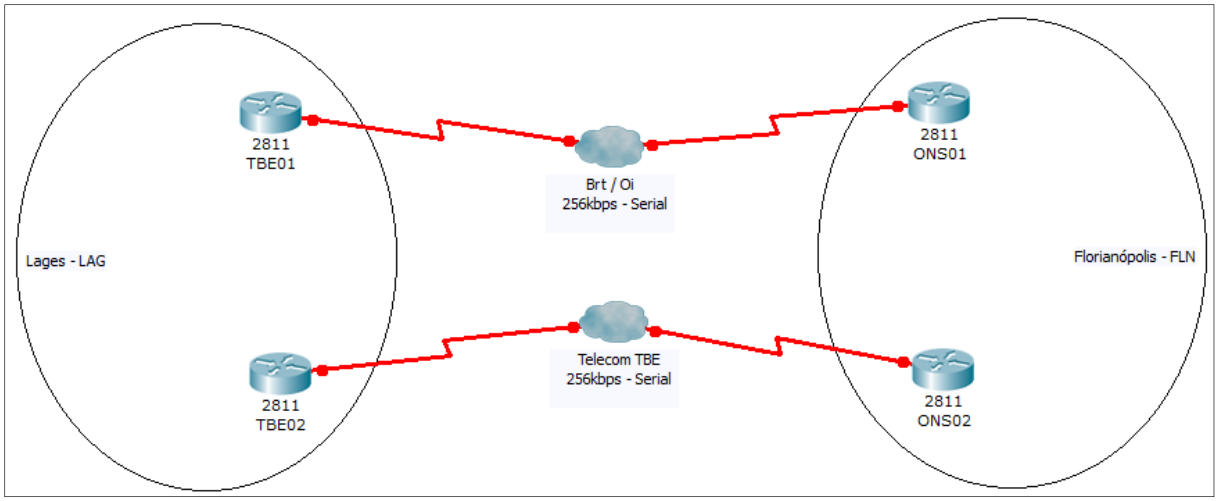

Figura 44. Topologia Simples da rede.
Fonte: próprio autor.

Na figura 46 são apresentados os endereços definidos para cada interface serial e ethernet, bem como o endereço virtual para o funcionamento do protocolo de redundância.

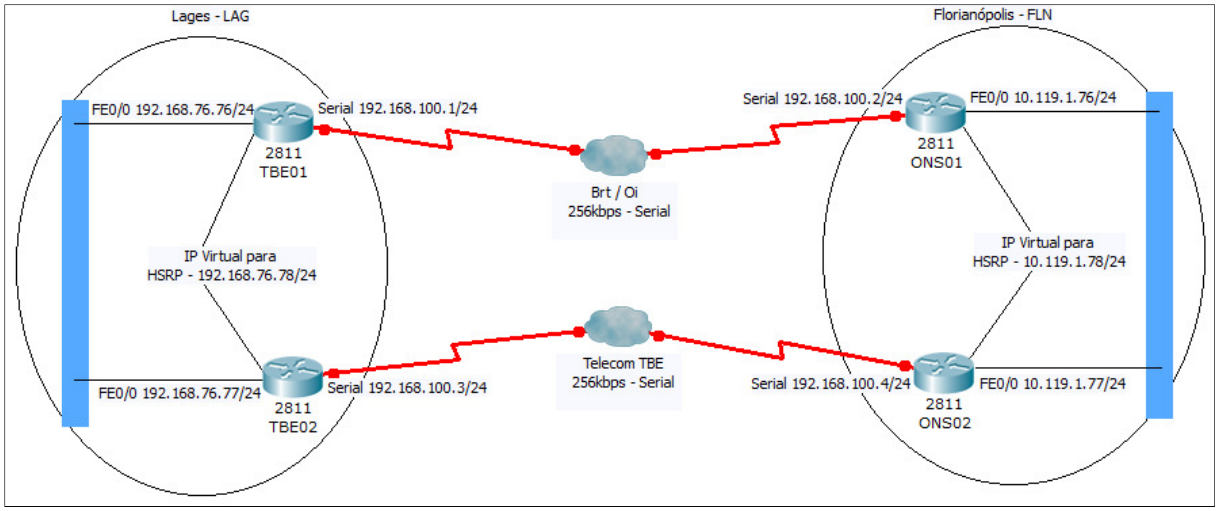

Figura 45. Topologia da rede com IP.

Fonte: próprio autor.

4.2.1. Configurações Gerais

Antes de proceder às configurações definitivas, os roteadores foram inicializados com os valores de fábrica *'erase startup-config'* (eliminar a configuração ativa), *'reload'* e *'cp startup config running config'* (copiando a configuração de boot para a configuração ativa) a fim de garantir a limpeza completa de qualquer configuração provisória utilizada para teste. A memória RAM é chamada pelo IOS de Running-Config e a memória Flash armazena as configurações da RAM chamando-as de Startup-Config. O primeiro comando é responsável pela limpeza da memória Flash enquanto o segundo provoca a reinicialização do router.

Ao ligar o roteador, as informações da Startup-Config devem ser carregadas para a Running-Config, ou seja, da Flash para a memória RAM, (processo similar a um computador pessoal quando carrega o sistema operacional do disco rígido para a memória RAM) neste caso o terceiro comando copia as configurações da Flash para a RAM, garantindo que ele opere com o que havia na Flash, ou seja, uma configuração limpa, pois a mesma foi apagada com o primeiro comando.

Nesta etapa foram definidos ainda os nomes *'hostnames'* para cada roteador conforme as topologias da rede mostradas nas figuras 45 e 46.

(configurando hostname)
Enable *(Habilita o modo de configuração)*
configure terminal *(Entra em modo de configuração)*
hostname ONS01 *(Associa nome ao equipamento)*
end *(Finaliza a configuração)*
wr *(Grava na memória)*

ONS01
ONS02
TBE01
TBE02

4.2.2. Segurança e Acesso

A fim de permitir o acesso remoto e a navegação para configuração do sistema, foi habilitado o serviço de Telnet na porta 23. O telnet é o serviço orientado à conexão não seguro (Point-to-Point Protocol Over Ethernet (ppoe) não criptografado), porém, por tratar-se de link dedicado entre agentes conhecidos do setor elétrico, concluímos que pode ser assim utilizado sem riscos consideráveis para segurança.

No que se refere ao acesso ao equipamento, foi utilizada senha criptografada disponível a partir do comando *enable secret.* Este comando implementa a senha mais forte disponível no roteador Cisco. A senha será solicitada no momento em que se tentar acessar o modo privilegiado para configuração.

> AAA trata-se de um framework arquitetural para configurar um grupo de três funções independentes de segurança de uma maneira consistente. AAA fornece um meio modular de configurar os seguintes serviços:
>
> - Authentication – Fornece o método de identificação de usuários, incluindo dialogo de login e password...
> - Authorization – Fornece o método para controle de acesso remoto...
> - Accounting – Fornece o método para coletar e enviar informações de segurança do servidor utilizadas para contabilizar, auditar e reportar...
>
> (CISCO, 2008, tradução nossa).

(configurando interface telnet)

no aaa new-model *(Desabilita AAA, pois a segurança será pelo método line.)*

enable secret level 15 LINE *(Habilita password com permissão alta para line)*

username tbe privilege 15 password xxx *(Define nome de usuário e password)*

line vty 0 4 *(Habilita a conexão da Virtual Terminal Line com Telnet)*

login *(Define o login como nulo)*

password cisco *(Define o password de acesso como cisco)*

privilege level 15 *(Define privilégio de acesso alto)*

4.2.3. Interfaces Físicas

Os endereços IP de cada interface foram definidos ainda na fase de projeto e constam na figura 46. *'Topologia da rede com IP'*. Estes endereços foram atribuídos às respectivas interfaces conforme amostragem.

(configurando interface serial)

enable *(Habilita o modo de configuração)*

configure terminal *(Entra em modo de configuração)*

interface serial 0/3 *(Seleciona a interface serial zero do slot três)*

no shutdown *(Ativa a interface)*

ip address 192.168.100.1 255.255.255.0 *(Define o IP da interface)*

(configurando interface fastEthernet)

enable *(Habilita o modo de configuração)*

configure terminal *(Entra em modo de configuração)*

interface fastEthernet 0/0 *(Seleciona a interface fast ethernet zero)*

no shutdown *(Ativa a interface)*

ip address 192.168.76.76 255.255.255.0 *(Define o IP da interface)*

As demais interfaces foram configuradas de modo similar, porém, respeitando os respectivos endereços pré-definidos. Para auxiliar na interpretação, foi criado um resumo dos endereços conforme o quadro 17 *'Referência das Interfaces'*. Uma vez configurados, os endereços podem ser lidos nos roteadores através do comando '*show running config'*, desta forma, obtém-se novamente os dados do quadro abaixo.

Router		Interface	Tipo	IP	Sub-Rede
Florianópolis	ONS01	Lan fe 0/0	FastEthernet	10.119.1.76	255.255.255.0
		Lan fe 0/1	FastEthernet	–	–
		Wan sr 0/3/0	Serial	192.168.100.2	255.255.255.0
		IP HSRP	Virtual	10.119.1.78	255.255.255.0
	ONS02	Lan fe 0/0	FastEthernet	10.119.1.77	255.255.255.0
		Lan fe 0/1	FastEthernet	–	–
		Wan sr 0/3/0	Serial	192.168.100.4	255.255.255.0
		IP HSRP	Virtual	10.119.1.78	255.255.255.0
Lages	TBE01	Lan fe 0/0	FastEthernet	192.168.76.76	255.255.255.0
		Lan fe 0/1	FastEthernet	–	–
		Wan sr 0/3/0	Serial	192.168.100.1	255.255.255.0
		IP HSRP	Virtual	192.168.76.78	255.255.255.0
	TBE02	Lan fe 0/0	FastEthernet	192.168.76.77	255.255.255.0
		Lan fe 0/1	FastEthernet	–	–
		Wan sr 0/3/0	Serial	192.168.100.3	255.255.255.0
		IP HSRP	Virtual	192.168.76.78	255.255.255.0

Quadro 17. Referência das Interfaces.
Fonte: próprio autor.

As interfaces são identificadas no software de acordo com a posição que assumem no hardware. Pode-se perceber pela figura 47 que a interface serial HWIC1T está inserida no slot 3 do chassi do roteador e em destaque azul ao lado do conector percebe-se a identificação *'serial0'*, assim ela é identificada como a primeira serial do slot 3, portanto *'interface serial 0/3'*.

A mesma ideia pode ser adotada para as demais interfaces que venham a ser inseridas no roteador exceto para as fastEthernet 0/0 e 0/1 as quais já possuem posição fixa definida (vide figura 41). Placas com mais de uma interface assumirão a designação sequencial da interface (0, 1, 2, ...) / slot.

O cartão de voz foi inserido no slot 2 (figura 48) em todos os roteadores, logo as identificações das portas para configuração serão 0/2 e 1/2. Na figura 49 pode-se perceber a vista frontal com que ficaram os roteadores após a instalação de todas as interfaces.

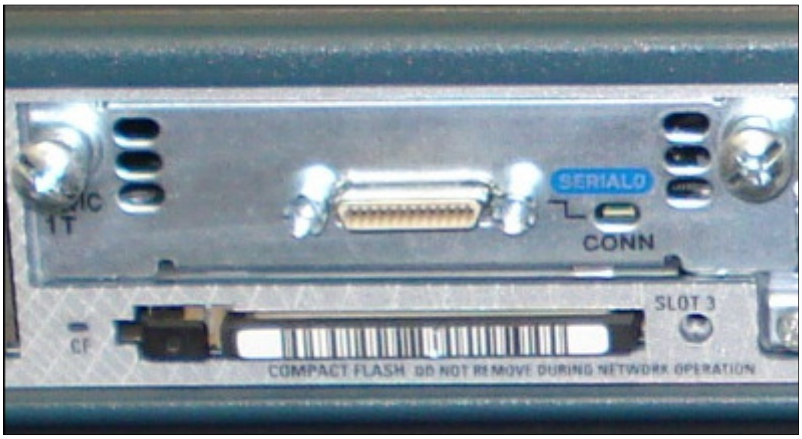

Figura 46. Interface Smart Serial – HWIC-1T.
Fonte: próprio autor.

Figura 47. Interface de voz – VIC-2FXS.
Fonte: próprio autor.

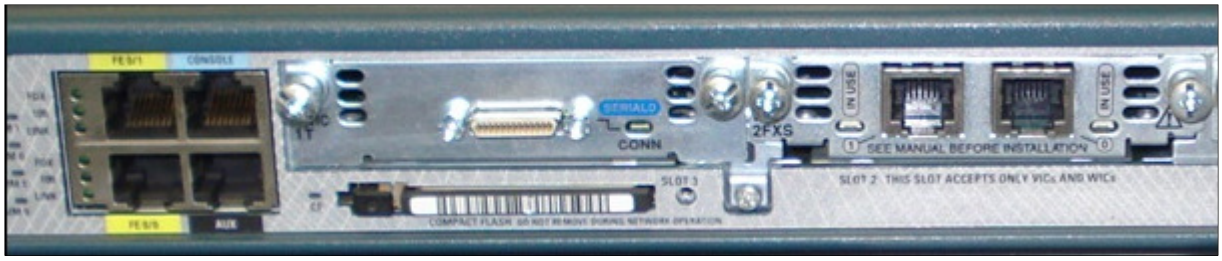

Figura 48. Vista geral das interfaces do roteador.
Fonte: próprio autor.

4.2.4. Configuração do Protocolo HSRP

Hot Standby Router Protocol (HSRP) foi desenvolvido para fornecer alta disponibilidade de rede pelo roteamento do tráfego IP dos hosts sobre a rede sem confiar na disponibilidade de apenas um único roteador. (CISCO, 2008, pág. 1435 tradução nossa).

Trata-se de um protocolo de redundância proprietário da Cisco. Filosoficamente, seu funcionamento consiste em cada roteador criar um endereço IP virtual comum entre eles. Outros dois parâmetros fundamentais são: a prioridade que cada roteador irá receber e o grupo o qual irá utilizar o IP virtual. Quando ambos estiverem ativos, aquele que tiver prioridade menor será o *'Active'* da rede, ou o responsável por assumir o IP virtual e rotear o tráfego entre as redes, caso este venha a falhar, o segundo roteador *'Standby'* identifica a ausência do primeiro e passa a sustentar então o IP virtual sendo o responsável pelo roteamento da rede e também mantem as aplicações em funcionamento contínuo. Como reflexo, a falha passa a ser minimizada para o usuário final. Os ativos que estiverem no mesmo grupo reconhecerão o IP Virtual, caso estejam em grupos diferentes, cada um reconhecerá o IP do grupo ao qual estiver associado.

No projeto, o HSRP foi configurado para utilizar o Grupo 76. A prioridade foi definida para 140 nos roteadores do link da TBE e 150 nos roteadores do link da operadora, desta forma, após testes, concluiu-se que os roteadores da TBE serão o *'Active'* e os roteadores da operadora serão o *'Standby'* na rede.

Constam abaixo as configurações básicas do protocolo para o roteador da TBE instalado na localidade de Lages, no entanto, vale lembrar que modos de funcionamento mais elaborados prevendo alterações de prioridade em casos de eventos ou contingências específicas são possíveis.

(configurando o HSRP no roteador da TBE)

enable *(Habilita o modo de configuração)*

configure terminal *(Entra em modo de configuração)*
interface fastEthernet 0/0 *(Seleciona a interface fast ethernet zero)*
ip address 192.168.76.77 255.255.255.0 *(Define o IP da interface)*
standby 76 ip 192.168.76.78 *(Define o IP de Standby da interface)*
standby 76 priority 140 *(Define a prioridade do IP standby da interface)*

4.2.5. Configuração de roteamento e voz

Conforme podemos perceber na figura 46, o objetivo final do conjunto é realizar o roteamento da rede 192.168.76.0/24 para a rede 10.119.1.0/24, no entanto, na prática, para alcançarmos este resultado, utilizamos uma terceira faixa IP que será para as interconexões seriais a qual recebeu o endereçamento 192.168.100.0/24. O que ocorre em termos de configuração em cada roteador é apenas a declaração das duas redes que ele possui, sendo uma a faixa da conexão fastEthernet e outra a da conexão serial, o restante do trabalho fica por conta do protocolo RIP o qual se encarrega de divulgar as redes de uma faixa para outra.

Para a realização das configurações básicas, este protocolo apresenta forma muito simples exigindo apenas a divulgação das redes (seguida pela máscara) que se quer rotear. Para proceder às configurações de roteamento, optou-se pela utilização do Routing Internet Protocol - RIP versão2, por esta apresentar algumas vantagens sobre a versão1 tais como: realização de anúncios do protocolo baseados em tráfego multicast e não mais broadcast e ainda segurança, autenticação e proteção contra a utilização de roteadores não autorizados.

(configurando o RIPv2)
enable *(Habilita o modo de configuração)*
configure terminal *(Entra em modo de configuração)*
router rip *(Define a utilização do protocolo rip para roteamento)*
version 2 *(Define a versão 2 do rip)*
network 10.119.1.0 *(Rede a ser roteada)*
network 192.168.100.0 *(Rede a ser roteada)*

Através do comando *'show ip route rip'* no modo enable pode-se obter os dados das redes configuradas no rip.

Para proceder às configurações de voz, optou-se por utilizar a topologia de "VOIP Between Gateways" em conjunto com "Private Line Automatic Ringdown – PLAR". A

tecnologia de voz sobre ip entre gateways, nada mais é do que estabelecer circuitos de voz entre roteadores que operam como gateways de uma rede, já o *'Plar'* estabelece a conexão de um telefone exclusivamente a outro, ou seja, basta abrir linha em um aparelho localizado em um gateway na extremidade A que automaticamente o outro aparelho correspondente irá chamar no gateway da extremidade B.

Chamadas PLAR automaticamente conectam um telefone a um segundo telefone quando o primeiro aparelho é retirado do gancho... . Quando esta conexão ocorre, o usuário não tem o tom de linha, porque a porta de voz habilitada para aquele telefone está conectada e pré-configurada com um número de discagem específico. (CISCO, 2009, pág. 147, tradução nossa).

Para o entendimento do funcionamento desta etapa, mais um conceito básico deve ser exposto, o *'pots'*. O '*Serviço antigo de telefone simples'* tratado como *'Plain old telephone service'* de onde vem a sigla POTS, transmite a ideia e mantém a forma de operação básica do serviço telefônico analógico antigo, porém, operando sobre uma tecnologia mais nova que é a de voz sobre IP. Entendidas estas informações, é possível compreender também os comandos de configuração de voz listados no exemplo de configuração abaixo.

(configurando as interfaces de voz do roteador TBE02 – IP 192.168.100.3)
dial-peer voice 1 pots *(Define o pots 1 como ponto de discagem de voz)*
destination-pattern 4000 *(Define o número do ponto de voz)*
port 0/2/0 *(Associa a porta zero do slot 2 ao ponto de voz)*
!
!
dial-peer voice 3 voip *(Cria o ponto de voip 3)*
destination-pattern 5000 *(define o número do ponto de voz)*
session target ipv4:192.168.100.4 *(Define o IP de destino deste ponto de voz)*
!
!
voice-port 0/2/0 *(Associa o ponto de voz à porta zero do slot 2 do ip destino)*
connection plar 5000 *(Define o número 5000 como conexão hotline)*

O processo tem inicio com a criação do ponto de voz 1 pots no roteador local. Os comandos *'destination-pattern 4000'* e *'port 0/2/0'* são responsáveis por atribuir respectivamente um valor lógico e um local físico a este ponto de discagem criado no

primeiro comando. A segunda sequencia de ajustes define o ponto lógico de voz sobre IP, sendo que o *'dial-peer voice 3 voip'* realiza a criação deste ponto como sendo 3, a seguir ele indica que o ponto terá como destino a porta 5000 *'destination-pattern 5000'* localizada no host 192.168.100.4.

As duas linhas do último grupo de comando fazem a conexão entre os pontos físicos de origem e os pontos lógicos de destino os quais foram declarados no início da sessão de configuração de voz. A lógica de configuração para as demais conexões de voz foi a mesma adotada no exemplo, mudando apenas os valores lógicos de atribuição da porta e de IP de destino. A topologia física simplificada do processo pode ser vista na figura abaixo.

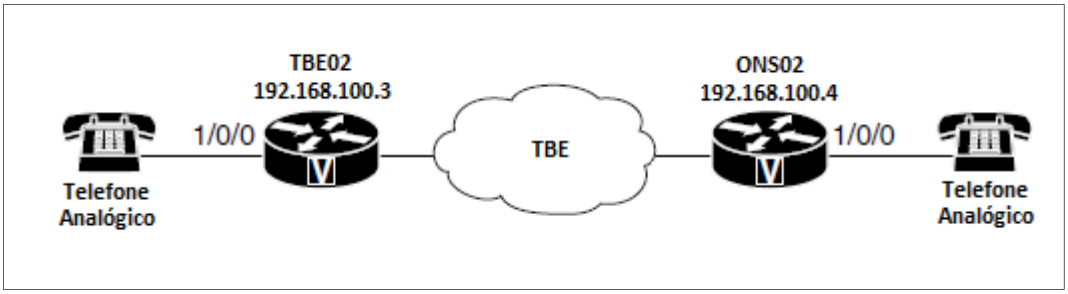

Figura 49. Topologia simplificada da ligação de voz.
Fonte: próprio autor.

A correspondência dos canais de voz foi definida com base nos endereços ip da rede. A fim de facilitar a visualização geral e documentar o processo foi criado o quadro 18 mostrado a seguir no qual são apresentados todos os endereços utilizados para voz.

Router		Interface	Tipo	IP	Pattern	IP - Destino	Pattern Destino	Plar
LAG	TBE01	Vic 0/2/0	Vic	192.168.100.1	4000	192.168.100.2	5001	5001
		Vic 0/2/1	Vic	192.168.100.1	4001	192.168.100.2	5002	5002
	TBE02	Vic 0/2/0	Vic	192.168.100.3	4002	192.168.100.4	5003	5003
		Vic 0/2/1	Vic	192.168.100.3	4003	192.168.100.4	5004	5004
FLN	ONS01	Lan fe 0/0	Vic	192.168.100.2	5001	192.168.100.1	4000	4000
		Lan fe 0/1	Vic	192.168.100.2	5002	192.168.100.1	4001	4001
	ONS02	Lan fe 0/0	Vic	192.168.100.4	5003	192.168.100.3	4002	4002
		Lan fe 0/1	Vic	192.168.100.4	5004	192.168.100.3	4003	4003

Quadro 18. Correspondência de voz.
Fonte: próprio autor.

Para o processo seguinte que é o monitoramento SNMP, há uma relativa importância no conhecimento sobre a forma de configuração dos equipamentos vista até aqui, pois poderá haver uma vasta lista de alarmes físicos e lógicos a serem aquisitados do roteador. Em muitos

casos, um entendimento básico da configuração adotada se faz necessária a fim de viabilizar uma leitura mais precisa.

4.2.6. Configuração do SNMPv3

Após a realização de testes, optou-se por utilizar a versão 3 do protocolo por esta apresentar maior segurança.

> A versão 3 do SNMP (SNMPv.3) trouxe como principais vantagens aspectos ligados à segurança. Esta segurança busca evitar a alteração das mensagens enviadas. Além disto, barra-se o acesso a elementos estranhos à execução de operações de controle, que são realizadas através da primitiva SetRequest. Evita-se também a leitura das mensagens por parte de estranhos, além de se garantir ao gerente o direito de alteração da senha dos agentes. A segurança é conseguida através da introdução de mecanismos de criptografia com o DES (Data Encryption Standard) e de algoritmos de autenticação que podem ser tanto o MD5 quanto o SHA (Secure Hash Algorithm). (GTA/UFRJ, 2002, Disponível em http://www.gta.ufrj.br/seminarios/semin2002_1/valeriana/snmp_4.htm).

4.2.7. Configuração nos roteadores – Agentes SNMP

Alguns parâmetros de configuração para acesso às informações do SNMP-SERVER foram sugeridos pelo ONS, são eles:

Nome do grupo de autenticação (groupname): **onsgrp**

Nome do usuário para autenticação (username): **onsuser**

Senha do protocolo md5 (password): **xxxx**

Endereço do host gerente (ip OpManager): **10.116.32.96**

Porta UDP (udp-port): **161**

De posse destes dados foi possível realizar as configurações básicas de gerenciamento SNMP de todos os roteadores da rede para a finalidade de gerenciamento por parte do ONS.

(configurando o snmp-server dos roteadores)

enable *(Habilita o modo de configuração)*

configure terminal *(Entra em modo de configuração)*

snmp-server group **onsgrp** v3 auth *(Cria um grupo snmp versão 3)*

snmp-server user **onsuser onsgrp** v3 auth md5 **md5ons** *(Cria um usuário snmp associado a um grupo na versão três com criptografia md5)*

snmp-server host **10.116.32.96** version 3 auth **onsuser** udp-port 161 *(Define o host associado ao usuário e a porta para o gerente)*

end *(Finaliza a configuração)*

wr *(Grava na memória)*

Os comandos *'enable'* e '*configure terminal'* apenas habilitam e acessam o modo de configuração, da mesma forma que *'end'* e *'wr'* respectivamente finalizam e gravam na memória os dados alterados. O comando *'snmp-server group **onsgrp** v3 auth'* define o nome do grupo de acesso (onsgrp), a versão do protocolo (v3) e a autenticação de um pacote sem encriptá-lo (auth).

A quarta linha de comando *'snmp-server user **onsuser onsgrp** v3 auth md5 **md5ons**'* define as configurações na sequencia que segue: o nome do usuário do host que conecta ao agente (onsuser), grupo de acesso, snmp na versão 3, autenticação sem encriptação, nível de autenticação com protocolo md5 e senha de autenticação do protocolo md5 (md5ons). Na quinta linha de configuração foi definido o endereço do host gerente para este grupo de usuários e a porta udp a ser utilizada.

Aprimoramentos destas configurações básicas foram realizados em testes experimentais constantes nas folhas de ensaio no apêndice E.

4.2.7.1. Gerente SNMP para o ONS

Para monitorar os links de comunicação entre os Centros Regionais e as demais empresas que compõem o setor elétrico o Operador Nacional do Sistema definiu a utilização do software OpManager da empresa ManageEngine para sua aplicação Gerente SNMP. Para rodar nos servidores SNMP, há preferência pela utilização da versão 3 do protocolo.

O gerente SNMP deverá realizar consultas às MIBs em períodos que podem variar de 1 a 3 minutos e os resultados devem apresentar desempenho e parâmetros de qualidade de acordo com o Procedimento de rede do ONS em seu Submódulo 13.2 – Requisitos Mínimos de Telecomunicações (Anexo A).

As informações interrogadas pelo ONS serão relativas às interfaces de voz (VIC 0/2/0 e VIC 0/2/1), de dados (FE 0/0 e FE 0/1) e disponibilidade dos roteadores em períodos específicos com a finalidade de gerar relatórios de desempenho visando cobrar o cumprimento dos requisitos do procedimento do anexo A.

4.2.7.2. Gerente SNMP para a TBE

A utilização do OpManager por parte da TBE foi definida (ao menos em um primeiro momento) pelo fato de a equipe em Lages ter a possibilidade de identificar eventuais falhas e visualizar os ativos da rede da mesma forma que o ONS o faz.

Foi utilizada a versão limitada do OpManager para rodar na NMS da TBE, no entanto, ela atende para este propósito devido ao fato de não haver necessidade de licença para uso em redes com menos de 10 agentes. A figura 51 apresenta a tela de instalação do OpManager no momento em que indica a limitação de uso do software em seu modo gratuito. Apesar da limitação do número de ativos a serem gerenciados, a licença não expira.

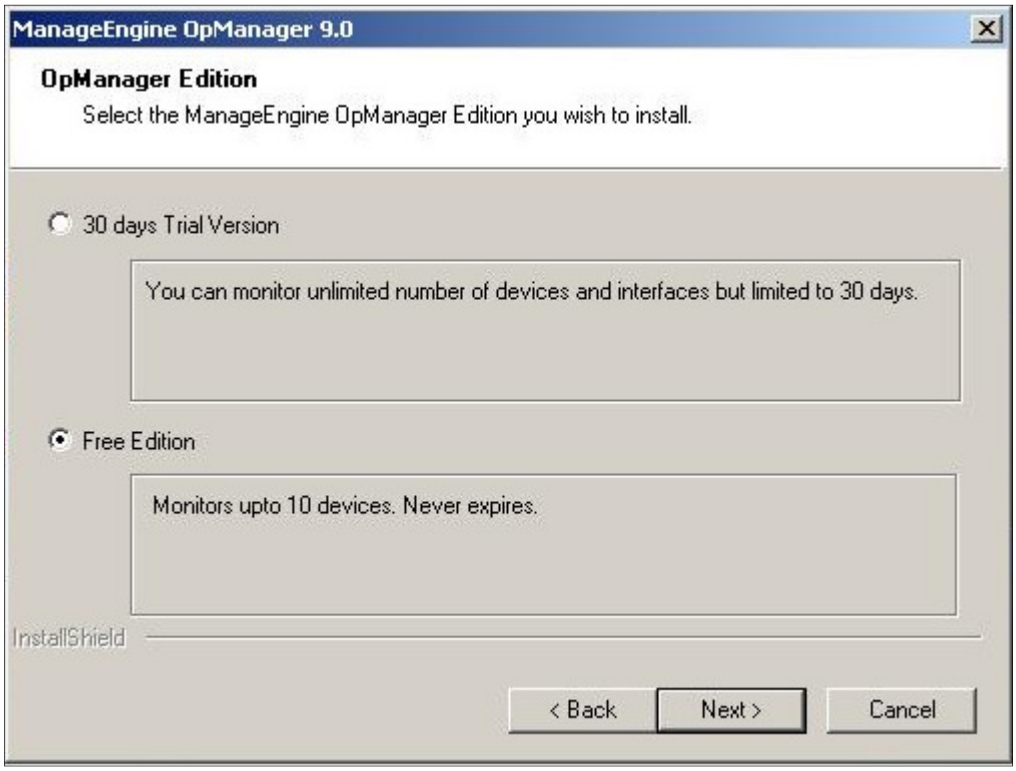

Figura 50. OpManager Free Edition.
Fonte: Software OpManager.

As informações acessadas pela TBE serão as mesmas monitoradas pelo ONS com acréscimo de outros dados que foram detectadas como essenciais ao longo do processo de testes do sistema. O acesso da TBE será diferenciado também no aspecto de permissões de escrita e leitura nos ativos da rede. Conforme visto na revisão bibliográfica, estas

funcionalidades permitirão escrever valores na MIB dos roteadores e alterar parâmetros remotamente por meio de interface gráfica.

4.2.8. Configuração do Servidor na TBE – Gerente SNMP

Inicialmente, o hardware responsável pela hospedagem do gerente SNMP na TBE apresentará características de desempenho que podem ser consideradas medianas, no entanto, considerando que a aplicação não exige alto poder de desempenho, ela deve atender com sobra as exigências do processo. A instalação do OpManager foi realizada sobre o Sistema Operacional Windows XP Professional completando assim a NMS.

Para a NMS foi definido o endereço IP 192.168.76.200/24 pelo que se pode concluir que ela ficará conectada fisicamente à mesma rede das portas fastEthernet 0/0 de ambos roteadores. Para alcançar o segundo roteador (extremidade B dos links) a NMS deverá ter como gateway o IP virtual definido na rede do lado da TBE, ou seja, 192.168.76.78/24.

A figura seguinte apresenta a topologia de rede do lado da TBE mostrando a NMS instalada no mesmo barramento de dados onde estão conectadas as portas fastEthernet do roteadores. Ao apontar como gateway o IP virtual de redundância, a NMS (a exemplo da aplicação principal) faz uso do roteamento RIP implantado nos roteadores para alcançar e gerenciar o lado B dos links.

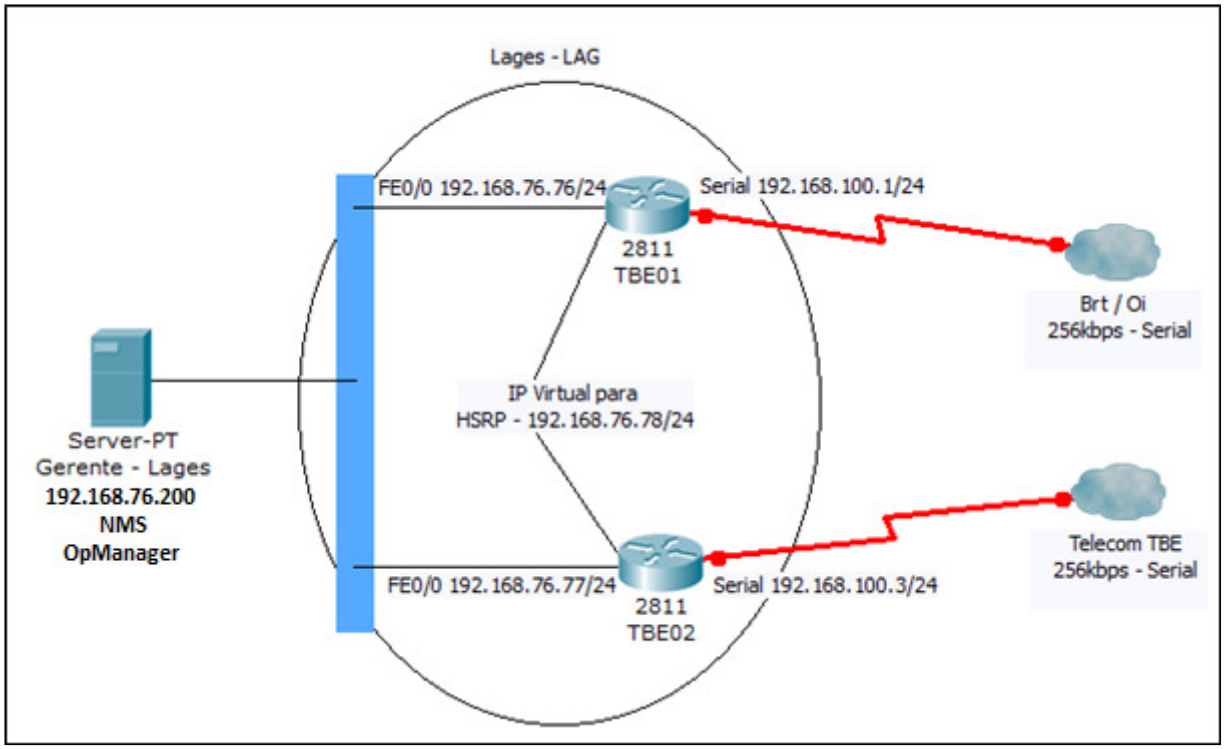

Figura 51. Topologia da rede no lado TBE.

Fonte: próprio autor.

A figura 53 apresenta a topologia de rede do lado do ONS mostrando a possível NMS a ser instalada naquela localidade.

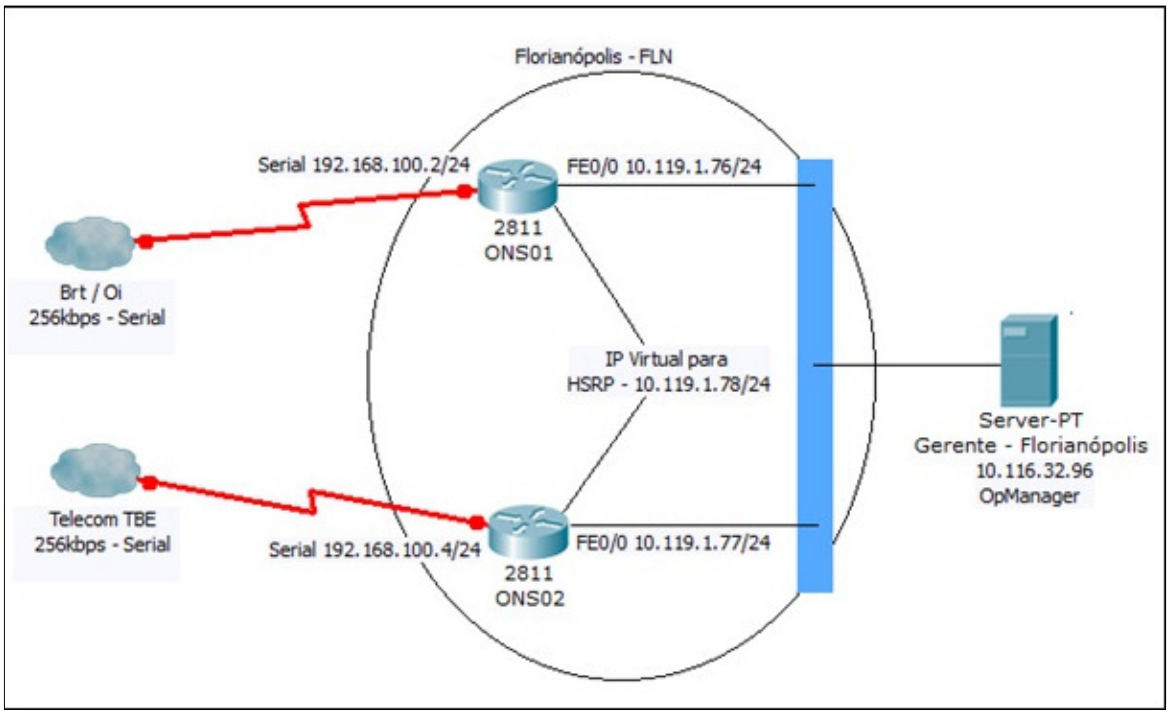

Figura 52. Topologia da rede no lado ONS.
Fonte: próprio autor.

Ao finalizar a instalação do software, foi verificada a conexão da NMS com os ativos da rede. Para aperfeiçoar os testes e analisar com mais qualidade os resultados, foi tomado como base o link 2 o qual é composto em sua totalidade por equipamentos da TBE.

A primeira inicialização do OpManager solicita um nome de usuário e password o qual por default é a string **admin** para ambos os campos. Assim que é acessada a tela inicial do OpManager é aberta na aba *'Home'* com visualização geral do sistema.

Figura 53. Tela de inicialização do OpManager.
Fonte: Software OpManager.

4.3. Monitoramento

A configuração inicial do software consiste em integrar ao OpManager os dispositivos de rede previamente configurados com o serviço SNMP-Server. A tela *´Admin´* oferece as opções necessárias à configuração do software, dentre elas *'Add Device'* a qual acrescentará os dispositivos por meio de seus respectivos endereços IP.

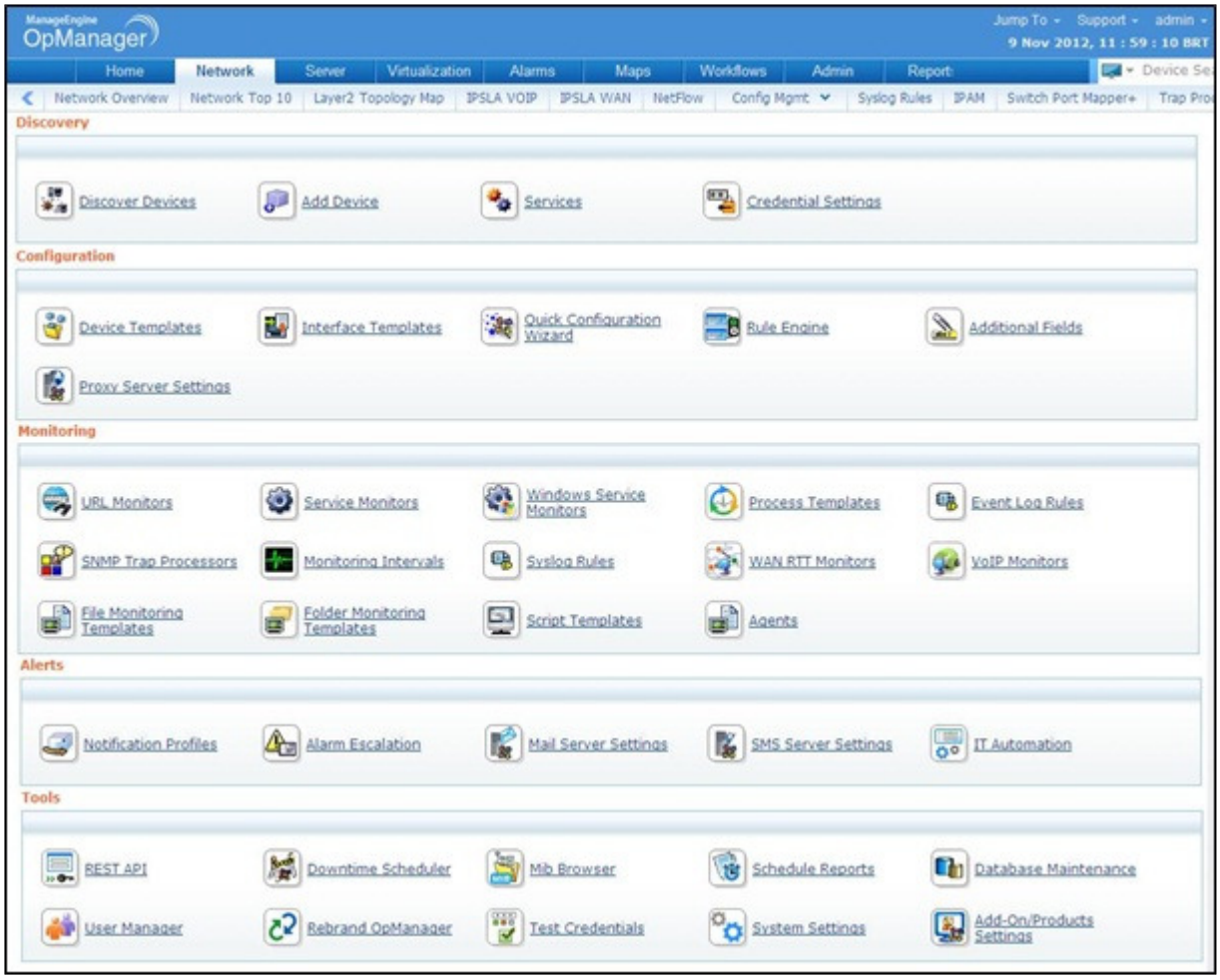

Figura 54. Tela de configuração do OpManager.
Fonte: Software OpManager.

Para o monitoramento foram definidos como essenciais os pontos das interfaces de rede, interfaces de voz e disponibilidade do equipamento dos quais alguns OIDs podem ser visualizados abaixo. Estes pontos vão apresentar-se ao usuário em forma de alarmes (All Alarms) ou de eventos (Event Summary e Recent Events).

(alguns OIDs disponíveis)

- 1.3.6.1.2.1.2.2 (org.dod.internet.mgmt.interfaces.ifTable) e respectivas entradas:

(amostragem da ifTable)

ifIndex.1:-->1

ifIndex.2:-->2

ifIndex.3:-->3

ifIndex.4:-->4

ifIndex.5:-->5

ifIndex.6:-->6

ifIndex.7:-->7

ifIndex.8:-->8

ifDescr.1:-->loopback (pseudo ethernet)

ifDescr.2:-->ti

ifDescr.3:-->Bridge

ifDescr.4:-->Ethernet

ifDescr.5:-->Ethernet over USB

ifDescr.6:-->ATM

ifDescr.7:-->RFC-2684B PPPoE Proxy

ifDescr.8:-->PPPoE

ifType.1:-->ethernet-csmacd(6)

ifType.2:-->94

Outros pontos passíveis de monitoramento podem ser importantes, no entanto, não são alvo de pesquisa por parte do ONS, devido a este fato, serão chamados de *´pontos não-essenciais´*. Os pontos não-essenciais, farão parte da lista de monitoramento da TBE, pois podem apresentar informações importantes para a manutenção preventiva dos ativos de rede, minimizando desta forma as paradas não planejadas dos serviços.

A configuração do refresh de tela foi configurada para um minuto, no entanto, ela não influencia na captura e registro dos valores configurados. O layout escolhido foi para apresentar as informações em duas colunas sendo selecionado pela aba *'overview – actions – edit layout'*.

Para uma visualização mais sugestiva, foram acrescentados mapas com base nas figuras 52 e 53 contendo a topologia da rede das duas localidades através do recurso *'Business view'*. Além da topologia o OpManager permite acrescentar links interativos sobre os dispositivos e suas respectivas ligações chamando a tela de relatórios ou mesmo telas de outras localidades que eventualmente tenham sido criadas. Após criado o modelo do Business View, ele foi selecionado para visualização geral na tela *'Network Overview'*. No BusinessView as figuras interativas dos equipamentos muda de cor indicando se o ativo está com alarme (amarelo, violeta e vermelho dependendo do tipo de severidade do alarme) ou normal (verde).

Para finalizar a configuração, podemos dizer que uma das opções importantes no OpManager é a ferramenta *'Workflow',* com ela é possível automatizar tarefas a partir da detecção de comportamentos indesejados no sistema sob supervisão. Dentro da opção

workflow foi inserido um novo workflow nomeado *'Verificação'* o qual prevê verificação diária da conectividade dos quatro equipamentos conforme figura abaixo.

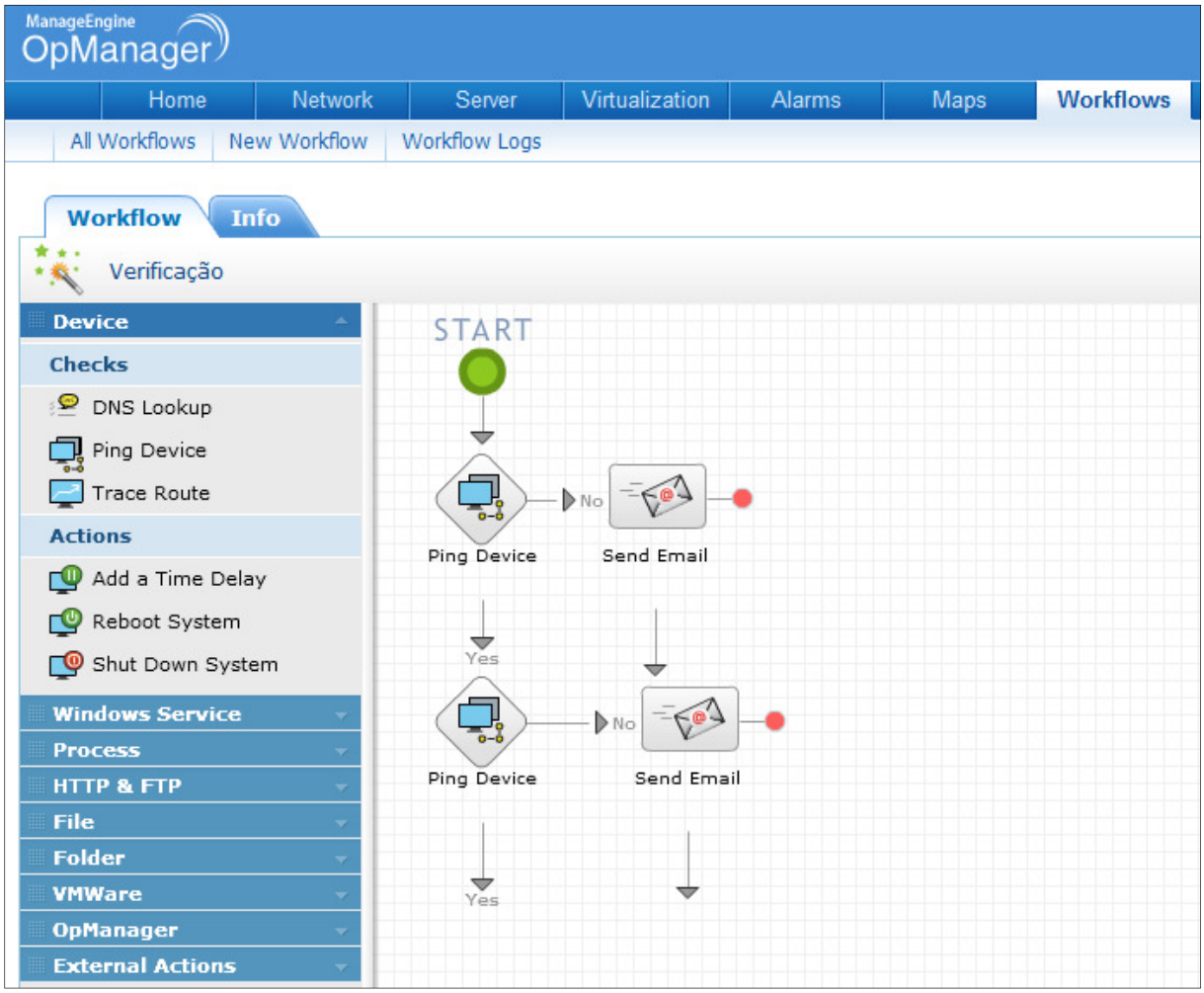

Figura 55. Tela do Workflow Verificação.
Fonte: Software OpManager.

Para que a opção de enviar e-mails em caso de falha funcione corretamente, duas condições precisam ser cumpridas: é preciso que a NMS possua acesso à internet e configurar o *'mail server settings'* dento da página *'Admin'*. A configuração dos ajustes de e-mail deve conter o servidor de saída de e-mail smtp do *'from e-mail ID'*, a porta utilizada (geralmente 587), o e-mail de destino, o nome de usuário e a senha do e-mail. Para o envio das mensagens foi utilizada a conta de e-mail da equipe do setor de manutenção de Sistema de Proteção, Controle, Supervisão e Telecom – SPCST de Lages.

(configuração do servidor de e-mail do OpManager)

Server name: smtp.gmail.com

Port: 587

From Email ID: spcs@tbe.com.br

To Email ID: tmachado@tbe.com.br

Time Out: 10

User Name: spcs

Password: •••••

A seguir pode ser visualizada a tela final já configurada para monitorar os equipamentos. Cada sub-quadro (Business View, All Alarms, etc...) é conhecido como *'Widgets'* e estes nada mais são do que pequenos aplicativos que rodam de forma individualizada dentro do software. Eles são úteis ainda pela funcionalidade que possuem de permitir copiar o código e acrescentá-los a uma página web, disponibilizando assim determinadas informações para domínio público ou simplesmente para consulta.

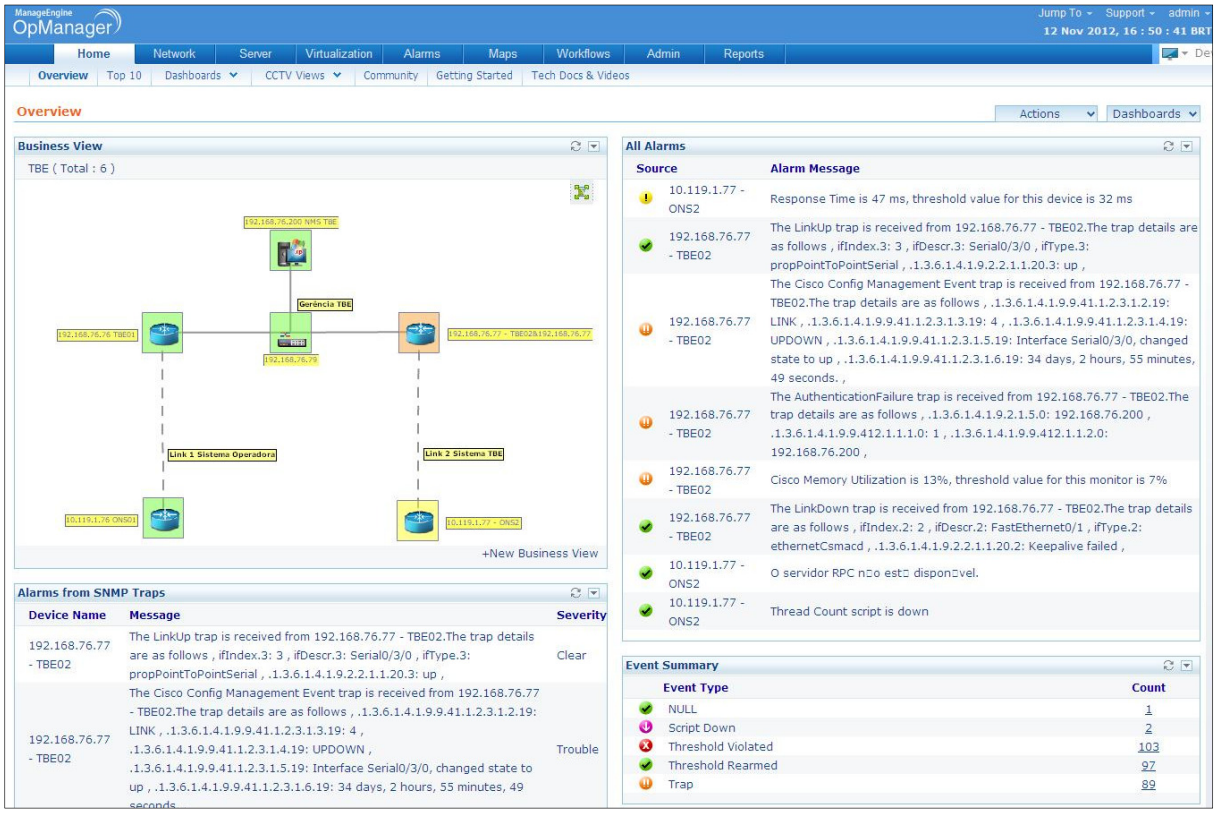

Figura 56. Layout final do sistema de monitoramento dos links.
Fonte: Software OpManager.

O layout final da tela OverView ficou com os widgets BusinessView e AlarmsGraph na coluna da esquerda e AllAlarms, EventSummary e RecentEvents na coluna da direita.

4.4. Relatórios e Histórico

O OpManager apresenta excelentes ferramentas de geração de relatórios e através das quais estão disponíveis também o histórico de sua vida útil, elas podem ser facilmente localizadas na aba *'Reports'*.

Podem ser definidos relatórios por uma variada gama de filtros (System, Health and Performance, All Events, etc...) e a partir do momento que eles são gerados podem ser diretamente impressos, transformados para relatório do tipo pdf, exportados para planilha do Excel ou ainda enviados diretamente para o e-mail do gestor da rede. Neste último caso o OpManager envia o relatório no formato <nome><data>.pdf dos eventos filtrados para o e-mail configurado no Report Mail.

Para facilitar a ilustração do acima exposto, foram extraídas algumas das telas de relatórios e gráficos disponíveis no OpManager as quais são apresentadas abaixo.

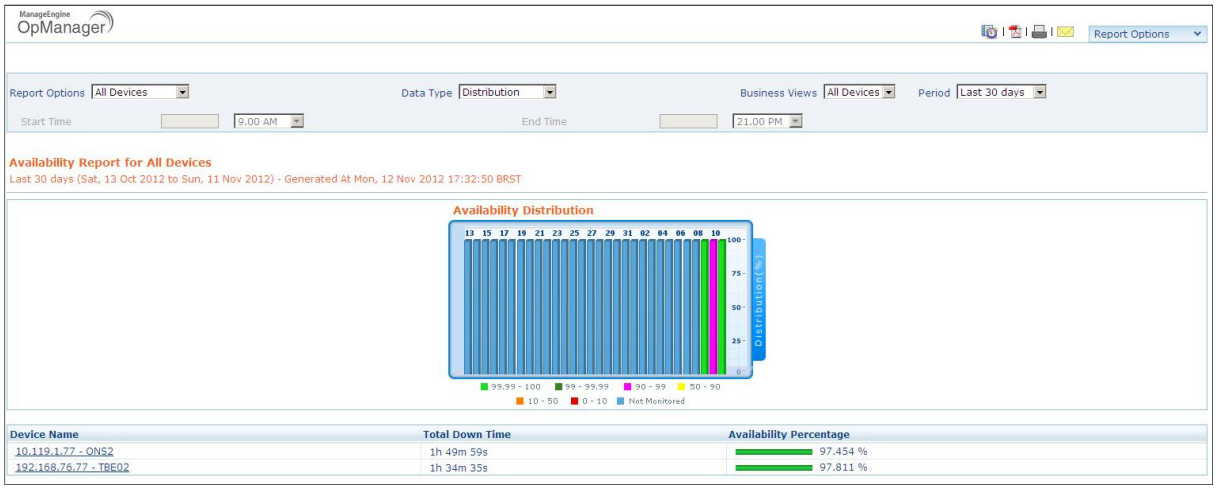

Figura 57. Tela de distribuição da disponibilidade x data.
Fonte: Software OpManager.

Figura 58. Tela de disponibilidade por equipamento.

Fonte: Software OpManager.

Figura 59. Tela de disponibilidade de um equipamento ao longo de uma semana.
Fonte: Software OpManager.

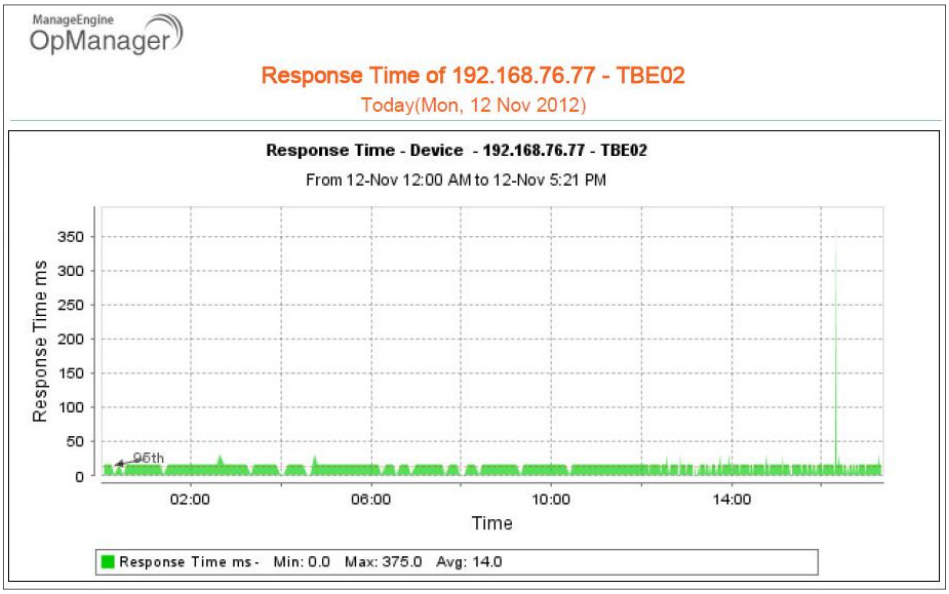

Figura 60. Gráfico do tempo de resposta de um período determinado.
Fonte: Software OpManager.

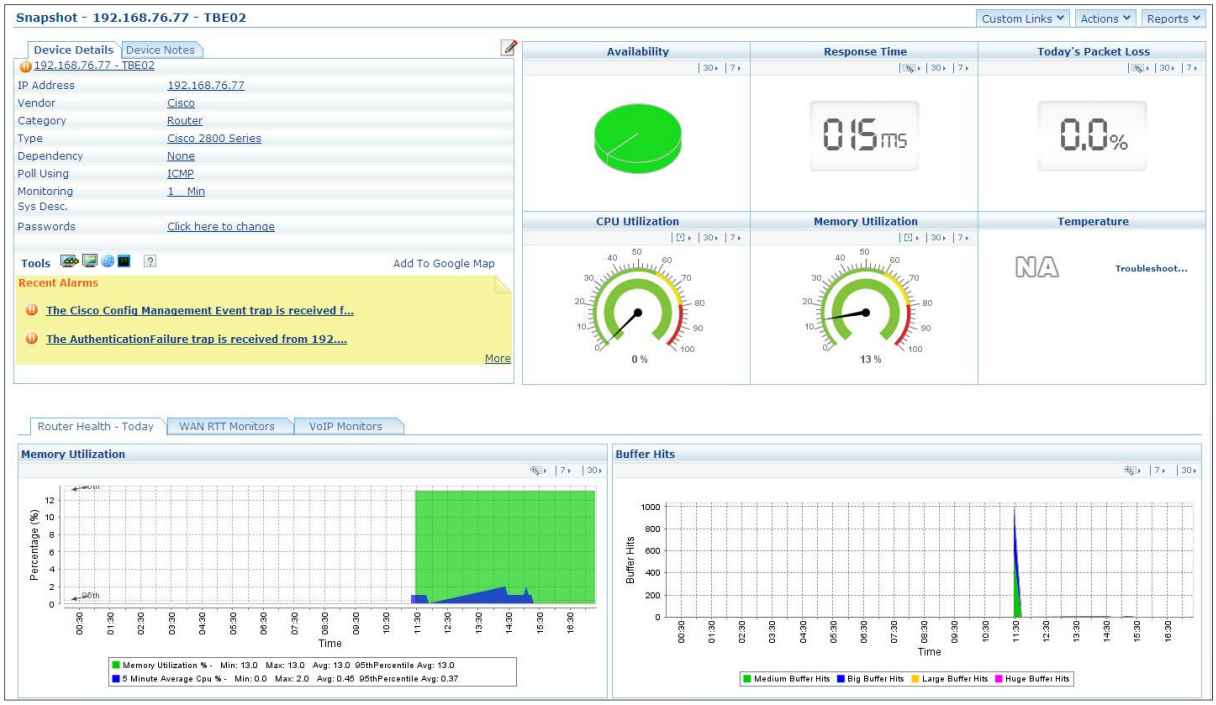

Figura 61. Gráfico de disponibilidade do TBE02.
Fonte: Software OpManager.

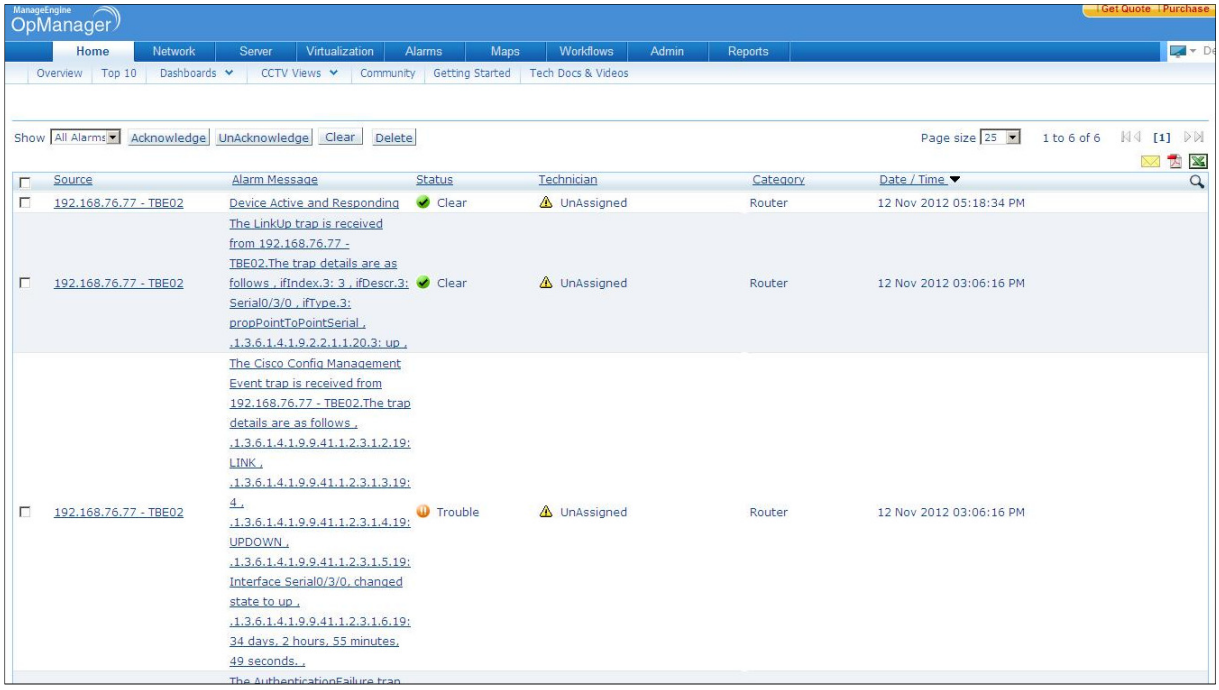

Figura 62. Tela de log de eventos.
Fonte: Software OpManager.

Inicialmente, os modelos de relatórios gerados pelo OpManager serão adotados para divulgação do desempenho dos canais monitorados para as áreas de interesse dentro da TBE.

IV – CONCLUSÃO

Este trabalho apresentou a metodologia completa para a implantação dos canais de dados e voz digital através de tecnologia roteada entre os centros de operação da TBE em Lages e o centro de operação do ONS em Florianópolis, desta forma estes links passaram a ser monitorados nos equipamentos de borda das instalações, possibilitando a utilização de todos os recursos e ferramentas disponíveis para a tecnologia IP.

Com o estudo do SNMP pôde-se observar o desempenho de algumas das ferramentas de monitoramento disponíveis no mercado. Impressionou a forma como um protocolo para gerência de redes o qual foi criado a mais de 30 anos apresentou-se nesta época como uma solução de alta eficiência para a problemática apresentada. A normatização do SNMP está estabelecida pelo IETF a partir do RFC1157, no entanto, observou-se a razão pela qual a contribuição do mercado da indústria foi importante no seu desenvolvimento. A necessidade do setor privado é um dos fatores que leva à pesquisa e ao crescimento das tecnologias.

Constatou-se que houve um elevado acréscimo de qualidade ao implantar o sistema de gerência migrando os antigos canais seriais/voz analógica para solução sobre IP, pois cada detalhe do processo agora pode ser registrado de forma contínua e até certo ponto automatizado.

A escolha dos pontos a serem monitorados foi em um primeiro momento realizada de forma abrangente, porém, a tendência é que com o crescimento do parque de rede da TBE aliado ao grande número de informações que os ativos propiciam por meio do SNMP, tenha início em breve um processo de filtragem de pontos a fim de evitar poluição de informação nas telas do gerenciamento da rede.

Foram apresentados alguns relatórios de desempenho emitidos a partir do software gerente da rede através dos quais se constatou o crescimento quanti-qualitativo das informações adquiridas pela equipe de SPCST da TBE de Lages para que esta possa conhecer o comportamento do sistema e embasar suas decisões de intervenção, no entanto, percebeu-se também que estes recursos evidenciam a necessidade de investimento e valorização do material humano envolvido no processo para que a empresa possa realmente ter qualidade e continuidade dos serviços essenciais.

Ainda que os objetivos do mercado privado em um mundo extremamente capitalista sejam os lucros, pode-se dizer que pequenas ações no final das contas podem contribuir para um aumento da confiabilidade do sistema elétrico nacional e consequentemente na qualidade

de vida da população do país como um todo. Esta constatação dá sentido nobre e torna a vida profissional mais humana.

V – REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 4. Ed. São Paulo: McGraw-Hill, 2008.

BARRETT, Diane; KING, Todd. **Redes de Computadores.** 1. Ed. Rio de Janeiro: LTC, 2010.

DANTAS, Mário **Redes de Comunicação e Computadores.** 1. Ed. Florianópolis: VisualBooks, 2009.

COMER, E. Douglas **Computer Networks and Internets.** 5. Ed. New Jersey-USA: Prentice Hall, 2008.

SEVERINO, A. Joaquim. **Metodologia do Trabalho Científico.** 22. Ed. São Paulo: Cortez, 2002.

CERVO, A. Luiz; BERVIAN, P. Alcino. **Metodologia Científica.** 4. Ed. São Paulo: MAKRON Books, 1996.

RICHARDSON, J. Roberto. **Pesquisa social: métodos e técnicas.** 3. Ed. São Paulo: Atlas, 1999.

MENDES, D. Rocha. **Redes de Computadores Teoria e prática.** 1. Ed. São Paulo: Novatec, 2007.

MAURO, R. Douglas; SCHIMIDT, J. Kevin. **Essential SNMP.** 2. Ed. Sebastopol, CA: O'Reilly Books, 2005.

ITU-T. **NULLSIMv1 and SIMv2 for SNMP all rely on ASN.1 MACROs which were removed in all versions of ASN.1 after 1988.** Disponível em [http://www.itu.int/net/ITU-T/info/answers.aspx?Fp=Default.aspx&Qn=91]. Acessado em 23 de setembro de 2012

ITU-T. **Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).**

ONS SM-25.12. **Indicadores de desempenho dos sistemas de supervisão e controle de serviço de telecomunicação.** Sub Módulo 25.12 revisão 1.1, 2010.

ONS SM-13.2. **Requisitos de telecomunicações.** Sub Módulo 13.2 revisão 1.0, 2009.

IETF. **About the IETF.** Disponível em [http://www.ietf.org/about/]. Acessado em 10 de outubro de 2012.

CISCO SYSTEMS, INC. Technical Support. **Telnet, Console and AUX Port Passwords on Cisco Routers Configuration Example.** Disponível em [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml]. Acessado em 25 de outubro de 2012.

CISCO SYSTEMS, INC. **Cisco IOS Security Configuration Guide.** Release 12.4. San Jose, CA: Cisco, 2008.

CISCO SYSTEMS, INC. **Cisco Voice over IP (CVOICE).** Third Edition. Indianapolis, IN: Cisco, 2009.

CISCO SYSTEMS, INC. **SNMPv3 Command Reference.** Release 12.0(3)T. Disponível em [http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html]. Acessado em 08 de novembro de 2012.

ADREM NETCRUNCH. **Software de Monitoramento de Rede para diferentes ambientes de rede.** Disponível em [http://www.adremsoft.com.br/netcrunch/]. Acessado em 02 de novembro de 2012.

Grupo de Teleinformática e Automação – UFRJ. **SNMP – Simple Network Management Protocol.** Disponível em [http://www.gta.ufrj.br/seminarios/semin2002_1/valeriana/snmp_4.htm]. Acessado em 08 de novembro de 2012.

ANEXO A – Submódulo 13.2 ONS

Operador Nacional
do Sistema Elétrico

Submódulo 13.2

Requisitos mínimos de telecomunicações

Rev. Nº.	Motivo da revisão	Data de aprovação pelo ONS	Data e instrumento de aprovação pela ANEEL
0.0	Este documento foi motivado pela criação do Operador Nacional do Sistema Elétrico.	27/06/2001	25/03/2002 Resolução nº 140/02
0.1	Atendimento à Resolução Normativa ANEEL nº 115, de 29 de novembro de 2004.	15/08/2005	25/09/2007 Resolução Autorizativa nº 1051/07
1.0	Versão decorrente da Audiência Pública nº 049/2008, submetida para aprovação em caráter definitivo pela ANEEL.	17/06/2009	05/08/2009 Resolução Normativa nº 372/09
2.0	Versão decorrente da Audiência Pública nº 002/2011.	01/12/2010	09/11/2011 Resolução Normativa nº 461/11

Endereço na Internet: http://www.ons.org.br

1 INTRODUÇÃO

1.1 Os serviços de voz e de dados atendem às seguintes atividades do Operador Nacional do Sistema Elétrico – ONS:

(a) operação em tempo real (Módulo 10 *Manual de Procedimentos da Operação* e Módulo 2 *Requisitos mínimos para instalações e gerenciamento de indicadores de desempenho da rede básica e de seus componentes*);

(b) normatização, pré-operação e pós-operação (Módulo 10);

(c) planejamento e programação da operação (Módulos 6 *Planejamento e programação da operação elétrica*, 7 *Planejamento da operação energética* e 8 *Programação Diária da Operação Eletroenergética*);

(d) apoio e coordenação dos serviços de telecomunicações (Módulo 13 *Telecomunicações*); e

(e) administração de serviços e encargos de transmissão (Módulo 15 *Administração de serviços e encargos de transmissão*).

1.2 Os serviços de telecomunicações, para suporte às atividades de operação do Sistema Interligado Nacional – SIN, subordinadas ao estabelecido no Módulo 10, abrangem serviços de comunicação de voz e de dados entre:

(a) centros de operação do ONS e centros de operação dos agentes de operação;

(b) centros de operação do ONS e instalações da rede de operação; e

(c) centros de operação dos agentes de operação e suas instalações.

1.3 O ONS se comunica por voz diretamente com a instalação do agente de operação quando este não tem centro de operação concentrando a supervisão destas instalações.

1.4 Alguns termos, a seguir indicados, são especificamente relevantes para o entendimento deste submódulo e encontram-se descritos detalhadamente no Módulo 20 - *Glossário de termos técnicos:* serviço de telefonia direta, serviço de telefonia comutada, Sistema Local de Aquisição de Dados (SAL) e Sistema Remoto de Aquisição de Dados (SAR).

1.5 Os submódulos aqui mencionados são:

(a) Submódulo 2.7 *Requisitos de telessupervisão para a operação*;

(b) Submódulo 10.2 *Hierarquia operacional*;

(c) Submódulo 10.14 *Requisitos operacionais especiais para os centros de operação e subestações e usinas da rede de operação*;

(d) Submódulo 13.3 *Implantação dos serviços de telecomunicações para atendimento às necessidades do Sistema Interligado Nacional*; e

(e) Submódulo 25.12 *Indicadores de desempenho dos sistemas de supervisão e controle e dos serviços de telecomunicações*.

2 OBJETIVO

2.1 O objetivo deste submódulo é definir os requisitos a que devem atender os serviços de telecomunicações para suporte às atribuições do ONS: os índices de disponibilidade estabelecidos para os serviços de telecomunicações, os valores mínimos dos parâmetros que devem ser assegurados para garantir a qualidade desses serviços e a configuração dos serviços necessários.

3 ALTERAÇÕES DESTA REVISÃO

3.1 Alterações decorrentes da redefinição de requisitos de disponibilidade para a classe A, B e C e configuração dos serviços de telecomunicação de voz e dados, bem como a inserção de prazos para adequações aos requisitos estabelecidos neste submódulo, quando da alteração dos mesmos ou de reclassificação da classe de serviços de voz e de dados.

4 .REQUISITOS

4.1 Requisitos de disponibilidade

4.1.1 Classes de serviço de voz e de dados

4.1.1.1 Para atender à operação do SIN, o serviço de telecomunicações deve dispor de serviços de comunicação de voz e de dados, em conformidade com este submódulo e com o Submódulo 25.12. Esses serviços devem ser oferecidos em três classes, a saber:

(a) Classe A: Deve apresentar disponibilidade total de 99,98%, apurada mensalmente, cujo valor de referência é o somatório dos últimos 12 (doze) meses. Isso implica uma indisponibilidade máxima total, num período de 12 (doze) meses, de 1 (uma) hora e 45 (quarenta e cinco) minutos. O serviço Classe A é um serviço prestado com recursos de telecomunicações disponibilizados através de duas rotas, que permitam monitoração de disponibilidade e apresentem, cada uma, uma disponibilidade de pelo menos 99%. Por esta razão, faz-se necessária a utilização de, pelo menos, duas rotas distintas e independentes, sendo uma direcionada para a localidade onde se encontra o Sistema Local de Aquisição de Dados (SAL) e outra direcionada para a localidade onde se encontra o Sistema Remoto de Aquisição de Dados (SAR), ambos situados em uma mesma região metropolitana. A disponibilidade do serviço será afetada somente quando as duas rotas estiverem indisponíveis simultaneamente. Será possível o direcionamento dos circuitos para diferentes SAL e/ou SAR do ONS em localidades distintas, com exceção das instalações de transmissão e de geração que atendam aos requisitos de Controle automático de Geração – CAG e Controle Automático de Tensão – CAT, conforme definido no Submódulo 2.7, por designação do ONS, após entendimento com o Agente envolvido.

(b) Classe B: Deve apresentar disponibilidade total igual ou superior a 99%, apurada mensalmente, cujo valor de referência é o somatório dos últimos 12 (doze) meses. A indisponibilidade máxima total num período de 12 (doze) meses para o serviço Classe B é de 87 (oitenta e sete) horas e 36 (trinta e seis) minutos. O serviço Classe B deve ser, preferencialmente, disponibilizado através de uma rota direcionada para a localidade designada pelo ONS. O Agente poderá ser chamado a instalar um segundo canal de comunicação de dados e/ou voz, na situação em que um único canal não esteja atendendo a disponibilidade necessária, cuja localidade tenha sido indicada pelo agente. Neste caso, o segundo canal será instalado na localidade indicada pelo ONS.

(c) Classe C: Deve apresentar disponibilidade total igual ou superior a 95%, apurada mensalmente, cujo valor de referência é o somatório dos últimos 12 (doze) meses. A indisponibilidade máxima total num período de 12 (doze) meses para o serviço Classe C é de 438 (quatrocentos e trinta e oito) horas. O serviço Classe C é uma rota direcionada para a localidade designada pelo ONS. O Agente poderá ser chamado a instalar um segundo canal de comunicação de dados e/ou voz, na situação em que um único canal não esteja atendendo a disponibilidade necessária.

4.2 Requisitos de qualidade

4.2.1 Todos os serviços de interesse do ONS realizados sobre sistemas de transmissão analógicos ou mistos – estes com parte analógica e parte digital – devem obedecer aos valores dos parâmetros a seguir:

(a) Níveis relativos nos pontos de entrada e saída analógicos, a 4 fios, em ambos os lados das conexões de voz:

(i) lado de transmissão: -5,5 ± 0,5 dBr; e

(ii) lado de recepção: -2,0 ± 0,5 dBr.

(b) Nível máximo aceitável de ruído na recepção: -40 dbmO.

(c) Relação sinal/ruído mínima: 40 dB.

(d) Taxa de erro máxima: 50 *bits*/milhão, sem código de correção de erro (circuitos de dados).

4.2.2 Todos os serviços de interesse do ONS realizados sobre sistemas de transmissão puramente digitais devem obedecer aos valores dos parâmetros a seguir:

(a) Níveis relativos nos pontos de entrada e saída analógicos, a 4 fios, em ambos os lados das conexões de voz:

(i) lado de transmissão: 0 ± 0,5 dBr; e

(ii) lado de recepção: 0 ± 0,5 dBr.

(b) Requisito qualitativo dos circuitos: taxa de erro de *bit*, medida durante 15 (quinze) minutos, igual a 0 (zero), para qualquer taxa de transmissão igual ou superior a 64 Kbps, em, pelo menos, uma medida entre três realizadas.

(c) No caso de uso de canais de voz com compressão, serão admitidas as subtaxas de 8 Kbps (ITU-T G.729) e 16 Kbps (ITU-T G.728), desde que não sejam utilizadas mais do que três seções com compressão em cascata.

(d) No caso de uso de redes para o provimento dos serviços:

(i) latência (round trip): ≤ 140 ms;

(ii) variação estatística do retardo: ≤ 20 ms; e

(iii) taxa de perda de pacotes: < 1%.

(e) No caso de uso de redes satélites para o provimento dos serviços:

(i) latência (round trip): ≤ 700 ms;

(ii) variação estatística do retardo: ≤ 90 ms; e

(iii) taxa de perda de pacotes: < 1%.

4.2.3 Para os requisitos de qualidade, são utilizados os padrões e as recomendações constantes em documentos emitidos pela TELEBRÁS (Práticas TELEBRÁS), ITU-T[1] e ETSI[2].

4.3 Requisitos de configuração de voz e de dados

4.3.1 Conforme hierarquia definida no submódulo 10.2, cuja representação é mostrada abaixo

(a) A Figura 1 apresenta a hierarquia operacional do SIN e as possíveis configurações dos serviços de comunicação de voz e de dados para suporte às atividades da operação,

[1] *International Telecommunication Union – Telecommunication Standardization Sector*
[2] *European Telecommunications Standards Institute*

considerando os centros de operação do ONS e os centros de operação dos agentes de operação.

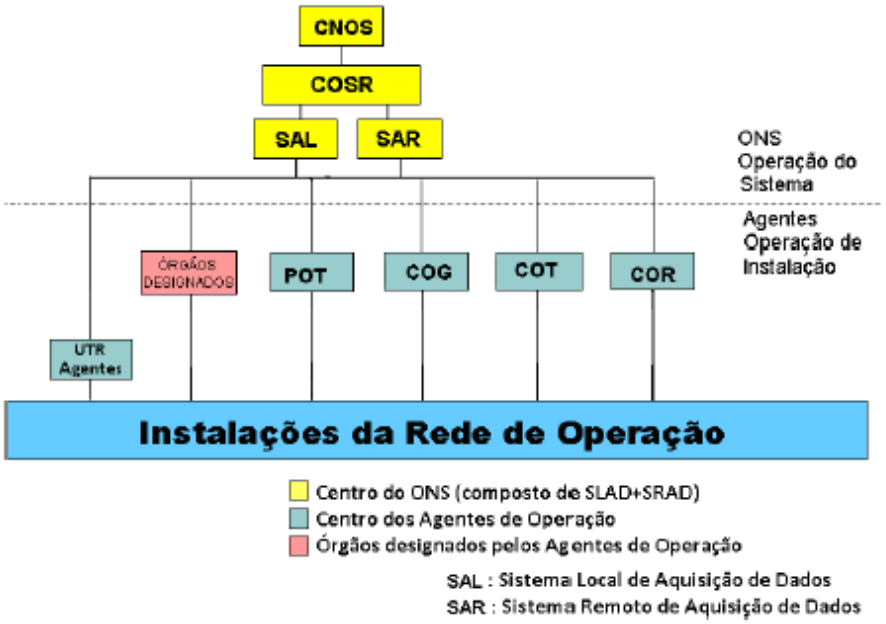

Figura 1 - Configurações possíveis para os serviços de telecomunicações de voz e de dados, considerando os centros de operação do ONS.

4.3.2 Os serviços de comunicação de voz dão suporte às atividades de normatização, pré-operação, operação em tempo real, pós-operação, apoio e coordenação de telecomunicações, planejamento e programação da operação.

4.3.2.1 Para suporte às atividades de operação em tempo real

(a) Devem ser disponibilizados serviços de telefonia direta Classe A:

(i) entre os centros de operação (SAL e SAR) do ONS[3];

(ii) entre os centros de operação (SAL e SAR) do ONS e os centros de operação próprios ou designados pelos agentes de operação; e

(iii) entre os centros de operação (SAL e SAR) do ONS e as instalações da rede de operação que não são subordinadas a um centro de operação de agente de operação que se relacione com o ONS.

(b) Devem ser disponibilizados, pelo menos, serviços de telefonia direta Classe B:

[3] Esses serviços são de responsabilidade do ONS.

(i) entre os centros de operação (SAL ou SAR), conforme designação do ONS, e instalações especificamente indicadas pelo ONS e devidamente justificadas, observados os critérios de segurança e economicidade.

4.3.2.2 O serviço de telefonia para as áreas de normatização, pré-operação e pós-operação e para atividades de apoio e coordenação dos serviços de telecomunicações requer, no mínimo, a disponibilização de serviço de telefonia comutada Classe C:

(a) entre os centros de operação (SAL) do ONS e os centros de operação próprios ou designados pelos agentes de operação que tenham instalações na rede de operação ou estejam conectados à rede básica.

4.3.2.3 O serviço de telefonia para as áreas de planejamento e programação da operação requer, no mínimo, a disponibilização de serviços de telefonia comutada Classe C:

(a) entre o escritório central do ONS e os centros de operação (SAL) do ONS (áreas de planejamento e programação da operação), a serem fornecido pelo ONS; e

(b) entre o escritório central do ONS e as áreas de planejamento e programação da operação dos agentes.

4.3.3 Os serviços de comunicação de dados dão suporte às atividades de normatização, pré-operação, operação em tempo real, pós-operação, planejamento e programação da operação, administração de serviços e encargos da transmissão.

4.3.3.1 Para suporte às atividades da operação em tempo real

(a) Devem ser disponibilizados serviços Classe A, em atendimento ao estabelecido no Submódulo 2.7:

(i) entre os centros de operação (SAL e SAR) do ONS[4];

(ii) entre os centros de operação (SAL e SAR) do ONS e os centros de operação dos agentes de operação com os quais o ONS se relaciona;

(iii) entre os centros de operação (SAL e SAR) do ONS e as instalações de transmissão e de geração, para atender aos requisitos de Controle Automático de Geração – CAG e Controle Automático de Tensão – CAT, conforme definido no Submódulo 2.7;

(iv) entre os centros de operação (SAL e SAR) do ONS ou do agente de operação e as instalações de transmissão e geração da rede de supervisão não contempladas nos itens anteriores, que devem ter comunicação direta com esses centros, conforme definido no Submódulo 10.2;

(v) entre os centros de operação (SAL e SAR) do ONS e os Centros de Operação de Distribuição – COD, conforme definido no Submódulo 10.2; e

(vi) entre os centros de operação (SAL e SAR) do ONS e os consumidores livres conectados à rede básica.

(b) Devem ser disponibilizados serviços Classe B, pelo próprio ONS, de acordo com o estabelecido no Submódulo 2.7:

(i) entre os centros de operação (SAL) do ONS e pontos definidos pelo ONS, para o controle de tensão e detecção de ilhamento.

4.3.3.2 Para suporte às atividades de normatização, pré-operação, pós-operação, programação e planejamento da operação, administração de serviços e encargos da transmissão e demais sistemas de apoio disponibilizados pelo ONS para os agentes de operação:

[4] Esses serviços são de responsabilidade do ONS.

4.3.3.3 Os agentes de operação devem dispor, por sua conta e risco, de meio de acesso à internet, dimensionado de forma a suportar o carregamento imposto pelo conjunto dessas atividades, através de serviço de comunicação de dados Classe B. As redes atualmente utilizadas como suporte para essas atividades só podem ser desativadas com a anuência das áreas do ONS por elas responsáveis

4.4 Prazos e adequações

4.4.1 O agente de operação que necessite se adequar aos requisitos de disponibilidade, qualidade e quantidade de rotas do sistema de telecomunicação, devido à reclassificação da classe de serviços de telecomunicação de voz e de dados da instalação, disporá de um período de até 6 (seis) meses, a partir da data em que for informado pelo ONS da necessidade dessa adequação.

4.4.2 O agente de operação que, por força de mudança de endereço de qualquer localidade do ONS (onde se encontram os SAL ou SAR), necessite adequar seus sistemas de telecomunicações, disporá de um período de até 6 (seis) meses, a partir da data em que for informado pelo ONS da necessidade dessa adequação.

APÊNDICE A – SHOW RUNNING-CONFIG TBE02

```
show running-config
Building configuration...

Current configuration : 1646 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname TBE02
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$bamN$NJyzCOjaRUwB3yNNyYfbq.
!
no aaa new-model
dot11 syslog
ip source-route
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
username TBE privilege 15 password 7
131718060E0D002539757A606177
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 description ETH0 SAGE
 ip address 192.168.76.77 255.255.255.0
 duplex auto
 speed auto
 standby 76 ip 192.168.76.78
 standby 76 priority 150
!
interface FastEthernet0/1
 description ETH1 GERERENCIA
 no ip address
 shutdown
duplex auto
speed auto
!
interface Serial0/3/0
 description SERIAL SAGE
 ip address 192.168.100.3 255.255.255.0
!
router rip
 network 192.168.76.0
 network 192.168.100.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
control-plane
!
!
voice-port 0/2/0
 connection plar 4001
!
voice-port 0/2/1
 connection plar 7778
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
dial-peer voice 1 pots
 destination-pattern 4000
 port 0/2/0
!
dial-peer voice 3 voip
 destination-pattern 4001
 session target ipv4: 192.168.100.4
!
dial-peer voice 2 pots
 destination-pattern 7777
 port 0/2/1
!
dial-peer voice 4 voip
 destination-pattern 7778
 session target ipv4:192.168.100.4
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 login local
!
scheduler allocate 20000 1000
end

TBE02#
```

APÊNDICE B – SHOW RUNNING-CONFIG ONS02

```
show running-config
Building configuration...

Current configuration : 1706 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ONS02
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$P9wg$DKByF6v19wEU/siSwPPrA1
enable password 7 072308626B
!
no aaa new-model
dot11 syslog
ip source-route
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
Password encryption aes
!
!
voice-card 0
!
!
username TBE privilege 15 password 7
131718060E0D002539757A606177
archive
 log config
  hidekeys
!
!
interface FastEthernet0/0
description ETH0 SAGE
 ip address 10.119.1.77 255.255.255.0
 duplex auto
 speed auto
 standby 76 ip 10.119.1.78
 standby 76 priority 140
!
interface FastEthernet0/1
 description ETH1 GERERENCIA
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/3/0
 description SERIAL SAGE
ip address 192.168.100.4 255.255.255.0
!
router rip
 network 10.0.0.0
 network 192.168.100.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
voice-port 0/2/0
 connection plar 4000
!
voice-port 0/2/1
 connection plar 7777
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
dial-peer voice 1 pots
 destination-pattern 4001
 port 0/2/0
!
dial-peer voice 3 voip
 destination-pattern 4000
 session target ipv4:192.168.100.3
!
dial-peer voice 2 pots
 destination-pattern 7778
 port 0/2/1
!
dial-peer voice 4 voip
 destination-pattern 7777
 session target ipv4:192.168.100.3
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 login local
!
scheduler allocate 20000 1000
end

TBE02#
```