

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

CLÉO PAGNO LISBÔA

**Caracterização de Novas Interfaces de
Telecom a partir de Interfaces e Dispositivos
Gerenciáveis.**

Dissertação apresentada como requisito parcial
para a obtenção do grau de Mestre em Ciência
da Computação

Prof. Dr. Jürgen Rochol
Orientador

Porto Alegre, julho de 2007.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Lisbôa, Cléo Pagno

Caracterização de Novas Interfaces de Telecom a partir de Interfaces e Dispositivos Gerenciáveis / Cléo Pagno Lisbôa – Porto Alegre: Programa de Pós-Graduação em Computação, 2007.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR-RS, 2007. Orientador: Prof. Dr. Jürgen Rochol.

1. Interfaces de Telecom. 2. Interfaces de telecomunicações utilizadas no Brasil. 3. Gerência de Redes. 4. Gerência de configuração. I. Rochol, Jürgen. II. Título.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Reitor: Prof. José Carlos Ferraz Hennemann

Vice-Reitor: Prof. Pedro Cezar Dutra Fonseca

Pró-Reitora de Pós-Graduação: Profa. Valquiria Linck Bassani

Diretor do Instituto de Informática: Prof. Flávio Rech Wagner

Coordenadora do PPGC: Profa. Luciana Nedel

Bibliotecária-Chefe do Instituto de Informática: Beatriz Regina Bastos Haro

AGRADECIMENTOS

Gostaria de dedicar este trabalho primeiramente ao meu orientador Prof. Dr. Jürgen Rochol, por ter pacientemente entendido minhas ausências em virtude dos meus afazeres profissionais e por ter me ajudado sempre e em qualquer circunstância. Agradeço também aos meus colegas de trabalho que souberam entender as minhas faltas em comemorações e festejos e por terem entendido as saídas no horário do expediente em virtude do mestrado. À minha esposa e à minha família pelo carinho, amor e compreensão, e sobretudo por terem sido aquela força a mais que é profundamente necessária para a conclusão da dissertação.

SUMÁRIO

LISTA DE ABREVIATURAS.....	6
LISTA DE FIGURAS.....	9
LISTA DE TABELAS.....	10
RESUMO.....	11
ABSTRACT.....	ERRO! INDICADOR NÃO DEFINIDO.
1 INTRODUÇÃO.....	13
2 SISTEMAS DE GERÊNCIA.....	15
2.1 Gerência de Falhas.....	16
2.2 Gerência de Configuração.....	18
2.3 Gerência de Contabilidade.....	19
2.4. Protocolo SNMP.....	20
2.4.1 O Agente.....	21
2.4.2 O Gerente.....	22
2.4.3 Formato das mensagens SNMP.....	24
2.4.4 Operações SNMP.....	24
2.4.5 Esgotamento do protocolo SNMP para gerência de equipamentos SDH.....	25
3 SOFTWARES DE GERÊNCIA DE TELECOM.....	27
3.1 Desenvolvimento de softwares de gerência de telecom.....	28
3.2 Atualização dos Sistemas de Gerência para suportar novos dispositivos.....	30
4 PESQUISA ENTRE AS INTERFACES DE TELECOM UTILIZADAS NO BRASIL.....	31
4.1 Interface serial RS-232.....	33
4.1.1 Configurações:.....	34
4.2 Interface V.35.....	35
4.3 Recomendação G.703.....	38
4.3.1 Estrutura dos quadros.....	39
4.4 Interfaces de Telefonia.....	41
4.4.1 Interfaces FXS e FXO.....	41
4.4.2 Interface E&M.....	43
4.5 Interfaces xDSL.....	45
4.5.1 Interface G. SHDSL.....	45
4.5.2 Interface ADSL.....	47
4.6 Interface Ethernet.....	49

5 IDENTIFICAÇÃO DE OBJETOS SEMELHANTES.	52
6 DEVICE COMPARE 1.0.....	57
6.1 Descrição	58
6.2 Apresentação do Software	59
6.3 Estrutura do Software.....	59
6.4 Estudo de caso - Suporte à interface Tr24E1.....	61
7 CONCLUSÃO	64
REFERÊNCIAS.....	66

LISTA DE ABREVIATURAS

ADSL	<i>Asymmetric Digital Subscriber Line</i>
ASN. 1	<i>Abstract Syntax Notation One</i>
BERT	<i>Bit Error Rate Test</i>
CAS	<i>Channel Associated Signaling</i>
CCITT	<i>The International Telegraph and Telephone Consultative Comitee</i>
CPU	<i>Central Processing Unit</i>
CRC4	<i>Cyclic Redundancy Check 4-bit</i>
CRC6	<i>Cyclic Redundancy Check 6-bit</i>
DBm	Decibel
DCD	<i>Data Carrier Detect</i>
DDR	Discagem Direta Ramal
DPSK	<i>Differential Phase Shift Keying</i>
DTMF	<i>Dual Tone Multi-Frequency</i>
DTR	<i>Data Terminal Ready</i>
EIA	<i>Eletronic Industries Association</i>
E&M	<i>Ear and Mouth</i>
EOC	<i>Embedded Operations Channel</i>
EPROM	<i>Erasable Programmable Read-only Memory</i>
fig.	Figura
FXO	<i>Foreign Exchange Office</i>
FXS	<i>Foreign Exchange Subscriber</i>
GFP	<i>Generic Framing Procedure</i>
GUI	<i>Graphical User Interface</i>
HDB3	<i>High-Density Bipolar-3 zeros</i>
HDSL	<i>High-bit-rate Digital Subscriber Line</i>
HZ	Hertz

ICMP	<i>Internet Control Message Protocol</i>
IP	<i>Internet Protocol</i>
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector.
Kbits/s	kilo bits por segundo
kHz	Kilohertz
LAN	<i>Local Area Network</i>
LCAS	<i>Link Capacity Adjustment Scheme</i>
LTU	<i>Line Termination Unit</i>
Mbps	Mega bits por segundo.
MIB	<i>Management Information Base</i>
mux	multiplexador
NMS	<i>Network Management System</i>
NTU	<i>Network Termination Unit</i>
PABX	<i>Private Automatic Branch Exchange</i>
PDH	<i>Plesiochronous Digital Hierarchy</i>
POTS	<i>Plain old Telephone Service</i>
pg.	página
RFC	Request for Comment
ROM	<i>Read Only Memory</i>
RTS	<i>Request To Send</i>
SDH	<i>Synchronous Digital Hierarchy</i>
SHDSL	<i>Single-Line High-bit-rate Digital Subscriber Line</i>
SMI	<i>Structure of Management Information</i>
SNMP	<i>Simple Network Management Protocol</i>
SNR	<i>Signal-to-Noise Ratio</i>
SLA	<i>Service Level Agreement</i>
TCP	<i>Transmission Control Protocol</i>
TDM	<i>Time Division Multiplexer</i>
Telecom.	Telecomunicações
TI	Tecnologia da informação
Tr	Tributário
TS	<i>Timeslot</i>

TTL	<i>Time-to-live</i>
UDP	<i>User Datagram Protocol</i>
UML	<i>Unified Modelling Language</i>
VLAN	<i>Virtual Local Area Network</i>
XTC	<i>External Transmit Clock</i>
WAN	<i>Wide Area Network</i>

LISTA DE FIGURAS

Figura 2.1: Modelo de Gerenciamento SNMP	21
Figura 2.2: Relacionamento de um gerente com objeto gerenciado.	22
Figura 2.3: Relacionamento entre gerente e agente.....	23
Figura 2.4: Formato das mensagens SNMP	24
Figura 3.1: Elementos de um sistema de gerência de rede.....	28
Figura 4.1: Pinagem da interface RS-232/V.24 num conector DB-9.....	34
Figura 4.2: Pinagem da interface RS-232/V.24 num conector DB-25.....	34
Figura 4.3: Conector da interface V.35	36
Figura 4.4: Sentidos dos sinais na interface V.35	37
Figura 4.5: Interface co-direcional	38
Figura 4.6: Interface com <i>clock</i> centralizado.	39
Figura 4.7: Estrutura dos quadros utilizados na interface E1 G. 703.....	40
Figura 4.8: Pinos da interface E&M.....	43
Figura 4.9: Frame G.shdsl - Estrutura dos blocos de dados	46
Figura 4.10: Utilização de banda no ADSL	48
Figura 6.1: Ferramenta <i>Device Compare</i>	58
Figura 6.2: Cadastro de Alarmes no <i>Device Compare</i>	59
Figura 6.3: Diagrama de Classes UML	61
Figura 6.4: Objetos da interface Tr-Eth do equipamento DmSTM-1 e interface E1 do Dm705 sendo comparados.....	63

LISTA DE TABELAS

Tabela 4.1: Características das interfaces pesquisadas	32
Tabela 4.2: Objetos monitorados pelo software de gerência para a interface V.35	37
Tabela 4.3: Objetos monitorados pelo software de gerência para a interface G.703	41
Tabela 4.4: Objetos monitorados pelo software de gerência para as interface FXS e FXO.....	42
Tabela 4.5: Objetos monitorados pelo software de gerência para a interface E&M.....	44
Tabela 4.2: Estrutura do Frame G. SHDSL.....	Erro! Indicador não definido.
Tabela 4.6: Objetos monitorados para a interface G.SHDSL	47
Tabela 4.7: Objetos monitorados para a interface ADSL.....	48
Tabela 4.8: Relação entre IEEE 802 e Modelo OSI da ISO.....	49
Tabela 4.9: Tecnologias de Redes utilizadas em redes locais. Fonte: IDC, Julho 2001	50
Tabela 4.10: Objetos monitorados para a interface Ethernet	50
Tabela 5.1: Comparação de objetos gerenciáveis entre algumas das interfaces pesquisadas.....	53

RESUMO

Com o desenvolvimento das redes de telecomunicações e o crescimento da heterogeneidade dos elementos presentes nessas redes, a tarefa de desenvolver o suporte de novas interfaces nos sistemas de gerência de redes de telecom ficou bastante complicada, pois cada interface e dispositivo de rede possuem suas peculiaridades, características e configurações.

Com o intuito de facilitar o monitoramento das novas interfaces de telecom nos sistemas de gerência de redes, esse trabalho visa identificar semelhanças entre as interfaces e dispositivos utilizados pelas operadoras de telecom no Brasil. O estudo foi realizado através de pesquisas junto a empresas que desenvolvem esses equipamentos, formando um grupo de objetos básicos para o suporte de novas tecnologias em telecom.

Para facilitar essa pesquisa na busca das semelhanças entre as interfaces de telecom, foi desenvolvida a ferramenta *Device Compare*, que a partir de uma base de dados de um sistema de gerência de redes de telecom, compara duas interfaces apresentando as similaridades entre os objetos gerenciados, mostrando o tipo do objeto (se é um objeto monitorado de configuração ou de estado), e o protocolo de comunicação utilizado para recuperar a informação.

A partir do resultado da pesquisa entre as interfaces de telecom utilizadas no Brasil e a comparação de objetos monitorados pelo sistema de gerência feito pela ferramenta *Device Compare*, foi desenvolvido um inventário de objetos presentes na maioria das interfaces de telecom que visa facilitar o monitoramento de novas interfaces nos sistemas de gerência, e, através do conhecimento de gerência das interfaces anteriores, criar o suporte para as novas interfaces e dispositivos que chegam ao mercado.

Palavras-Chave: Interfaces de Telecom, Interfaces de telecomunicação utilizadas no Brasil, Gerência de Redes, Gerência de configuração.

Characterization of new telecom's interfaces from devices and already managed interfaces.

ABSTRACT

With the development of telecommunications networks and the different types of network components, the task of supporting new technologies in network management systems became too complicated, due to the fact that every interface and every network element has different attributes, characteristics and configurations.

This work will identify similarities between devices and interfaces used by telecom providers in Brasil with the intention of facilitating the support of new technologies in network management systems. This research will be done on companies that develop these devices forming a basic set of objects to support new technologies.

In order to find these similarities, we developed the *Device Compare* which is a tool that accesses a database of network management system, and compares two interfaces showing the similarities among the monitored objects, presenting the type of the object, i.e. it shows if the object is monitored to derive status or if it has to be configured, showing the communication protocol used to retrieve the information.

From the result of this study on telecom interfaces used in Brasil and the comparison of objects monitored by the management system made by *Device Compare* tool we implemented a list with the most common objects in telecom interfaces. This list will be used to facilitate the support of new interfaces in management systems, and through the knowledge of old interfaces management, create the support to new interfaces and new devices that appear in the telecommunication market.

Keywords: Telecom interfaces, Telecom interfaces used in Brasil, Network Management, Configuration Management.

1 INTRODUÇÃO

As mudanças das características das redes de telecomunicação, de pequenas redes de transmissão para grandes redes espalhadas geograficamente; de redes homogêneas para redes heterogêneas, bem como a evolução da tecnologia dos equipamentos de telecomunicação, tem dificultado em muito o desenvolvimento de software de gerência.

Com o rápido crescimento das redes de telecomunicação e o desenvolvimento de interfaces e protocolos diferentes associados a cada nova tecnologia desenvolvida, surge a necessidade de desenvolver mecanismos que facilitem o gerenciamento dessas novas interfaces pelos sistemas de gerência de telecom já existentes e instalados nas operadoras, visto que cada tecnologia possui várias características e dados diferentes a serem gerenciados.

Grandes equipes de desenvolvimento são necessárias para desenvolver o suporte a essas novas tecnologias nos softwares de gerência, que envolvem a criação de novas janelas de configuração e visualização de estado, coerências de configuração, suporte a novos eventos e alarmes, criação de relatórios, etc. Porém, antes de chegar à fase de desenvolvimento do suporte à nova tecnologia que chega ao mercado, é necessário conhecer e identificar os parâmetros configuráveis e os objetos que denotarão falhas e situações de erro em cada interface. Esta tarefa envolve tempo de analistas e programadores, que poderiam estar desenvolvendo outras ferramentas necessárias à gerência de redes de telecom, como provisionamento, correlação de eventos e falhas, e melhorias nos próprios sistemas de gerência.

Para facilitar o desenvolvimento do suporte às novas tecnologias de telecom, este trabalho tenta identificar as características e semelhanças entre as diversas interfaces de telecom utilizadas no Brasil, para que se obtenha um conjunto de objetos que sejam gerenciados na maioria, ou em um grupo grande das interfaces. De posse desses objetos, será possível iniciar o desenvolvimento da gerência de uma nova interface de telecom, a partir de um grupo de objetos em comum. Outro objetivo do trabalho é identificar semelhanças entre as interfaces, para que dessa maneira a construção da gerência de uma nova interface, seja baseada numa interface antiga já gerenciada e conhecida pelo sistema. Conhecendo as diferenças e similaridades entre as interfaces, torna-se possível desenvolver algoritmos e estruturas de dados, que facilitam a entrada desses equipamentos nos softwares de gerência já existentes e, instalados nas operadoras de telecom, ou, até mesmo, um padrão para o desenvolvimento do suporte a novas interfaces e equipamentos, visando facilitar o “*upgrade*” dos softwares de gerência.

Para que seja possível selecionar os atributos em comum entre as interfaces de telecom utilizadas no Brasil, e se conheçam as semelhanças entre essas interfaces,

foram feitas pesquisas nas recomendações, manuais e padrões que descrevem as interfaces, tentando sempre identificar objetos e parâmetros que sejam configuráveis ou atributos interessantes para a gerência de falhas.

Para facilitar essa comparação, foi desenvolvida uma ferramenta, o software *Device Compare*, que apresenta os objetos monitorados para cada uma das interfaces já gerenciadas pelo sistema de gerência da empresa Datacom-Telemática. A ferramenta acessa a base de dados do sistema e apresenta os objetos gerenciados, separando-os em objetos de configuração e objetos de estado, podendo ainda comparar interfaces duas a duas.

O trabalho está organizado como segue:

No capítulo dois, foi feita uma revisão das necessidades de um sistema de gerência, revisão do protocolo SNMP e problemas que ele apresenta para a gerência de redes de telecom. No terceiro capítulo, apresentamos as dificuldades e o tempo gasto por empresas que desenvolvem softwares de gerência de telecom, no suporte de novas interfaces e novos dispositivos, diminuindo assim, o tempo para o desenvolvimento de novas funcionalidades próprias de gerência de redes.

No capítulo quatro, são apresentados as interfaces de telecom pesquisadas, com suas características, peculiaridades, objetos de configuração e quais objetos identificam o estado de operação. Ao final do capítulo, apresentamos as semelhanças entre os objetos identificados de cada interface. Os resultados apresentados nesse capítulo também foram obtidos a partir do uso da ferramenta desenvolvida.

No quinto capítulo apresentamos o software desenvolvido, descrevendo-o em detalhes, apresentando sua estrutura e a estrutura da base de dados utilizada. No sexto capítulo, são apresentados estudos de caso utilizando a ferramenta *Device Compare*, para um melhor entendimento dos resultados que podem ser obtidos utilizando o software. Na conclusão apresentamos as dificuldades encontradas no desenvolvimento do trabalho e a colaboração que o estudo pode trazer para o desenvolvimento de softwares de gerência de equipamentos de telecomunicações, mostrando ainda os trabalhos que podem ser derivados a partir da pesquisa e da própria ferramenta desenvolvida.

2 SISTEMAS DE GERÊNCIA

A necessidade do uso de um sistema de gerência surgiu com o crescimento das redes de computadores. No início, quando as redes eram compostas de poucos computadores, todos eles utilizando o mesmo sistema operacional e tendo hardwares muito semelhantes, a verificação e posterior diagnóstico de erros nas máquinas podiam ser feitos *in loco*, já que as redes restringiam-se a laboratórios ou no máximo um único prédio.

Ainda nos primeiros avanços das redes de computadores, a verificação das máquinas na rede podia ser feita através do programa *ping*, que verificava se os pacotes ICMP enviados de uma determinada máquina estavam chegando ao *host* de destino. O tempo para o recebimento dos pacotes também podia ser diagnosticado através desse simples programa, além do número de nós (*hops*) pelo qual os pacotes enviados precisaram passar para chegar ao seu destino.

Com a posse apenas das informações geradas pelo programa *ping*, o usuário podia detectar o atraso na chegada dos pacotes, a perda de pacotes e *loops* gerados pelas rotas da rede.

Com o advento do programa *TraceRoute*, já tornou-se possível conhecer o caminho que um pacote IP percorria até chegar ao seu destino. O programa *TraceRoute* baseava-se no campo TTL (*time-to-live*). A estação que executava o programa, enviava um *ping* com campo TTL = 1 e, através da resposta ICMP gerada no roteador, já que o campo TTL do pacote tinha chegado ao valor 0, identificava o primeiro roteador pelo qual os pacotes para a estação de destino passavam. Utilizando o programa *ping* com o campo TTL com os valores subsequentes, era possível determinar toda a rota até a máquina de destino [Tanenbaum].

Com o crescimento das redes TCP/IP e o advento da Internet ao longo da década de 80, tornou-se impossível gerenciar os equipamentos de rede sem o uso de ferramentas e protocolos voltados especificamente para a gerência de redes. A demora no surgimento de soluções abertas baseadas no modelo OSI, fez com que um grupo de engenheiros decidissem elaborar uma solução baseada num novo protocolo, o protocolo *SNMP* (*Simple Network Management Protocol*), que obtivesse de forma simples e rápida as informações necessárias para gerenciar os equipamentos das redes que continuavam a crescer. O protocolo SNMP foi definido na RFC 1157. Começava a ser criado o que conhecemos hoje como Gerência de Redes.

“O objetivo da gerência de redes é garantir aos usuários acesso aos serviços oferecidos pela rede com a qualidade de serviço esperada”.

O modelo de referência ISO/OSI subdividiu a gerência de redes em cinco grandes áreas funcionais: Gerência de falhas, de configuração, de performance, de segurança e

de contabilidade (KLERER, 1999). Essas funções têm sido comumente aplicadas para desenvolver uma gerência reativa de redes, ou seja, estão sendo utilizadas na detecção de problemas na rede e na busca de uma solução quando esses problemas ocorrem.

- Gerência de falhas (*fault management*)
- Gerência de contabilidade. (*accounting management*)
- Gerência de configuração (*configuration management*)
- Gerência de performance (*performance management*)
- Gerência de segurança (*security management*)

Como o objetivo do trabalho é apresentar e verificar semelhanças apenas entre objetos de configuração e de estado, apresentaremos somente os conceitos de gerência de falhas, gerência de configuração e gerência de contabilidade (alguns desses objetos são monitorados no *polling de status* de sistemas de gerência).

2.1 Gerência de Falhas

O objetivo da gerência de falhas é identificá-las o mais rápido possível e apontar causas, para que ações corretivas sejam tomadas para voltarmos a uma situação de normalidade na rede.

Para manter a operação apropriada de uma rede complexa, um gerente de rede precisa cuidar do sistema como um todo, e cada componente da rede individualmente.

Para entendermos o conceito de gerência de falhas, é fundamental entender o significado de uma falha. Falhas devem ser diferenciadas de erros. Uma falha é uma condição anormal que requer uma ação da gerência para ser reparada, enquanto um erro é um evento ocorrido na rede. Uma falha é geralmente indicada por uma anormalidade na operação do sistema ou por uma quantidade de erros excessivos. Por exemplo: se uma linha de comunicação é fisicamente cortada, nenhum sinal vai passar por essa linha. Um corte em um cabo pode causar grandes distorções, então haverá uma taxa persistente de erros de bits. Alguns erros, por exemplo, um erro de bit em uma linha de comunicação, podem ser considerados normais e não serem considerados falhas. Normalmente esse tipo de erro pode ser compensado utilizando-se um mecanismo de controle de erro existente em vários protocolos de comunicação (STALLINGS, 1999).

A monitoração da rede é o mais importante aspecto de uma gerência de rede automatizada. Embora muitos sistemas de gerência de rede, devido a uma falta de mecanismos de segurança, não incluam facilidades de controle, todos os sistemas de gerência incluem um componente de monitoração da rede.

A maioria dos sistemas executa um *polling* nos equipamentos gerenciados, para detectar situações de erro e ilustrar o problema de forma gráfica ou textual. A maioria desses softwares permite que as mensagens de erro sejam configuradas pelo usuário (gerente da rede), que também pode configurar a maneira como ele será avisado de que existe algum problema na rede.

Em um ambiente de rede complexo, localizar e diagnosticar falhas pode ser uma tarefa difícil. A seguir, uma lista de problemas específicos associados com observações sobre as falhas.

- Falhas não observáveis: certas falhas são dificilmente identificadas localmente. Por exemplo, a existência de um *deadlock* entre um processo distribuído pode não ser identificável localmente. Outras falhas podem não ser observadas porque a empresa responsável pela venda do equipamento não providenciou ferramentas para a apresentação da falha ao usuário (STALLINGS, 1999).
- Falhas parcialmente observáveis: a falha em um nodo pode ser observável, mas a observação pode ser insuficiente para identificar claramente o problema. Por exemplo, um nodo pode não estar respondendo devido a uma falha na comunicação entre um equipamento anexo ao equipamento observado. (STALLINGS, 1999).
- Observações incertas: mesmo quando observações detalhadas de falhas são possíveis, pode haver incertezas ou mesmo inconsistências associadas às observações. Por exemplo, a falta de resposta de um equipamento remoto pode significar que o equipamento está sobrecarregado, e não que ele tenha sido desligado por algum motivo.

Uma vez que as falhas são observadas, é necessário isolar o problema para um componente particular.

Normalmente os equipamentos gerenciados enviam *traps* avisando da ocorrência dos erros na rede (quando o problema não afeta o envio das informações de gerência) à medida que os erros vão ocorrendo. A partir da chegada desses eventos (*traps*), o sistema de gerência executa o *polling* para verificar a nova situação do equipamento, verificando um grupo pré-definido de objetos gerenciáveis e definindo o seu estado operacional para a gerência.

O usuário final espera uma resolução rápida e confiável para os eventuais problemas na sua rede. A maioria dos usuários tolera pequenos problemas na sua rede, mas quando esses se tornam mais frequentes, ou quando tem uma severidade maior, o usuário final espera receber imediatamente a notificação do problema para que possa ser resolvido o mais rápido possível. Para possibilitar esse nível de resolução de falhas, são necessários mecanismos rápidos e confiáveis de detecção e diagnóstico de falhas. O impacto e a duração das falhas são, muitas vezes, minimizados pelo uso de componentes redundantes e, através do uso de rotas de comunicação alternativas, para dar a rede um certo nível de tolerância a falhas. As funções de tolerância a falhas podem, por sua vez, serem redundantes para aumentar a confiabilidade da rede.

O usuário espera se manter atualizado em relação ao estado da rede, inclusive a respeito dos processos que são executados paralelamente pelo sistema de gerência, como *backup* da base de dados, exportação de eventos antigos, quantidade e tempo de *pollings* nos equipamentos da rede, etc. O usuário também espera de um sistema de gerência, funcionalidades de testes nos equipamentos e interfaces da rede, para verificar o funcionamento dos dispositivos, além de *logs* das ações do próprio usuário nesses equipamentos.

Deve ser possível gerar relatórios periódicos das falhas na rede de dados (relatório de alarmes), relatório de eventos na gerência, relatório de ativações de configuração, onde devem ser apresentados a hora da ativação no equipamento e o nome do usuário que efetuou a ativação. Relatório de performance das interfaces que disponibilizam estes dados também são comumente requisitados pelas operadoras de telecomunicações,

umentando significativamente a importância dos relatórios nos sistemas de gerência de falhas.

Após corrigir uma falha e restaurar o funcionamento normal do sistema, o serviço de gerência de falhas deve verificar se o problema está realmente resolvido e se nenhum novo problema foi introduzido.

Além de todos esses aspectos fundamentais, o sistema de gerência de falhas não deve afetar de forma significativa a performance da gerência nos usos de *pollings* e acesso para testes nos dispositivos (STALLINGS, 1999).

Em termos teóricos, o modelo ideal para atualização de estado dos equipamentos da gerência se daria através da recepção de eventos, que precisariam ser gerados no momento da alteração do estado no dispositivo, e, cada evento (*trap*), teria os seus objetos alterados no equipamento e nas suas interfaces com os respectivos novos valores. Essa nova situação precisa ser automaticamente refletida para o gerente da rede nos mapas e janelas de eventos da gerência e outros sistemas como envio de mail ou toque de alarme sonoro disparados se o sistema de gerência estiver configurado para isso.

2.2 Gerência de Configuração

A gerência de configuração é, provavelmente, a parte mais importante de um sistema de gerência, pois não é possível gerenciar corretamente uma rede utilizando um software onde não se possa alterar a configuração dos elementos dessa rede.

A gerência de configuração está preocupada com a inicialização, a manutenção e o desligamento de componentes e subsistemas da rede e seus recursos de comunicação.

A gerência de configuração controla o processo de inicialização, identificando e especificando as características dos recursos e componentes que irão constituir a rede. Os recursos gerenciados incluem recursos físicos (por exemplo, um servidor ou um roteador) e objetos lógicos (por exemplo, um *timer* de retransmissão do nível de transporte).

Através da gerência de configuração, podem ser especificados valores iniciais ou valores padrão para atributos dos recursos da rede. Para que esses possam iniciar a sua operação no estado desejado, possuam os corretos parâmetros de funcionamento e tenham o relacionamento desejado com outros componentes da rede.

Na gerência de rede de telecom, modems, multiplexadores e roteadores têm suas portas, interfaces e CPUs configurados antes do início da transmissão de dados de clientes, de forma que, quando os circuitos de transmissão forem criados, esses equipamentos já estejam preparados para o início da transmissão.

Enquanto a rede está em operação, a gerência de configuração é responsável por monitorar a configuração e fazer mudanças em resposta a comandos do usuário ou em resposta a outras funções de gerência da rede. Por exemplo, se as funções de monitoração de performance detectam que o tempo de resposta está sendo degradado devido a um incorreto balanceamento de carga, a gerência de configuração pode ajustar a configuração de modo a corrigir o balanceamento de carga. Similarmente, se a gerência de falhas detecta e isola uma falha, a gerência de configuração pode alterar a configuração para “by-passar” essa falha.

A gerência de configuração inclui as seguintes funções:

- Define informações de configuração;
- Seta e modifica valores de atributos;
- Define e modifica o relacionamento entre os elementos da rede;
- Inicializa e termina operações na rede;
- Distribui software;
- Examina valores e relacionamentos;
- Gera relatórios de estado das configurações.

Os dois últimos itens da lista são funções de monitoração de configuração. Através de uma interação de pergunta e resposta, uma estação de gerência pode examinar as informações de configuração mantidas por um determinado agente.

Quando uma falha é apontada na rede pelo sistema de gerência, algumas configurações devem ser feitas nos elementos da rede para que o funcionamento adequado da rede possa ser restabelecido.

Mudanças, adições e remoções na rede precisam ser coordenadas pelo sistema de gerência. Periodicamente o sistema de gerência ainda deve verificar a configuração dos nodos da rede para assegurar-se que a configuração da rede ainda é conhecida.

2.3 Gerência de Contabilidade

Gerência de contabilidade é uma maneira de contabilizar o acesso e a utilização de recursos da rede por parte dos usuários. Os requisitos para essa função variam bastante. Em alguns ambientes, a contabilidade pode ser gerada de uma forma bem natural. Por exemplo: um sistema de contabilidade pode ser utilizado apenas para verificar a média de uso dos recursos e para determinar o custo de cada recurso compartilhado. Em outros casos, como na gerência de redes de telecomunicações (que oferecem um serviço público) e em sistemas com apenas usuários internos, a utilização da rede precisa ser contabilizada por conta, por projeto ou mesmo individualmente por usuário para fins de bilhetagem. Nesse último caso, a informação recuperada pelo monitor do sistema precisa ser mais detalhada e mais precisa do que as informações recuperadas para todo o sistema.

Exemplos de recursos que podem estar sujeitos à monitoração de contabilidade:

- Facilidades de comunicação: LANs, WANs, linhas alugadas, linhas discadas e sistemas de PABX;
- Hardware: Estações e servidores;
- Software e sistemas: Aplicativos e softwares utilitários em servidores, *data-centers* e sistemas para o usuário final;
- Serviços: incluem todas as comunicações de âmbito comercial e servidores de informação disponíveis para os usuários da rede.

Para qualquer tipo de recurso, os dados de contabilidade recuperados estão baseados nos requisitos da organização. Por exemplo: os seguintes dados de contabilidade relacionados à comunicação podem ser recuperados e mantidos para cada usuário.

- Identificação do usuário: provido pelo originador de uma transação ou requisição de serviço;
- Receptor: identifica o componente da rede ao qual uma conexão é realizada ou tentada;
- Número de pacotes: contagem dos dados transmitidos ou recebidos;
- Nível de segurança: identifica a transmissão e suas prioridades;
- Marcação de tempos: associado com cada transmissão e evento processado (por exemplo: horário do início de uma transmissão e horário do final da transmissão);
- Códigos de estado da rede: indica a natureza do mau funcionamento ou erro detectados;
- Recursos Utilizados: indica quais recursos foram invocados pela transmissão ou evento detectado.

2.4. Protocolo SNMP

O modelo de gerenciamento de redes baseado no protocolo SNMP (*Simple Network Management Protocol*), refere-se a um conjunto de padrões para gerenciamento de redes, incluindo o protocolo SNMP, a especificação da estrutura de dados, e o conjunto de objetos de dados. Foi adotado como padrão para redes TCP/IP em 1989 e é amplamente utilizado nos dias atuais.

Este protocolo tem como premissa a flexibilidade e a facilidade de implementação, também em relação aos produtos futuros. Sua especificação está contida no RFC 1157.

O SNMP é um protocolo de gerência definido em nível de aplicação, utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. Os dados são obtidos através de requisições de um gerente, a um ou mais agentes utilizando os serviços do protocolo de transporte UDP (*User Datagram Protocol*) para enviar e receber suas mensagens através da rede.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado da rede, em tempo real, podendo ser utilizado para gerenciar diferentes tipos de sistemas.

Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP. Portanto, SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB e a aplicação de gerência, e é também o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração do valor de um objeto, a obtenção dos valores de um objeto e suas variações.

A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas características.

O funcionamento do SNMP é baseado em dois dispositivos, o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam

informações referentes ao seu estado atual, ficando estas disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

Fazem parte do modelo de gerenciamento SNMP:

- Uma ou mais estações de gerenciamento contendo aplicações de gerenciamento (gerentes);
- Um ou mais nodos gerenciados contendo uma entidade de processamento denominada agente;
- As informações de gerenciamento (objetos) presentes em cada nodo gerenciado (agente), que descrevem a configuração, o estado, as estatísticas e controlam as ações do nodo gerenciado.

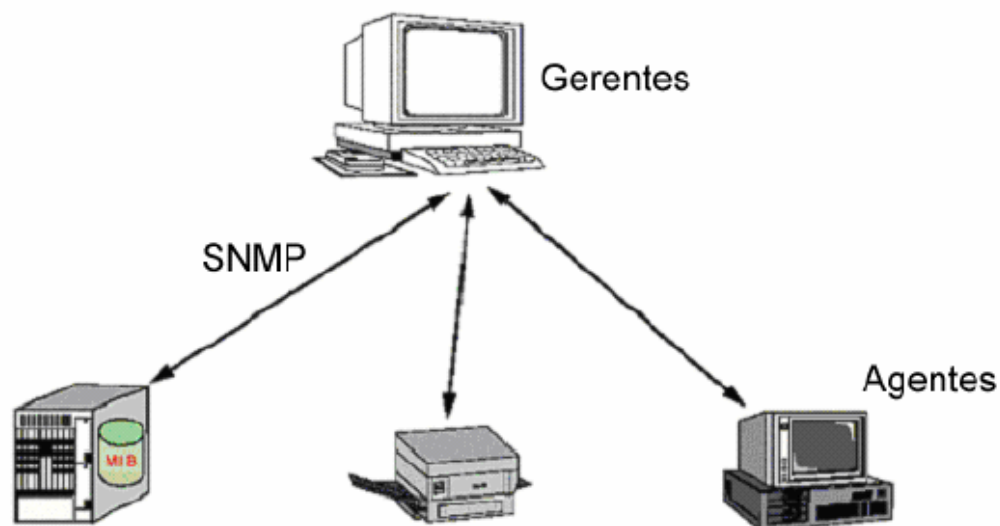


Figura 2.1: Modelo de Gerenciamento SNMP

2.4.1 O Agente

É um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina. As funções principais de um agente são:

- Atender as requisições enviadas pelo gerente;
- Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado.

O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC (*Remote Procedure Call*) para o controle das informações da máquina.

2.4.2 O Gerente

É um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.

É no gerente que são instalados os sistemas de gerência responsáveis por monitorar centenas de outros agentes de rede, que podem variar desde computadores, passando por multiplexadores, roteadores e até impressoras.

A figura 2.2 mostra como funciona o relacionamento de um gerente com o objeto gerenciado.

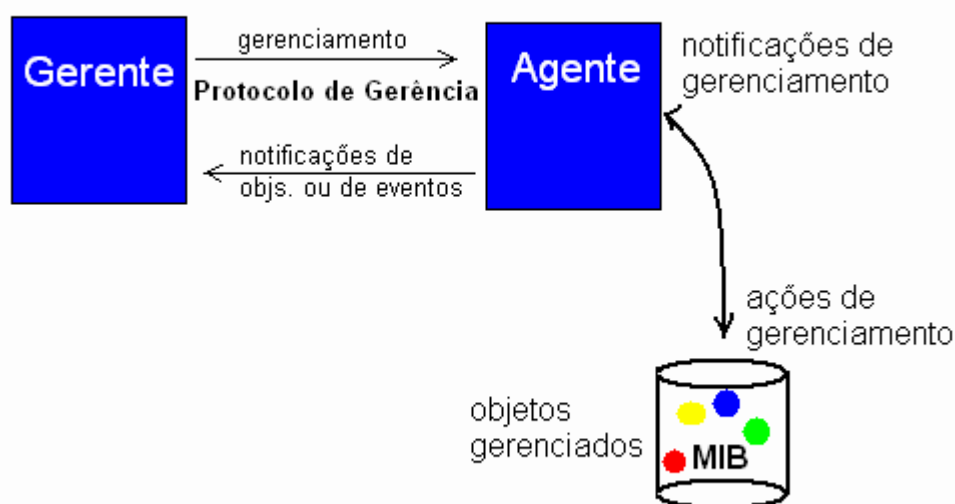


Figura 2.2: Relacionamento de um gerente com objeto gerenciado.

A gerência através do protocolo SNMP baseia-se no conceito de objeto gerenciado. Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados e as estruturas dos dados resultantes são objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso.

O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas, enquanto o agente fica responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

A figura 2.3 mostra o relacionamento entre gerente e agente baseado no modelo TCP/IP.

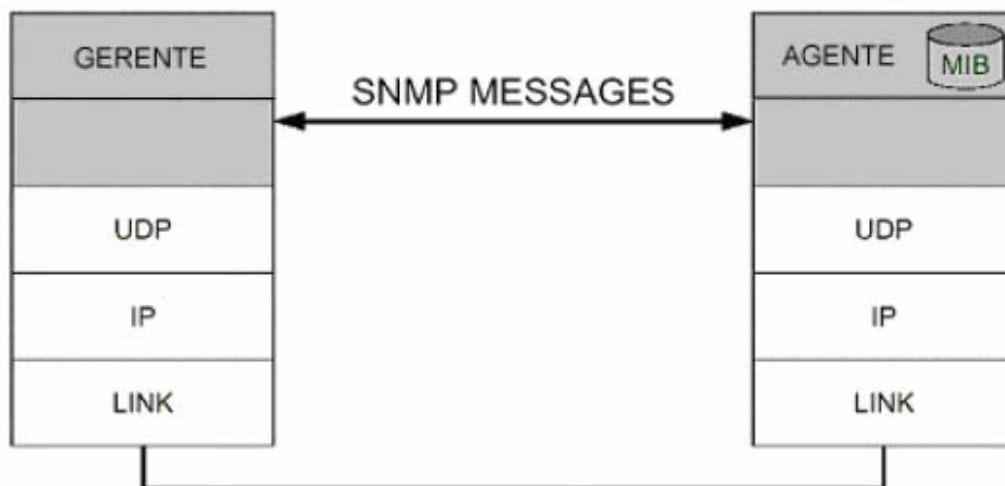


Figura 2.3: Relacionamento entre gerente e agente.

Dessa forma, o conjunto de dados gerenciados que cada equipamento de rede suporta é definido através de especificações denominadas MIB (*Management Information Base*). As MIBs são descritas utilizando a notação ASN.1 (*Abstract Syntax Notation One*), que especifica como as informações serão codificadas. Um agente pode suportar um ou mais módulos MIB, incluindo as MIBs padrões, especificadas como parte do SNMP, e as MIBs proprietárias, definidas pelos fabricantes dos equipamentos para seus produtos específicos.

A RFC 1066 apresentou a primeira versão de uma MIB, a MIB I. Este padrão explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas na pilha de protocolos TCP/IP. A evolução aconteceu com a RFC 1213 que propôs uma segunda MIB, a MIB II, para uso baseado na pilha de protocolos TCP/IP.

A MIB II que é considerada uma evolução da MIB I, fornece informações gerais de gerenciamento sobre um determinado equipamento gerenciado. Através da MIB II podemos obter informações tais como: números de pacotes transmitidos, estado da interface, entre outras.

As MIBs experimentais são aquelas em que seus componentes (objetos) estão em fase de desenvolvimento e teste. Em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

As MIBs privadas são aquelas em que seus componentes fornecem informações específicas dos equipamentos gerenciados. Cada empresa obtém um ramo da mib *enterprise* para colocar suas MIBs privadas. A falta de padronização das MIBs privadas é uma das principais causas da dificuldade de se desenvolver um software de gerência genérico para todos os equipamentos de rede. Os equipamentos de telecom, devido a suas peculiaridades, são os equipamentos que mais fazem uso de MIBs privadas.

As regras de construção das estruturas da MIB são descritas através da SMI (*Structure of Management Information*). A estrutura de informações de gerência SMI é um conjunto de documentos que definem:

- Forma de identificação e agrupamento das informações;
- Sintaxes permitidas;

- Tipos de dados permitidos.

Os objetos de uma MIB são especificados de acordo com a ASN.1 - *Abstract Syntax Notation One*. A notação sintática abstrata, é uma forma de descrição abstrata de dados, com o objetivo de não levar em consideração a estrutura e restrições do equipamento no qual está sendo implementada. Para cada objeto são definidos: nome, identificador, sintaxe, definição e acesso. As instâncias do objeto são chamadas de variáveis.

- O Object Name é o nome do objeto, é composto por uma string de texto curto.
- O Object Identifier é o identificador do objeto, é formado por números que são separados por pontos.
- A sintaxe do objeto descreve o formato ou o valor da informação. Ela pode ser uma sintaxe do tipo simples que pode ser um inteiro, uma string de octetos, um *Object Identifier* ou um valor nulo. Pode ser também uma sintaxe de aplicação podendo ser um endereço de rede, um contador, uma medida ou um intervalo de tempo.

2.4.3 Formato das mensagens SNMP

As informações são trocadas entre a estação gerenciadora (gerente) e a máquina gerenciada (agente) na forma de mensagens SNMP. Cada mensagem inclui o número da versão do SNMP, um nome de comunidade (utilizada para autenticar o gerente no agente) e um dos cinco tipos de unidades de dado do protocolo, como mostrado na figura 2.4.

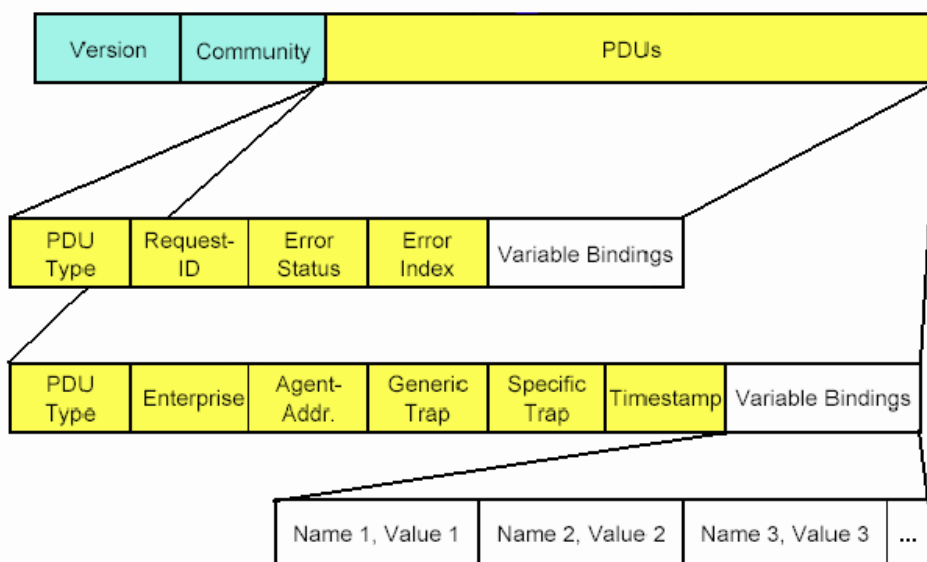


Figura 2.4: Formato das mensagens SNMP

2.4.4 Operações SNMP

As operações em SNMP são limitadas a recuperar os valores do conjunto de dados gerenciados, modificar estes valores e avisar a ocorrência de um evento. Existem quatro tipos de operações no protocolo SNMPv1:

- *getRequest*: operação para recuperação do valor de uma informação gerenciada (objeto) específica. O nodo gerenciado (agente) responderá com a mensagem *GetResponse*;
- *getNextRequest*: operação para recuperação dos valores de informações gerenciadas seqüenciais em uma MIB. O nodo gerenciado responderá com a mensagem *GetResponse*;
- *setRequest*: operação para modificar o valor de uma informação gerenciada específica pertencente à MIB. O nodo gerenciado responderá com a mensagem *GetResponse*;
- *trap*: mensagem de gerenciamento enviada pelo nodo gerenciado informando a ocorrência de um evento significativo.

As operações permitidas para os objetos gerenciados são definidas através de direitos de acesso, indicados nas MIBs através da cláusula “*ACCESS*” em cada objeto gerenciado. As categorias de acesso permitidas são:

- *read-only*: permite apenas que o objeto seja lido pela estação de gerenciamento (utilizando operações *getRequest* e *getNextRequest*). Não permite que seja feita uma operação *setRequest*;
- *read-write*: permite que o objeto seja lido (*getRequest* e *getNextRequest*) e modificado (*setRequest*) pela estação de gerenciamento;
- *write-only*: permite que o objeto seja modificado. Não permite que seja lido.
- *not-accessible*: não permite que a estação de gerenciamento efetue operações de leitura e escrita.

2.4.5 Esgotamento do protocolo SNMP para gerência de equipamentos SDH

O protocolo SNMP é o protocolo de gerência de fato para gerência de redes locais e redes de telecom, devido a sua simplicidade de uso e implementação e sua popularidade.

Nos últimos anos, as empresas que desenvolvem equipamentos de comunicação mais complexos, com milhares de portas e características configuráveis, começaram a adotar outros protocolos de comunicação, às vezes, até proprietários, devido a dificuldade do protocolo SNMP de transmitir uma quantidade maior de informação, como as diversas configurações possíveis de serem alteradas dos equipamentos SDH de maior hierarquia como STM-4 e STM-16.

Outro problema latente são as grandes falhas de segurança do protocolo, que pode dar acesso a equipamentos no *backbone* da Internet, já que as comunidades de leitura e escrita passam em claro na rede.

Com a adoção de múltiplos protocolos de gerência de redes e, inclusive o desenvolvimento de alguns protocolos proprietários, a tarefa de gerência de novos dispositivos sofreu outro baque, e o tempo despendido para suportar um novo protocolo de gerência ou mesmo identificar como são estruturados os dados de gerência de cada fabricante e a maneira em que eles foram disponibilizados para gerência aumentou enormemente.

A solução para padronizar e facilitar o suporte a esses novos dispositivos, passa por levantar os objetos gerenciados padrões, já que não existe mais a forma de como recuperá-los do equipamento gerenciado, as possibilidades de configuração de cada equipamento e interface, definir coerências de configuração (entendendo cada interface), de modo a possibilitar as configurações possíveis de serem ativadas e criar uma base de dados com os objetos gerenciados para cada interface, variando de equipamento para equipamento e de fabricante para fabricante apenas a forma como esses dados serão recuperados e ativados.

O desenvolvimento desse tipo de estrutura e o levantamento desses dados, colocando-os a disposição na base de dados do software de gerência, permitiria um gasto muito menor no suporte a novas interfaces, e a possibilidade da utilização do tempo de cada desenvolvedor na criação de novas funcionalidades próprias da gerência de redes de telecom.

3 SOFTWARES DE GERÊNCIA DE TELECOM

Os sistemas de gerência de redes de telecomunicações tem um objetivo mais específico, gerenciar equipamentos responsáveis por trafegar dados de operadoras de telecom, onde uma falha por alguns instantes em algum nodo da rede, pode custar muito dinheiro devido aos contratos de alta disponibilidade firmado entre operadoras e seus clientes, as SLAs (*Service Level Agreement*).

Atualmente, podemos definir software de gerência de telecom como uma coleção de ferramentas de monitoração e controle, que utilizando uma interface amigável com o usuário (GUI), realiza a maioria ou todas as tarefas de gerência de redes mostradas anteriormente nos equipamentos de telecomunicações, tendo o cuidado de informar as falhas na rede ao operador do sistema de gerência da forma mais rápida possível e através de várias maneiras, para que se tenha um controle da interrupção na transmissão de dados na rede e um histórico para posterior consulta e análise das tendências de erros na rede.

Normalmente, o sistema de gerência é composto do software de gerência propriamente dito, um servidor de base de dados, que pode ou não ser executado na mesma máquina do software de gerência e, algumas vezes, um servidor WEB, que também pode ser executado numa estação diferente do servidor principal onde roda o software de gerência.

Muitas vezes, o sistema de gerência pode ser composto de um servidor principal e máquinas consoles, que irão acessar a máquina principal e apresentar a rede de telecom ao operador. Outras vezes, as consoles são substituídas, utilizando-se um sistema de emulação de terminal.

O software propriamente dito, ainda faz uso de diversos protocolos de comunicação como o SNMP, para acessar os nodos gerenciados e comunicar-se com outros sistemas de gerência que por ventura estejam integrados (como um sistema de correlação de eventos ou outros sistemas de gerência de mais alto nível).

O sistema de gerência é desenvolvido para que se possa ter uma visão de toda a rede, como se ela fosse uma entidade única, com os endereços de rede e rótulos apontando para cada atributo da rede (nodos gerenciados) e as relações entre cada atributo gerenciado (links, circuitos comutáveis, etc).

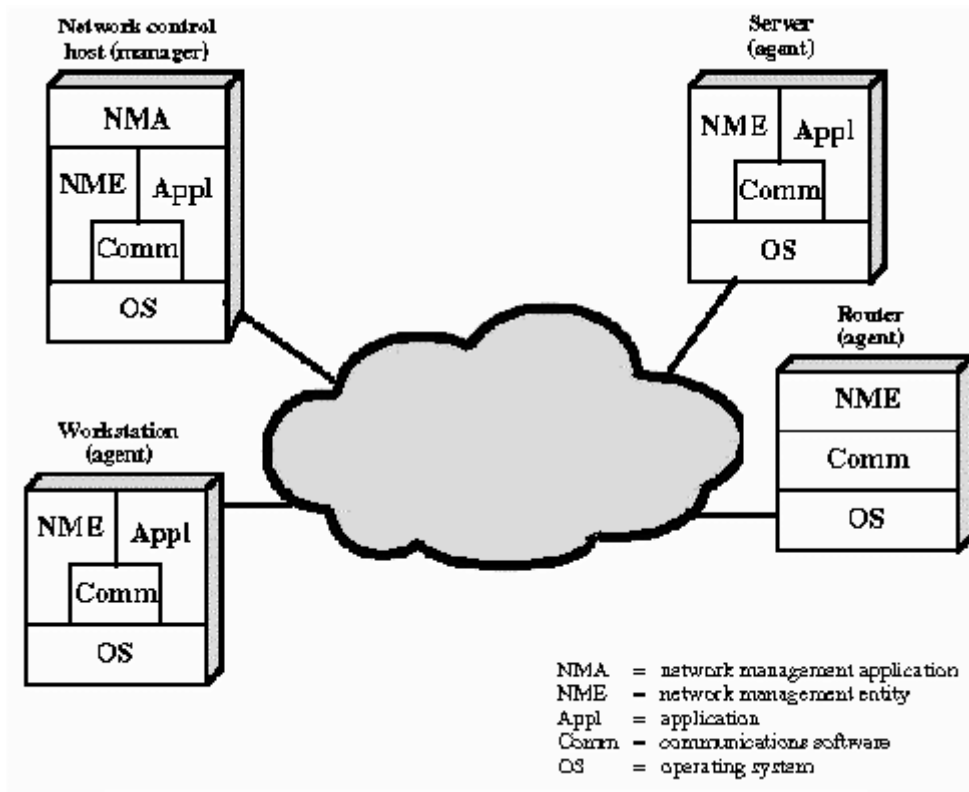


Figura 3.1: Elementos de um sistema de gerência de rede

Por fim, os sistemas de gerência são capazes de receber eventos enviados pelos nodos da rede e informar ao usuário o acontecimento desses eventos, da forma previamente escolhida pelo usuário e apresentando relatórios periódicos desses eventos da rede.

3.1 Desenvolvimento de softwares de gerência de telecom.

Os softwares de gerência de redes de telecomunicação, normalmente são desenvolvidos pelas próprias empresas que desenvolvem os equipamentos de comunicação de dados. Normalmente, esses equipamentos possuem uma interface CLI (*Command Line Interface*) a partir da qual é possível configurar o equipamento via interface serial (utilizando o padrão RS-232) ou, através do software *telnet*, pois a empresa que vende os equipamentos precisa fornecer um software que possibilite configurar e verificar os alarmes ativos para esses dispositivos.

Com o advento das interfaces gráficas para gerência de redes, as próprias empresas fornecedoras dos produtos de telecom começaram a desenvolver seus softwares de gerência, aproveitando assim, o conhecimento dos engenheiros responsáveis pelo desenvolvimento de interfaces/equipamentos e, desenvolvendo dessa maneira, uma equipe de programadores com conhecimento da configuração dos equipamentos e do desenvolvimento do software de gerência.

O trabalho de encontrar os objetos de configuração que poderão ser alterados via software de gerência e os objetos de estado que deverão ser monitorados para apresentar eventuais problemas ao gerente da rede, é feito pelos engenheiros que desenvolvem cada nova tecnologia, juntamente com as pessoas que desenvolvem o software de gerência dos equipamentos. Muitas vezes, esses engenheiros não possuem conhecimento sobre gerência de redes, estando acostumados apenas a configurar e

verificar o estado de um único equipamento ou interface (justamente aquele equipamento ou interface desenvolvido pelo engenheiro).

Para desenvolver o suporte à gerência remota de novos equipamentos e interfaces de telecom, são identificados objetos que irão derivar a situação de cada interface, objetos que possibilitarão alterar as configurações de operação, objetos que irão disponibilizar testes remotos para o usuário ou objetos que identificarão cada interface e cada equipamento.

Para identificar falhas ou mesmo configurar parâmetros de equipamentos presentes nas redes das operadoras de telecomunicação, existe um grupo de objetos que os softwares de gerência monitoram para apresentar as falhas ocorridas na rede ou disponibilizar ao usuário para possibilitar a configuração desses equipamentos.

Cada interface utilizada nas redes de telecom possui suas características e peculiaridades como foi visto no capítulo anterior. Porém, deve existir um grupo grande de objetos que são respondidos para os softwares de gerência que estão presentes em todas as interfaces ou na maioria delas.

Visando auxiliar na detecção dos objetos gerenciáveis das interfaces de telecom, e buscar essas semelhanças entre os objetos respondidos para cada uma delas, foi desenvolvido um software, tendo como base as informações contidas no banco de dados do software de gerência da empresa DATACOM. O software faz a comparação entre os objetos respondidos por cada interface, demonstrando as semelhanças e as diferenças entre cada interface.

Com base nas descrições e recomendações das interfaces pesquisadas, foram encontradas várias características e possíveis maneiras de configurá-las em comum, que na maioria das vezes são transformadas em objetos remotamente gerenciáveis, via protocolos de gerência como SNMP. Objetos esses que devem ser gerenciados para facilitar a gerência de redes de telecom por parte de gerentes de rede, através dos softwares de gerência de redes ou NMSs (*Network Management Systems*).

Buscando facilitar o desenvolvimento do suporte de novas interfaces nos softwares de gerência de redes de telecom, iremos demonstrar o resultado da pesquisa que tentou relacionar as semelhanças entre as interfaces de telecom utilizadas atualmente, ou seja, objetos que podem ser verificados ou configurados por todas as interfaces ou na sua maioria. De posse desses dados, será possível identificar falhas e efetuar modificações na configuração de novas interfaces nos softwares de gerenciamento, bastando inserir na base de dados desses softwares os objetos que, com certeza, a interface possui nas suas bases de gerenciamento.

No entanto, as operadoras de telecom começaram a ter dificuldades na utilização de vários softwares de gerência ao mesmo tempo, visto que são utilizados equipamentos de diversas empresas e, ao mesmo tempo, diversos softwares de gerência diferentes.

A nova meta na construção de softwares de gerência de telecom, é desenvolver um software genérico, que possa configurar equipamentos e interfaces desenvolvidos por outras empresas. E, tornar o software flexível e de fácil manutenção para que novos dispositivos possam ser gerenciados, bastando para isso apenas um *patch* alterando a base de dados do software e suas janelas de configuração.

3.2 Atualização dos Sistemas de Gerência para suportar novos dispositivos

Devido, principalmente às peculiaridades de configuração de cada interface utilizada nas redes de telecomunicação para suportar uma nova tecnologia, é necessário desenvolver uma série de janelas de configuração e monitoração que irão apresentar respectivamente os objetos passíveis de sofrerem alteração para re-configurar os equipamentos e os objetos que irão derivar o estado de operação dos dispositivos e apresentar suas falhas.

Nas janelas que deverão configurar os dispositivos, existem peculiaridades para cada uma das interfaces, como verificação de coerências de configuração, onde determinadas configurações não podem ser configuradas se uma outra característica estiver habilitada, apresentando as possibilidades de configurações referentes à nova tecnologia, a apresentação do objeto passível de sofrer alteração da melhor forma possível graficamente, etc. Porém, os objetos de estado das interfaces são muito mais restritos (ao menos os objetos de interesse do *polling* de estado) e, através das pesquisas dos objetos monitorados para as interfaces existentes atualmente, é possível determinar uma gama bastante considerável de características que devem ser recuperadas em todas as interfaces.

A dificuldade em desenvolver janelas que funcionam genericamente independente de tecnologia, está, obviamente, nas diferenças que existem em cada uma delas. Mas também na maneira como são desenvolvidas pelas empresas fornecedoras de equipamentos de telecomunicação. Para alguns fabricantes, por exemplo, para criar um mapeamento entre uma interface tributária e uma interface agregada de um equipamento PDH, é necessário primeiramente habilitar a operação da interface. Para outros fornecedores, a criação do mapeamento já habilita o objeto de operação da interface.

Esse tipo de dificuldade praticamente inviabiliza o desenvolvimento de um software genérico, que faça o gerenciamento de interfaces de rede distintas sem o desenvolvimento de *patches* ou novas versões dos softwares de gerência utilizados pelas operadoras de telecomunicação. Portanto, é muito mais útil um software que possa auxiliar no desenvolvimento do suporte de uma nova interface, baseando-se no conhecimento dos objetos de interfaces que tiveram a sua gerência desenvolvida anteriormente. Mas sempre será necessária a intervenção do homem para desenvolver o software de gerência.

4 PESQUISA ENTRE AS INTERFACES DE TELECOM UTILIZADAS NO BRASIL

A partir de uma amostra das interfaces utilizadas nos equipamentos de telecomunicação no Brasil, iremos caracterizar cada uma delas, com base nas suas recomendações, suas características de configuração, seus possíveis usos no mercado e, principalmente, levantar e entender seus objetos gerenciáveis.

Primeiramente são descritas todas as características das interfaces pesquisadas, não sendo levado em consideração se os dados levantados são configurados ou gerenciados por softwares de gerência (como é o caso de algumas características físicas das interfaces, que não podem ser alteradas), para podermos conhecer as interfaces como um todo, seus usos, características e configurações. Em uma segunda etapa, serão recuperados apenas os objetos gerenciáveis por softwares de gerência.

Com essas informações, será possível apontar semelhanças entre as interfaces de redes de telecom, e as características gerenciáveis que forem semelhantes num grupo grande de interfaces, podem servir como base para o suporte de novas tecnologias nos sistemas de gerência.

De outra forma, também podem ser criados grupos de interfaces que possuam características semelhantes. Quando uma nova tecnologia precisa ser suportada no software de gerência, podem ser consultados os grupos para verificar se o novo dispositivo não se encaixa no perfil de um dos grupos já criados.

Tabela 4.1: Características das interfaces pesquisadas

Interface	Descrição	Características Funcionais	Características Físicas	Órgão Padronizador
RS-232	Interface serial para comunicação full-duplex.	Rec. V.24	Conector padrão ISSO DB25/DB9	ITU-T
V.35	Interface serial comumente utilizada a taxa de 48 Kbits/s para modems de banda.	Rec. V.35	Conector de 34 pinos	ITU-T
E1 / T1	Hierarquias PDH que utilizam TDM (multiplexação no tempo)	Rec. G.704	BNC ou RJ45	ITU-T
ADSL	Tecnologia baseada na rede de par trançado existente no mundo.	T1.413	Conector RJ45	ANSI
G. SHDSL	Permite comunicação bidirecional com velocidades de 192 kbits/s a 2.31 megabits/s. Utiliza a rede telefônica pública.	G.991.2	Conector RJ45	ITU
FXS/FXO	Interfaces utilizadas para conexão com a rede de telefonia pública.	G. 711	Conector RJ11 Conector RJ45	ITU-T
E&M	Interface que trafega canal de voz (64Kbits/s)	G. 711	Conector RJ11	ITU-T
ETHERNET	Interface padrão em redes locais	Rec. 802.3	Conector RJ45	IEEE

Observações:

- Rec. V.24: é um padrão do ITU-T que define a troca de circuitos entre o DTE (*Data Terminal Equipment*) e o DCE (*Data Communication Equipment*)
- Rec. V.28: padrão ITU (1972), que define as funções de todos os circuitos para a interface RS-232.

4.1 Interface serial RS-232

Foi criada em 1962 pelo EIA (*Eletronics Industries Association*) nos Estados Unidos, com o intuito de se tornar um formato padrão para comunicação serial entre computadores e periféricos. O padrão RS-232 descreve as características dos conectores a serem utilizados (tamanho, numero de pinos e formato), os níveis de voltagem a serem suportados e as funções de controle designados para cada pino. O padrão também apresenta um simples protocolo de *handshaking*, que determina quando o equipamento terminal está pronto para enviar e receber dados. Apesar das primeiras idéias a respeito do seu futuro, esse tipo de interface continua sendo largamente utilizado na indústria pela sua simplicidade, estando presente na maioria dos dispositivos que comunicam com um computador.

Nesse tipo de interface, canais independentes são estabelecidos para uma comunicação *full-duplex*.

- **Características Lógicas:** descritas na recomendação V.24 do EIA.
- **Características Elétricas:** os sinais na interface RS232 são representados por diferenças de níveis de voltagens em relação ao fio terra. O estado de “*Idle*” (ou MARK) tem o seu sinal negativo em relação ao terra, e o sinal ativo (SPACE) tem o sinal positivo em relação ao terra. RS232 tem várias linhas de *handshaking* (primeiramente utilizada nos modems) .
- **Características Físicas:** Descritas nas figuras 4.1.1 e 4.1.2

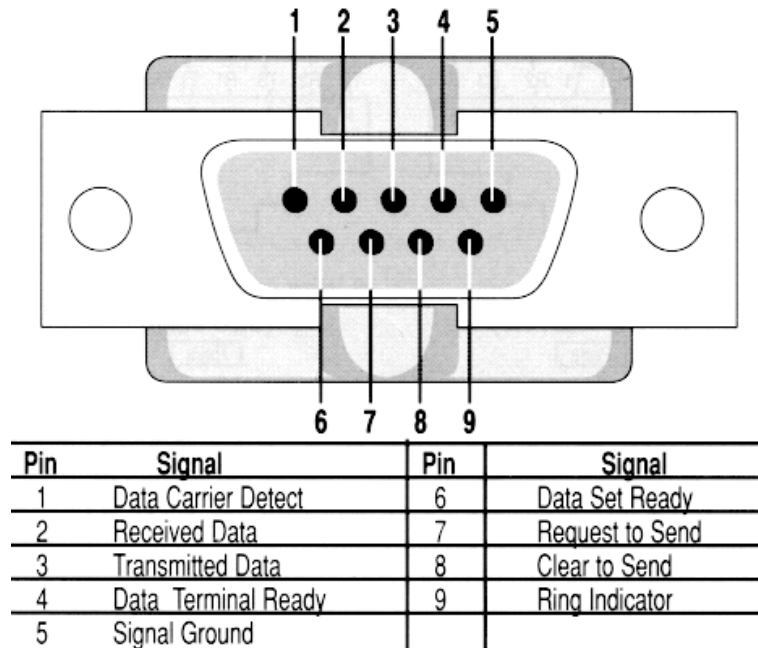


Figura 4.1: Pinagem da interface RS-232/V.24 num conector DB-9

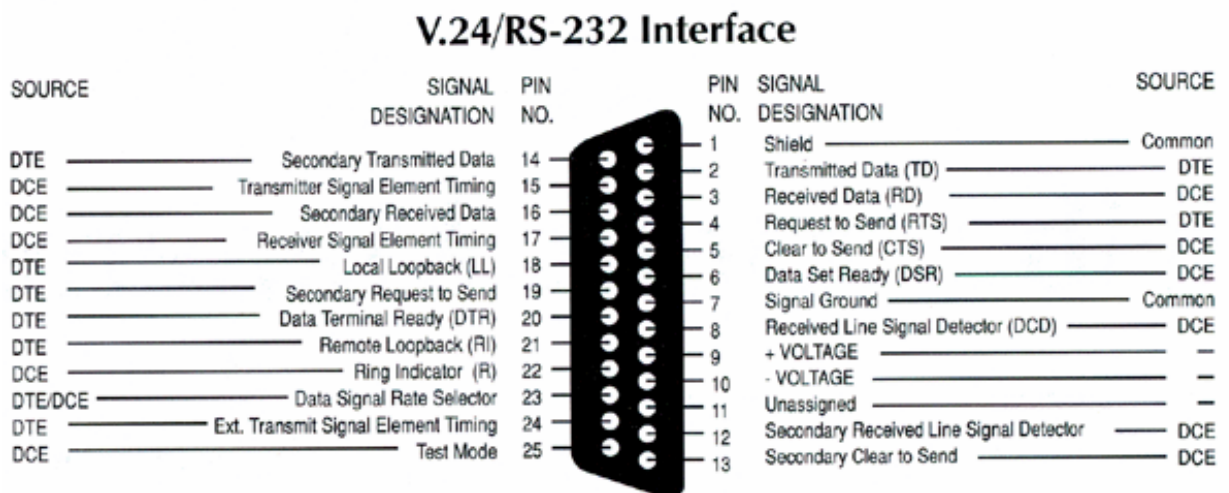


Figura 4.2: Pinagem da interface RS-232/V.24 num conector DB-25

4.1.1 Configurações:

Há várias configurações de software para conexões seriais. As mais comuns são velocidade e bits de paridade e parada. Taxas comuns de transmissão são 300, 1200, 2400, 9600, 19200 bits por segundo. Tipicamente, ambos os dispositivos devem estar configurados com a mesma velocidade, sendo que alguns podem ser configurados para auto-detectar a velocidade. A paridade é normalmente nula (não usada), mas pode ser par ou ímpar.

Existe uma convenção para a notação de uma configuração de uma conexão serial. Esta notação é da forma D/P/S, sendo que a configuração mais comum é a 8/N/1 que especifica que são transmitidos 8 bits de dados, paridade nula e um bit de parada. O número de bits de dados pode ser 7, 8 ou, às vezes, 9. A paridade pode ser nula (N), ímpar (O) ou par (E). O bit de paridade é emprestado dos bits de dados, então 8/E/1 significa que um dos oito bits de dados é utilizado como bit de paridade. Outras configurações definem quando pinos enviam sinais de "handshake", ou checagens de integridade dos dados. Combinações comuns são RTS/CTS, DTR/DSR, ou XON/XOFF, que não usam pinos no conector, mas caracteres especiais no fluxo dos dados. O caractere XON diz ao receptor que o remetente do caractere está pronto pra receber mais dados. O caractere XOFF diz ao receptor para parar de enviar caracteres. O XON/XOFF está em desuso, e é preferível que se utilize o controle de fluxo RTS/CTS. O XON/XOFF é um método "em banda" que funciona entre dois pontos, mas ambos devem suportar o protocolo.

O RTS/CTS foi desenvolvido com o intuito de permitir que a teletypewriter e o modem coordenassem ligações half-duplex onde apenas um modem pode transmitir por vez. O terminal deve "levantar" o sinal Pronto Pra Enviar e esperar que o modem responda com Envie os Dados. RTS/CTS é um "handshake" no nível do hardware, mas tem suas vantagens. Uma teletypewriter ASR tinha um leitor de fita de papel, os caracteres eram enviados quando a fita era lida (ASR vem de Automatic Send Receive, envia e recebe automaticamente). Quando a máquina recebia um caractere XOFF, ela desligava a leitora de fita e ao receber um XON a religava. O sistema remoto poderia enviar um XOFF quando era necessário que o remetente diminuísse sua velocidade.

4.2 Interface V.35

A interface V.35 é uma das mais antigas definidas pelo ITU-T e sua primeira versão data de 1968. Originalmente uma especificação de modems de grupo na taxa de 48Kbit/s, hoje em dia tem sua importância restrita praticamente à interface digital definida no Apêndice-II da recomendação. Esta interface é hoje, largamente adotada pela maioria dos fabricantes de equipamentos de comunicação, tanto europeus, como principalmente americanos, em taxas de 48Kbit/s a 10Mbit/s.

A sua principal inovação em relação à interface V.24/V.28, é que os sinais de dados e relógio são balanceados, enquanto os sinais de controle continuam sendo bipolares como na recomendação V.24/V.28.

As características elétricas desta interface são descritas no apêndice da recomendação V.35 (transmissão de dados a 48Kbits/s usando um grupo básico de 60-108KHz). Ainda que aplicável principalmente a taxas de 48Kbits/s, a interface V.35 tem aplicação também em 56 e 64Kbits/s.

Uma característica especial da placa V. 35 é a possibilidade da porta 1 destas interfaces ser configurada para operar com velocidades mais baixas que 2,048Mbit/s, usando uma estrutura de dados proprietária, tendo como grande vantagem a conservação do sincronismo de octeto (bit e byte), sendo chamada nesses casos de interface V. 35 estruturada. Dessa forma, o sinal da V.35 pode ser entendido como um *frame* contendo um *timeslot* de sincronismo e N *timeslots* de dados. O número de *timeslots* de dados disponíveis depende da velocidade configurada na interface, sendo que cada *timeslot* é composto por 8 bits, ou seja, pegando a velocidade da V.35 dividida

por 64k têm-se o número total de *timeslots* na interface, subtraindo o *timeslot* de sincronismo obtém-se o número de *timeslots* disponíveis para dados (N).

Na figura 4.5 apresentamos uma implementação de um circuito de interface balanceado de acordo com as características elétricas da recomendação V.35 do ITU-T. Esta recomendação estabelece os seguintes parâmetros para o circuito do gerador balanceado:

- a) impedância de saída entre 50 e 150 ohms;
- b) resistência dos pontos Va ou Vb para o terra de sinal (CT 102), 150 +/- 15 ohms;
- c) quando terminado com carga de 100 ohms e transmitindo dígitos binários igual a zero, a tensão sobre a carga deve ser $V_{ab} = 0,55 \text{ volts} \pm 20\%$;
- d) o tempo de subida do sinal, com a terminação de 100 ohms, deverá ser menor que 1% do tempo de bit (T_b);
- e) a média aritmética da tensão do ponto Va ou Vb, em relação ao terra de sinal (CT 102), não deve ser maior que 0,6 volts, com terminação de 100 ohms.

Para o circuito do receptor, a recomendação estabelece:

- a) impedância de entrada em torno de 100 +/- 10 ohms, essencialmente resistiva;

Os níveis lógicos para os sinais de relógio e sinais de dados são as seguintes:

$$1 = -0,55V \pm 20\%$$

$$0 = +0,55V \pm 20\%$$

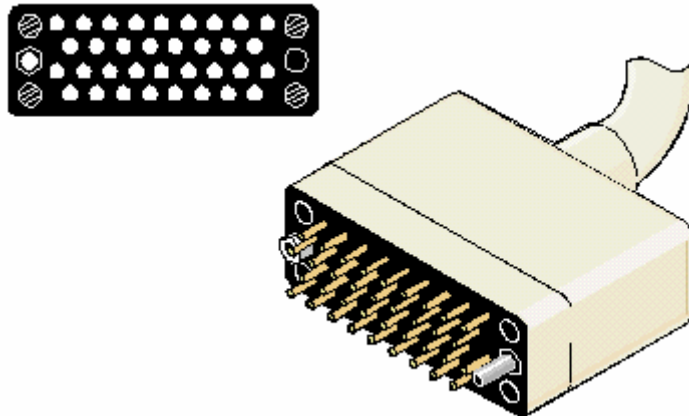


Figura 4.3: Conector da interface V.35

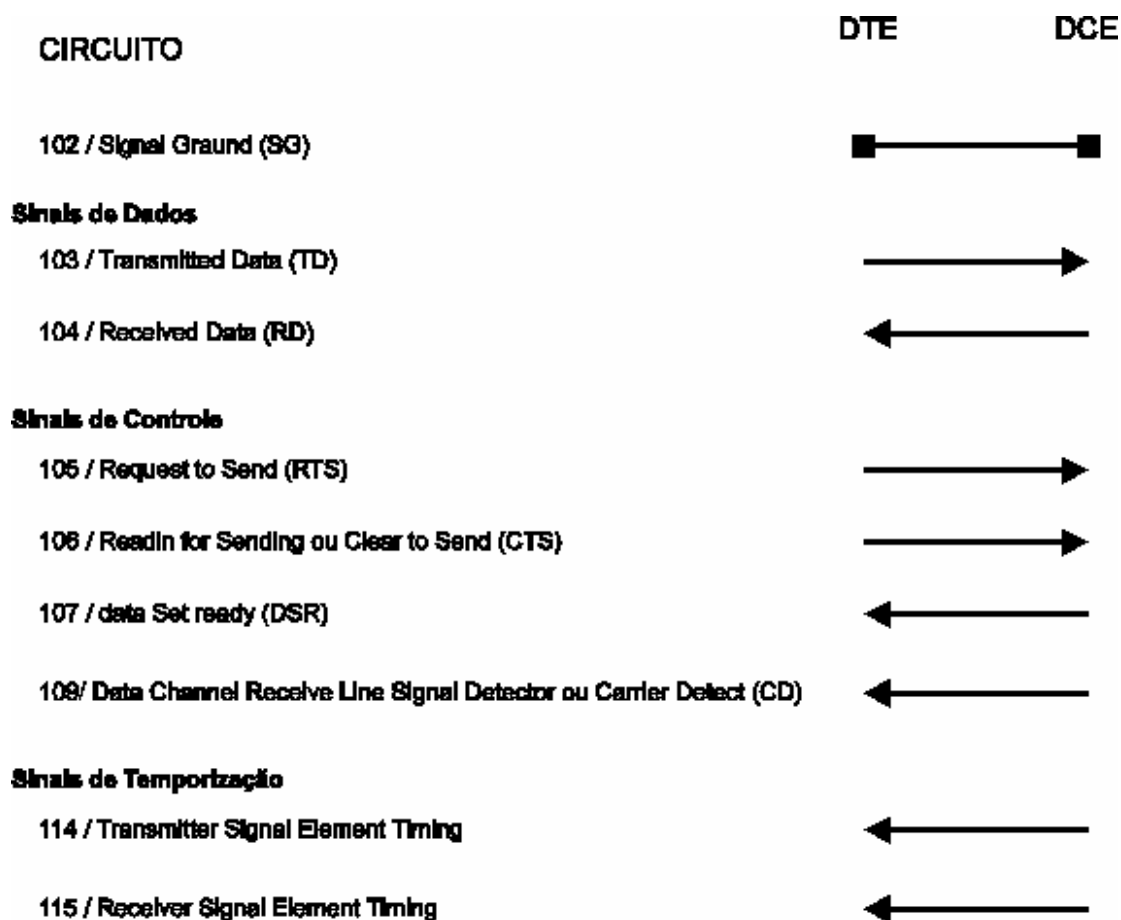


Figura 4.4: Sentidos dos sinais na interface V.35

Através do uso da ferramenta *Device Compare*, foram encontrados os seguintes objetos monitoráveis pelo software de gerência.

Tabela 4.2: Objetos monitorados pelo software de gerência para a interface V.35

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStcurrentPortSlip	Indica estouro do <i>buffer</i> de leitura.
mitfStDigitalItfCt105	Informações do sinal RTS
mitfStDigitalItfCt108	Informações do pino DTR
mitfStDigitalItfCt109	Informações do pino DCD
mitfStDigitalItfCt113	Informações do pino XTC
mitfStDigitalItfCt128	Informações do pino ERC
GenDvInfPortHwId	Identifica a versão de hardware da porta
genDvInfPortFimVersion	Versão de <i>firmware</i> da interface

mitfCfgDigitalItfClock	Fonte de relógio da interface
mitfCfgDigitalItfProtocol	Identifica o protocolo utilizado na porta V.35
mitfCfgDigitalItfSpeed	Configuração da velocidade de operação da porta.
mitfCfgPortBackup	Identificador da porta backup
mitfCfgPortChannelsNum	Número de canais configurados na porta
mitfCfgPortIdleByte	Byte enviado nos <i>timeslots</i> não mapeados
mitfCfgPortLDRtest	Habilitação de teste LDR (Loop Digital Remoto)
mitfCfgPortRemoteManag	Habilita gerência remota através da porta
genDvAlCfSt	Habilitação/Desabilitação de envio traps

4.3 Recomendação G.703

A recomendação G.703 foi criada pelo grupo de estudo XVIII do CCITT (*The International Telegraph and Telephone Consultative Comitee*) e foi aprovada sobre a resolução número 2 em abril de 1991. A recomendação versa sobre as características físicas e elétricas de interfaces de hierarquias digitais.

A recomendação G.703 tem sido utilizada nos últimos anos em links WAN para voz e dados. Essa interface pode operar com velocidades entre 64 Kbps e 34 Mbps, porém a velocidade mais utilizada atualmente no Brasil e amplamente utilizada nas empresas pesquisadas é de 2,048 Mbps nas linhas E1.

O G.703 é uma recomendação ITU-T que trata das especificações da interface física a 4 fios e da sinalização digital para transmissão à 2,048 Mbps (E1). Atualmente, também inclui as especificações para o T1 a 1,544 Mbps (utilizada nos Estados Unidos), porém, geralmente é utilizado para se referir à interface de transmissão européia a 2,048 Mbps.

O padrão G.703 utiliza um método de transmissão isossíncrono, ou seja, o sincronismo do sinal é codificado com os dados, existindo apenas dois pares de sinal: transmissão e recepção.

A técnica mais comum de codificação é utilizando o protocolo HDB3 (*High-Density Bipolar-3 zeros*), entretanto, muitas outras técnicas são admissíveis.

A interface G.703 pode ser usada como uma interface co-direcional, ou seja, uma interface que transmite nos dois sentidos e que os dados e o tempo de sinal associado são transmitidos na mesma direção.

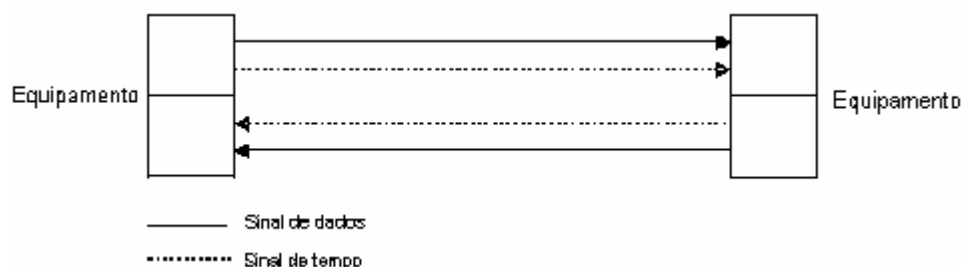


Figura 4.5: Interface co-direcional

Outra alternativa é utilizar a interface G. 703 com *clock* centralizado, ou seja, é a interface onde em ambos sentidos da transmissão do sinal de dados, o sinal de tempo associado é fornecido por um relógio centralizado, que pode ser derivado, por exemplo, por outros sinais utilizados na transmissão.

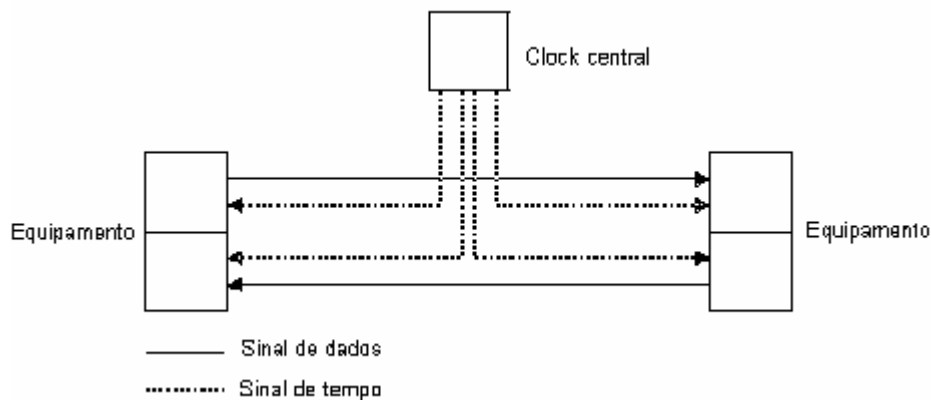


Figura 4.6: Interface com *clock* centralizado.

As interfaces do tipo co-direcional e de *clock* centralizado devem ser utilizadas em redes sincronizadas (do tipo PDH), para assegurar um intervalo adequado no sinal de *clock*.

Existe ainda um terceiro tipo de interface G. 703, chamada de interface contradirecional, onde o sinal de *clock* é enviado pela outra interface utilizada na transmissão (ou seja enviada no outro sentido, pelo outro equipamento utilizado na transmissão).

4.3.1 Estrutura dos quadros

A comutação das fatias de tempo dentro do quadro caracteriza a comutação entre os canais digitais segundo um matriz de comutação do tipo 32 x 32. Abaixo, temos um esquema da estrutura dos quadros de uma interface G. 703 de hierarquia E1 co-direcional.

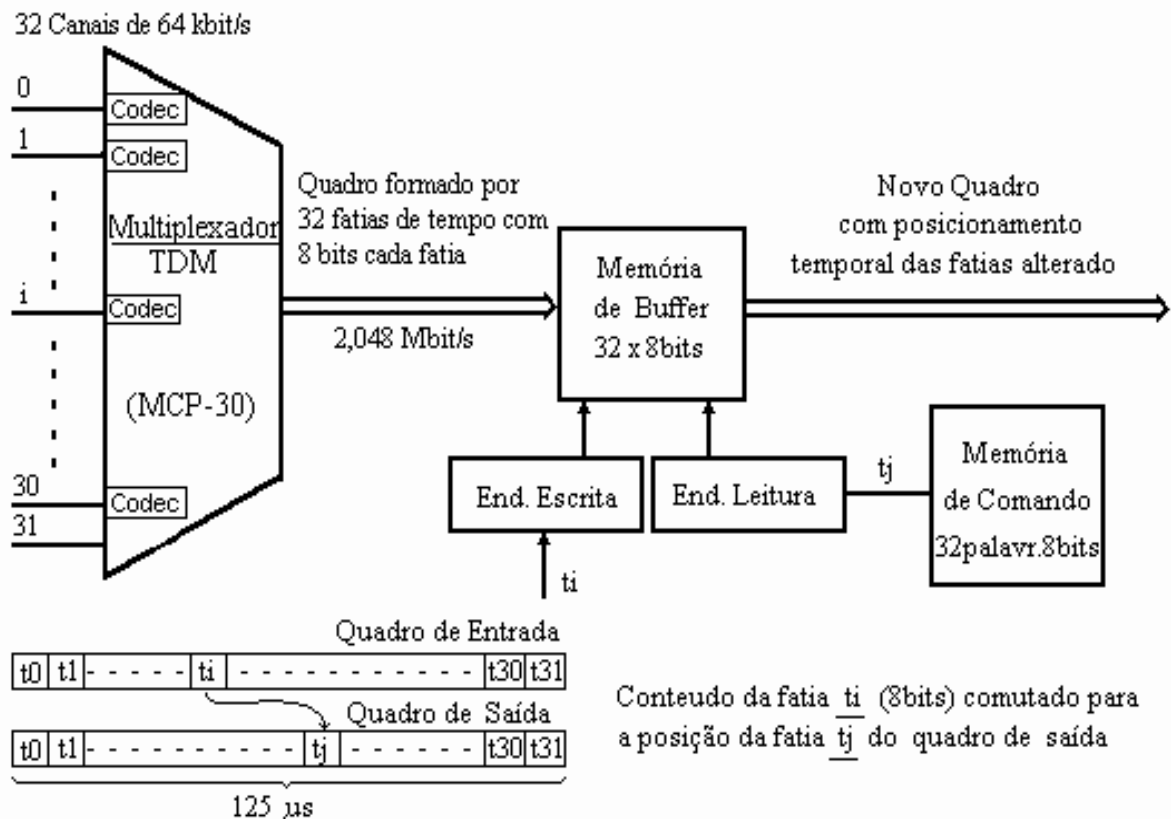


Figura 4.7: Estrutura dos quadros utilizados na interface E1 G. 703

Na G.703, dois tipos de interfaces são utilizados. O padrão foi originalmente desenvolvido para o uso sobre um par de cabos coaxiais de 75 ohms, mas foi posteriormente incluída a interface balanceada de par trançado, que se tornou muito popular na Europa.

Nas placas do tipo G. 703 pesquisadas, podem ser configurados:

- Número de canais de dados utilizados;
- *Timeslot* inicial dos canais de dados;
- Transmissão de dados no *timeslot* 16;
- Avaliação da recepção de CRC4;
- Habilitação de testes.

Além dessas opções, é possível configurar a interface G. 703 como um link de *backup* de uma outra. Um link de *backup* pode ser configurado numa das seguintes formas de operação: desligado, automático ou semi-automático.

- **Desligado** significa que o equipamento não chaveará para a placa *backup* quando houver falha no link principal. Essa opção, geralmente é utilizada para forçar o funcionamento do link principal, mesmo que este não esteja funcionando adequadamente;

- **Automático** faz com que os dados sejam chaveados para o link de *backup* e, somente retornem para o link principal após a manutenção da estabilidade ou quando o link de *backup* cair (caso o link principal esteja funcionando);

- **Semi-automático** faz com que os dados passem a trafegar pelo link de *backup* até que o mesmo caia ou que o usuário reconfigure os links. O semi-automático retoma o link principal quando ocorrer falha nos dois links simultaneamente

Através do uso da ferramenta *Device Compare*, foram encontrados os seguintes objetos monitoráveis pelo software de gerência.

Tabela 4.3: Objetos monitorados pelo software de gerência para a interface G.703

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStcurrentPortSlip	Indica estouro do <i>buffer</i> de leitura.
mitfCfgG703CAS	Define o comportamento da sinalização CAS
mitfCfgG703CRC4	Habilita o uso de CRC-4 na interface
mitfCfgG703InitialTs	<i>Timeslot</i> inicial para envio de dados
mitfCfgG703LnImpedance	Impedância da linha
mitfCfgG703TS16	Habilitação do <i>timeslot</i> 16 para envio de dados
mitfCfgG703UnusedChannels	Ação a ser tomada nos <i>timeslots</i> não mapeados
genDvInfPortHwId	Identifica a versão de hardware da porta
genDvInfPortFimVersion	Versão de <i>firmware</i> da interface
mitfCfgPortBackup	Identificador da porta backup
mitfCfgPortChannelsNum	Número da canais configurados na porta
mitfCfgPortIdleByte	Byte enviado nos <i>timeslots</i> não mapeados
mitfCfgPortLDRtest	Habilitação de teste LDR (Loop Digital Remoto)
mitfCfgPortRemoteManag	Habilita gerência remota através da porta
genDvAlCfGTrapSt	Habilitação/Desabilitação de envio traps

4.4 Interfaces de Telefonia

4.4.1 Interfaces FXS e FXO

As interfaces FXS (*Foreign Exchange Subscriber*) e FXO (*Foreign Exchange Office*), são utilizadas normalmente para efetuar a conexão entre um equipamento de dados (roteador) e um equipamento de voz (PABX).

A interface FXS, disponibiliza serviços POTS (*Plain old Telephone Service*) devendo ser ligada diretamente à um telefone comum ou como um tronco de entrada em um PABX (*Private Automatic Branch Exchange*), dependendo da aplicação desejada.

A interface FXO (*Foreign Exchange Office*), fornece endereçamento, ou seja, disca números telefônicos, comportando-se como um telefone.

Tipos de conexões entre interfaces FXS/FXO a um PABX

PABX ligado à uma interface FXS

Neste tipo de conexão, a interface FXS será ligada como um tronco de entrada no PABX, comportando-se como uma linha telefônica comum. Como a interface FXS provê apenas alimentação e *ring*, ou seja, não disca, ao encaminhar a chamada para o PABX não poderá escolher qual ramal deseja chamar. Desta forma, todas as chamadas deverão ser encaminhadas a uma única posição, por exemplo uma telefonista.

PABX ligado à uma interface FXO

Neste tipo de conexão, a interface FXO será ligada em um ramal do PABX, comportando-se como um telefone. Sendo assim, ao encaminhar uma chamada ao PABX, o roteador poderá escolher qual ramal deseja chamar, discando o número do ramal específico, com funcionamento igual à um tronco DDR (Discagem Direta à Ramal).

Este tipo de ligação é o mais comum e mais simples, uma vez que não requer configuração específica do PABX, no entanto, pode prender a chamada na interface dependendo da configuração da rede.

Isto acontece porque a forma do PABX indicar que terminou uma chamada, quando o ramal origem desliga o telefone, é através de tom de ocupado. Assim, a pessoa que recebeu a chamada sabe que deve desligar e colocar o telefone no gancho.

Já os equipamentos não têm como identificar que o tom de ocupado significa que é necessário desconectar a chamada, prendendo a interface até que receba explicitamente o sinal de desconexão. Atualmente, a empresa Cisco desenvolve mecanismos que resolvem este problema.

Através do uso da ferramenta *Device Compare*, foram encontrados os seguintes objetos monitoráveis pelo software de gerência.

Tabela 4.4: Objetos monitorados pela gerência para as interface FXS e FXO.

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStVoiceItfPowerSupply	Informa o estado da fonte da interface
mitfStVoiceItfOverheating	Estado de aquecimento da interface
mitfCfgVoiceItfImpedance	Define a impedância da linha analógica
mitfCfgVoiceItfInterfSel	Define o modo de operação na linha analógica (2 ou 4 fios)
mitfCfgVoiceItfMetering	Define tipo de tarifação da linha analógica
mitfCfgVoiceItfRingFilter	Habilita o filtro de <i>Ring</i> na interface
mitfCfgVoiceItfRxGain	Define o ganho na recepção

mitfCfgVoiceItfSigMode	Define a forma como a sinalização é aplicada
mitfCfgVoiceItfSigType	Define o tipo de sinalização
mitfCfgVoiceItfTxGain	Define o ganho na transmissão
genDvInfPortHwId	Identifica a versão de hardware da porta
genDvInfPortFimVersion	Versão de <i>firmware</i> da interface
mitfCfgPortBackup	Identificador da porta backup
mitfCfgPortChannelsNum	Número de canais configurados na porta
mitfCfgPortIdleByte	Byte enviado nos <i>timeslots</i> não mapeados
mitfCfgPortLDRtest	Habilitação de teste LDR (Loop Digital Remoto)
mitfCfgPortRemoteManag	Habilita gerência remota através da porta
genDvAlCfgTrapSt	Habilitação/Desabilitação de envio traps

4.4.2 Interface E&M

A interface E&M (*Ear & Mouth*), é uma interface do tipo *tie-line*, utilizada em entroncamento entre PABXs. É uma placa de interface de voz, possuindo os mais variados números de portas com conectores RJ45 na maioria das vezes. Nas implementações consultadas, as portas podem ser configuradas para transmissão a 2 ou a 4 fios de forma independente. Esse tipo de interface opera na faixa de frequência de um canal de voz de 300Hz a 3400Hz, sem compressão.

Uma interessante aplicação encontrada na implementação da interface pela empresa Datacom-Telemática, é a operação com transmissão, mesmo sem uma chamada estabelecida (*on hook transmission*);

PABX ligado à uma interface E&M

Esta é a forma mais correta de conectar um roteador à um PABX, funcionando como um *tié-line*. Em termos de funcionalidade a E&M é idêntica à FXO, porém com uma grande vantagem referente à sinalização. A interface E&M pode possuir de 2 a 4 fios apenas para sinalização, além de 2 ou 4 fios utilizados para encaminhar a chamada de voz.

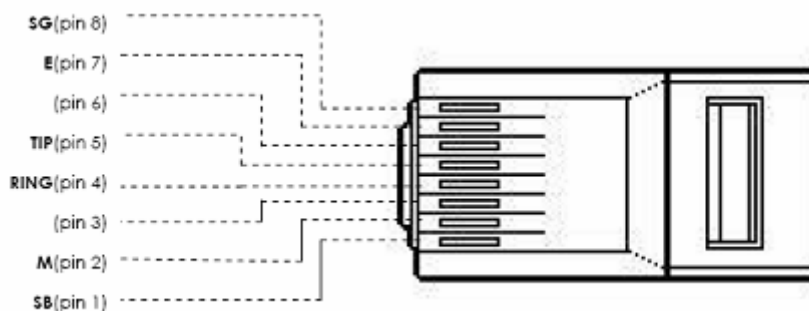


Figura 4.8: Pinos da interface E&M

Como a interface possui canal dedicado apenas à sinalização, o problema que temos com a FXO e o tom de ocupado não ocorre aqui, já que o sinal de desconexão é enviado pelos pinos E e M. No momento da configuração é necessário escolher qual o tipo de E&M a ser utilizado, podendo ser do tipo I, II, III e V. O tipo I e V utilizam 2 fios para a sinalização dos pinos E e M, e 2 ou 4 para a voz. Já os tipos II e III utilizam 4 fios para E e M, e 2 ou 4 fios para voz.

Descrição dos principais pinos da interface E&M:

- Pino 7 - E (*Ear or Earth*)
- Pino 2 - M (*Mouth or Magnet*)
- Pino 8 - SG (*Signal Ground*) – usado nas interfaces E&M de tipos 2,3, 4 (tipo 4 não é suportado nos roteadores CISCO. Atualmente não é um padrão).
- Pinos 5 e 4 - T / R (*Tip / Ring*) – O fio T/R leva o sinal de áudio entre a unidade de sinalização e o circuito de *trunking*. Em uma operação a dois fios, esse par de fios transmite o áudio de forma *full-duple*..
- Pino 1 - SB (*Signal Battery*) – Usado nas interfaces E&M de tipos 2,3, 4 (tipo 4 não é suportado nos roteadores CISCO. Atualmente não é um padrão).

A interface E&M aceita somente discagem por tons multifrequenciais (DTMF).

Utilizando a ferramenta *Device Compare* foram encontrados os seguintes objetos gerenciados pelo sistema de gerência para a interface E&M.

Tabela 4.5: Objetos monitorados pelo software de gerência para a interface E&M.

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStVoiceItfPowerSupply	Informa o estado da fonte da interface
mitfStVoiceItfOverheating	Estado de aquecimento da interface
mitfCfgVoiceItfImpedance	Define a impedância da linha analógica
mitfCfgVoiceItfInterfSel	Define o modo de operação na linha analógica (2 ou 4 fios)
mitfCfgVoiceItfMetering	Define tipo de tarifação da linha analógica
mitfCfgVoiceItfRingFilter	Habilita o filtro de <i>Ring</i> na interface
mitfCfgVoiceItfRxGain	Define o ganho na recepção
mitfCfgVoiceItfSigMode	Define a forma como a sinalização é aplicada
mitfCfgVoiceItfSigType	Define o tipo de sinalização
mitfCfgVoiceItfTxGain	Define o ganho na transmissão
genDvInfPortHwId	Identifica a versão de hardware da porta
genDvInfPortFimVersion	Versão de <i>firmware</i> da interface
mitfCfgPortBackup	Identificador da porta backup

mitfCfgPortChannelsNum	Número da canais configurados na porta
mitfCfgPortIdleByte	Byte enviado nos <i>timeslots</i> não mapeados
mitfCfgPortLDRtest	Habilitação de teste LDR (Loop Digital Remoto)
mitfCfgPortRemoteManag	Habilita gerência remota através da porta
genDvAlCfgTrapSt	Habilitação/Desabilitação de envio traps

4.5 Interfaces xDSL

4.5.1 Interface G. SHDSL

SHDSL significa (*Single-Line High-bit-rate Digital Subscriber Line*). Este é um padrão internacional, também conhecido como G.991.2 desenvolvido pela ITU. Ao contrário do ADSL (*Asymmetric Digital Subscriber Line*), popular atualmente, onde as taxas de *upload* são muito mais baixas que as de *download* (por isso o uso da palavra *assimetric*), o G.SHDSL permite uma comunicação bidirecional com velocidades de 192 kbits a 2.31 megabits usando um par de fios de cobre (em outras palavras, um cabo telefônico comum), mesmo a grandes distâncias. Nas interfaces pesquisadas, encontrou-se uma implementação que pode transportar de 1 a 32 *timeslots* com alinhamento de canais.

A potência do sinal transmitido é de 13,5dBm para taxas inferiores a 2048kbit/s e 14,5dBm para 2048kbit/s na implementação encontrada nas pesquisas, também podendo ser configurada para operar em modo plesiócrono, síncrono ou seleção automática. As negociações de *handshake* se dão conforme a recomendação G.994.1 do ITU-T.

O padrão também possibilita um melhor desempenho e um melhor aproveitamento da rede de cobre se comparado com os atuais modems HDSL.

Pode ser configurado para funcionar como LTU ou NTU. A interface ainda permite testes como laço digital local e geração de padrão de teste com detecção de erros através de comandos pela porta de controle. Nas implementações pesquisadas no trabalho encontrou-se apenas portas com conectores RJ45. As interfaces utilizavam um modem DPSK (*Differential Phase Shift Keying*) de 12 kHz para efetuar o *handshake* quando configurado como NTU e 20kHz para o LTU. As mensagens predefinidas pela norma (G.994.1) são trocadas e as duas pontas determinam um modo comum de operação.

Estrutura do Frame G.shdsl

O frame G.shdsl possui 4 blocos de dados (*payload blocks*) separados pelos bits de cabeçalho. Ele se repete a cada 6ms, independente da taxa configurada.

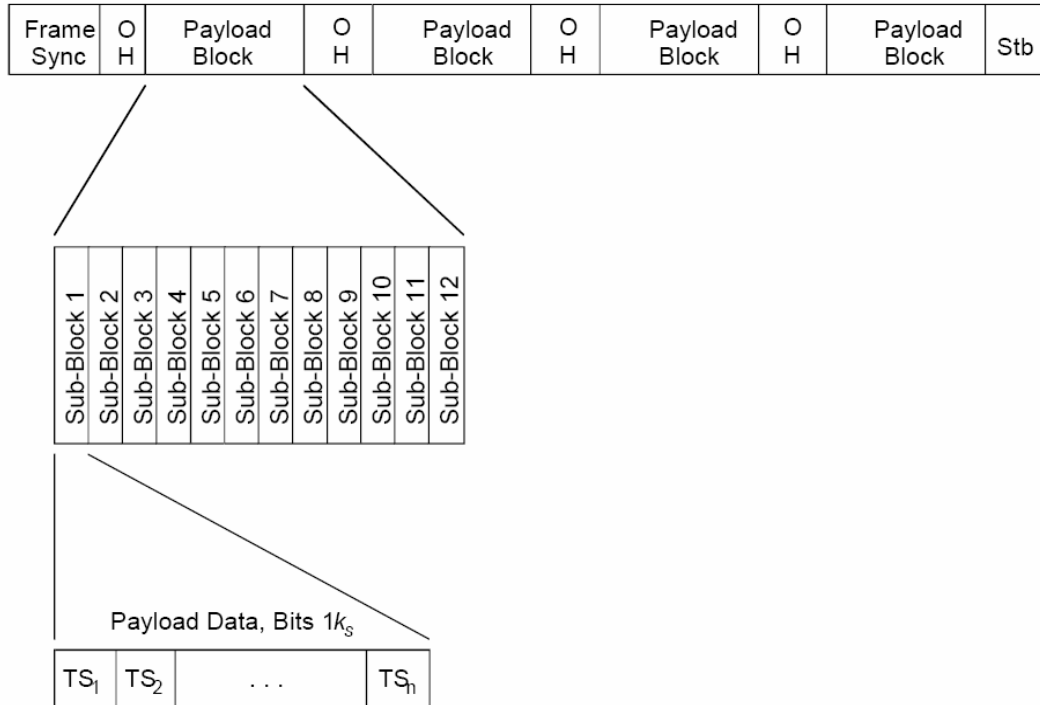


Figura 4.9: Frame G.shdsl - Estrutura dos blocos de dados

O cabeçalho exerce função essencial na transmissão dos dados, pois garante alinhamento, transporta informações de gerência via EOC (*Embedded Operations Channel*) e ainda possui um mecanismo de identificação de erros nos dados (CRC6).

Através do uso da ferramenta *Device Compare*, foram encontrados os seguintes objetos monitoráveis pelo software de gerência.

Tabela 4.6: Objetos monitorados para a interface G.SHDSL

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStcurrentPortLink	<i>Status</i> do link da porta
mitfStDslItfLoopAtnDef	Indica atenuação na linha
mitfStDslItfSNRMarginDef	Configura margem para ativar alarme de SNR
mitfStDslItfDataRate	Taxa de operação da interface DSL
mitfStDslItfFrameMode	Modo de operação dos frames DSL
genDvInfPortHwId	Identificador da versão de hardware da porta
genDvInfPortFimVersion	Versão de <i>firmware</i> da interface
mitfCfgDslItfAnnex	Indica anexo da norma que deve ser usado
mitfCfgDslItfUnitType	Indica se a interface vai operar como <i>terminator</i>
mitfCfgPortAlarmDetection	Deteção de alarmes na porta
mitfCfgPortBackup	Identificador da porta backup
mitfCfgPortChannelsNum	Número de canais configurados na porta
mitfCfgPortIdleByte	Byte enviado nos <i>timeslots</i> não mapeados
mitfCfgPortLDRtest	Habilitação de teste LDR (Loop Digital Remoto)
mitfCfgPortRemoteManag	Habilita gerência remota através da porta
genDvAlCfgTrapSt	Habilitação/Desabilitação de envio traps

4.5.2 Interface ADSL

ADSL é a sigla para *Assymmetric Digital Subscriber Line* ou "Linha Digital Assimétrica para Assinante". Trata-se de uma tecnologia que permite a transferência digital de dados em alta velocidade por meio de linhas telefônicas comuns. A cada dia, o ADSL ganha novos usuários, tanto que este é o tipo de tecnologia para conexão à internet em banda larga mais usado no Brasil e um dos mais conhecidos no mundo.

Como funciona o ADSL

A tecnologia ADSL basicamente divide a linha telefônica em três canais virtuais, sendo um para voz, um para download (de velocidade alta) e um para upload (com velocidade média se comparado ao canal de download). Teoricamente, as velocidades de download podem ir de 256 Kbps até 6.1 Mbps. No caso do upload essas taxas variam de 16 Kbps até 640 Kbps. É por causa dessas características que o ADSL ganhou o termo "assymmetric" (assimétrica) no nome, pois indica que a tecnologia possui maior velocidade para download e menor velocidade para upload.

Entre os três canais, existe um disponível para voz. Isso permite que o usuário fale ao telefone e ao mesmo tempo navegue na internet, ou seja, não é necessário desconectar para falar ao telefone. Para separar voz de dados na linha telefônica, é instalado na linha do usuário um pequeno aparelho chamado Splitter.

Na central telefônica também há uma espécie de Splitter. Assim, quando é realizada uma chamada telefônica (voz), o sinal é encaminhado para a rede de comutação de circuitos da companhia telefônica (PSTN - *Public Switched Telephone Network*) e segue seu caminho habitual.

Quando uma linha telefônica é usada somente para voz, essas chamadas utilizam frequências baixas, geralmente entre 300 Hz e 4000 Hz. As linhas de par trançado existentes na rede telefônica pública, permitem transmissões em taxas muito maiores que acabam sendo desperdiçadas. Explicando de maneira simples, o ADSL aproveita essas frequências que não são usadas no canal de voz para a transmissão de dados. Como é possível usar mais de uma frequência ao mesmo tempo na linha telefônica, pode-se usar o telefone para voz e dados ao mesmo tempo. A ilustração abaixo exemplifica este esquema:



Figura 4.10: Utilização de banda no ADSL

A comunicação entre os dispositivos que utilizam ADSL ocorre em frequências acima de 5000 Hz, não interferindo na comunicação de voz (que funciona entre 300 Hz e 4000 Hz). Quando o modem ADSL estabelece uma conexão com o modem da central telefônica, o sinal vai para um roteador, em seguida para o provedor e finalmente para a internet.

O sinal citado acima, depois de enviado à central telefônica, é separado e os dados vão para um equipamento DSLAM (*Digital Subscriber Line Access Multiplexer*), que limita a velocidade do usuário e une várias linhas ADSL, enviando o sinal para uma linha ATM (*Asynchronous Transfer Mode*) de alta velocidade que está conectada à internet.

Utilizando a ferramenta de *Device Compare*, foram encontrados os seguintes objetos monitoráveis pelo software de gerência para a interface ADSL.

Tabela 4.7: Objetos monitorados para a interface ADSL

Objeto da MIB	Descrição
mitfCfgPortOperation	Operação da porta (habilitada/desabilitada)
mitfStCurrentPortTest	Identificador de testes executados na porta
mitfStcurrentPortLink	Status do link da porta
mitfStDslItfLoopAtnDef	Indica atenuação da linha

<code>mitfStDslItfSNRMarginDef</code>	Margem do nível sinal-ruído.
<code>mitfStDslItfDataRate</code>	Taxa de operação da interface DSL
<code>mitfStDslItfFrameMode</code>	Modo de operação dos <i>frames</i> DSL
<code>genDvInfPortHwId</code>	Identificador da versão de hardware da porta
<code>genDvInfPortFimVersion</code>	Versão de <i>firmware</i> da interface
<code>mitfCfgDslItfUnitType</code>	Indica tipo da interface (<i>network</i> ou <i>terminator</i>)
<code>mitfCfgPortAlarmDetection</code>	Detecção de alarmes na porta
<code>mitfCfgPortBackup</code>	Identificador da porta backup
<code>mitfCfgPortChannelsNum</code>	Número de canais configurados na porta
<code>mitfCfgPortIdleByte</code>	Byte enviado nos <i>timeslots</i> não mapeados
<code>mitfCfgPortLDRtest</code>	Habilitação de teste LDR (<i>Loop</i> Digital Remoto)
<code>mitfCfgPortRemoteManag</code>	Habilita gerência remota através da porta
<code>genDvAlCfgTrapSt</code>	Habilitação/Desabilitação de envio traps

4.6 Interface Ethernet

Ethernet é o nome dado para o padrão 802.3 do IEEE utilizado em Redes Locais (LAN) que emprega o método de acesso compartilhado aos meios de transmissão tipo CSMA/CD. A relação entre este padrão e as Camadas OSI é apresentada na figura a seguir.

Tabela 4.8: Relação entre IEEE 802 e Modelo OSI da ISO

Camada OSI		
7	Aplicação	
6	Apresentação	
5	Sessão	
4	Transporte	
3	Rede	Camadas IEEE 802
2	Enlace de dados	Controle do Enlace Lógico (Logical Link Control - LLC)
		Controle de Acesso ao Meio (MAC)
1	Física	Física

O IEEE 802.3 abrange diversos tipos de meios e técnicas para uma variedade de taxas de sinais. As famílias de sistemas suportados são a Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s) e Gigabit Ethernet (1 Gbit/s).

A Ethernet atual veio de um longo caminho desde que foi implementada nos anos 70, onde a Ethernet funcionou originalmente sobre um cabo coaxial espesso e forneceu aos usuários uma conexão compartilhada da largura de faixa de 10 Mbit/s.

A Ethernet logo progrediu e passou a funcionar sobre um par trançado metálico, oferecendo conexões dedicadas de 10 Mbit/s usando comutação. Hoje, a Ethernet comutada permite conexões dedicadas de 100 Mbit/s ao computador com troncos de 1 Gbit/s e, dentro de alguns anos, os peritos da indústria predizem 1 Gbit/s ao computador com troncos de 10 Gbit/s.

Em aproximadamente trinta anos de existência, a Ethernet tornou-se onipresente; uma tecnologia plug and play amplamente padronizada, que é usada em mais de noventa por cento das redes locais (LANs) corporativas que utilizamos. A Ethernet alcançou este nível de aceitação porque é simples de usar e muito barata.

Tabela 4.9: Tecnologias de Redes utilizadas em redes locais. Fonte: IDC, Julho 2001

Tecnologia de Redes	Ano 2000
Ethernet Total (10 Mbit/s, Fast E, Gigabit E)	91%
Wireless LAN	6%
Token Ring	3%
ATM	<1%

Tabela 4.10: Objetos monitorados para a interface Ethernet

Objeto da MIB	Descrição
sdhInfStatusItfEthSpeedMode	Velocidade de operação da porta
sdhInfStatusVcVcgLCASCtrl	Estado da máquina de estado do LCAS
sdhInfStatusVcgLCASAck	Indica qual dos membros de LCAS contém a sinalização
sdhInfStatusVcgLCASActiveRx	Número de VCs LCAs ativos em Rx
sdhInfStatusVcgLCASActiveTx	Número de VCs LCAs ativos em TX
sdhInfStatusVcgDiffDelay	Reporta o atraso de pacotes
sdhItfMultiGenOperation	Operação da porta (habilitada/desabilitada)
sdhMxPortsStCrSncpTribProtSt	Estado da proteção do tributário
sdhRxHoldOvrDiscardCnt	Contador do numero de frames descartados
sdhRxTotalBytesCnt	Contador do número de bytes recebidos
sdhRxTotalFrmCnt	Contador do número de frames recebidos
sdhStEpFifoStatElapsedTime	Tempo desde o último reset de contadores

sdhCfgCosConfigDiffServ	Habilita DiffServices
sdhCfgCosConfigQueuePolicy	Configura política na fila
sdhCfgCosConfigVlanTag	Configura <i>Tag</i> de VLAN
sdhCfgCosPortConfigPriority	Configura prioridade da porta
sdhCfgEpCfgProtocol	Configura modo de operação do GFP
sdhCfgPortVlanCfgPVID	Id da VLAN
sdhCfgSwitchCfgLoopDetection	Habilita a detecção de loops
sdhCfgSwitchCfgMode	Habilita função <i>Switch</i>
sdhFramePathProtCfgHoldoffTime	Tempo entre detecção de evento e disparo de alarme
sdhFrPathProtCfgRevertiveMode	Define comutação <i>protection->work</i>
sdhItfMultiGenAlarmDetection	Habilita detecção de alarme
sdhItfMultiGenAlarmPropagation	Habilita propagação de estado de alarme
sdhItfMultiGenEnableTests	Habilita execução de testes na interface
sdhItfMultiGenLinkFraming	Habilita análise de estrutura de frames
sdhItfMultiGenLinkSpeed	Configura velocidade do link
sdhItfMultiGenPathLabel	Configura o valor a ser inserido no <i>label</i> do <i>path</i>
sdhMultiItfEthCfgAutoNegotiation	Configura auto negociação

5 IDENTIFICAÇÃO DE OBJETOS SEMELHANTES.

Através das pesquisas entre os objetos monitorados de cada interface, foi possível identificar um grupo de características, configuráveis ou não, que aparecem na maioria, e por muitas vezes, em todas as interfaces de telecom.

A tabela abaixo apresenta os objetos monitorados de algumas das interfaces pesquisadas. Esses são os objetos apresentados anteriormente, também no formato de tabela, ao final da apresentação de cada interface de telecom do capítulo anterior.

Logo após, é apresentado o significado dos objetos em comum encontrados entre todas as interfaces pesquisadas. Dando ênfase para a importância de cada um deles na gerência de redes de telecom.

A partir do levantamento desses objetos em comum, pretendemos ter um grupo de objetos básicos para monitorar novas interfaces de telecom. Sendo assim, torna-se desnecessário pesquisar os objetos respondidos pela nova interface para começar o desenvolvimento do suporte a uma nova interface no sistema de gerência.

Tabela 5.1: Comparação de objetos gerenciáveis entre algumas das interfaces pesquisadas

V35	G703	FXS/FXO	E&M	G.SHDSL
mitfCfgPortOperation	mitfCfgPortOperation	mitfCfgPortOperation	mitfCfgPortOperation	mitfCfgPortOperation
mitfStCurrentPortTest	mitfStCurrentPortTest	mitfStCurrentPortTest	mitfStCurrentPortTest	mitfStCurrentPortTest
mitfStcurrentPortSlip	mitfStcurrentPortSlip	mitfStVoiceltfPowerSupply	mitfStVoiceltfPowerSupply	mitfStcurrentPortLink
mitfStDigitalItfCt105	mitfCfgG703CAS	mitfStVoiceltfOverheating	mitfStVoiceltfOverheating	mitfStDslltfLoopAtnDef
mitfStDigitalItfCt108	mitfCfgG703CRC4	mitfCfgVoiceltfEnSig	mitfCfgVoiceltfEnSig	mitfStDslltfSNRMarginDef
mitfStDigitalItfCt109	mitfCfgG703InitialTs	mitfCfgVoiceltfImpedance	mitfCfgVoiceltfImpedance	mitfStDslltfDataRate
mitfStDigitalItfCt113	mitfCfgG703LnImpedance	mitfCfgVoiceltfInterfSel	mitfCfgVoiceltfInterfSel	mitfStDslltfFrameMode
mitfStDigitalItfCt128	mitfCfgG703TS16	mitfCfgVoiceltfMetering	mitfCfgVoiceltfMetering	genDvInfPortHwld
genDvInfPortHwld	mitfCfgG703UnusedChann.	mitfCfgVoiceltfRingFilter	mitfCfgVoiceltfRingFilter	genDvInfPortFimVersion
genDvInfPortFimVersion	GenDvInfPortHwld	mitfCfgVoiceltfRxGain	mitfCfgVoiceltfRxGain	mitfCfgDslltfAnnex
MitfCfgDigitalItfClock	genDvInfPortFimVersion	mitfCfgVoiceltfSigCtrl	mitfCfgVoiceltfSigCtrl	mitfCfgDslltfUnitType
MitfCfgDigitalItfProtocol	MitfCfgPortBackup	mitfCfgVoiceltfSigMode	mitfCfgVoiceltfSigMode	mitfCfgPortAlarmDetection
MitfCfgDigitalItfSpeed	mitfCfgPortChannelsNum	mitfCfgVoiceltfSigSel	mitfCfgVoiceltfSigSel	mitfCfgPortBackup
MitfCfgDigitalItfTransMode	mitfCfgPortIdleByte	mitfCfgVoiceltfSigType	mitfCfgVoiceltfSigType	mitfCfgPortChannelsNum
MitfCfgPortBackup	mitfCfgPortLDRtest	mitfCfgVoiceltfTxGain	mitfCfgVoiceltfTxGain	mitfCfgPortIdleByte
MitfCfgPortChannelsNum	mitfCfgPortRemoteManag	genDvInfPortHwld	genDvInfPortHwld	mitfCfgPortLDRtest
MitfCfgPortIdleByte	genDvAICfgTrapSt	genDvInfPortFimVersion	genDvInfPortFimVersion	mitfCfgPortRemoteManag
MitfCfgPortLDRtest		mitfCfgPortBackup	mitfCfgPortBackup	genDvAICfgTrapSt
mitfCfgPortRemoteManag		mitfCfgPortChannelsNum	mitfCfgPortChannelsNum	
genDvAICfgTrapSt		mitfCfgPortIdleByte	mitfCfgPortIdleByte	
		mitfCfgPortLDRtest	mitfCfgPortLDRtest	
		mitfCfgPortRemoteManag	mitfCfgPortRemoteManag	
		genDvAICfgTrapSt	genDvAICfgTrapSt	

A primeira característica em comum a ser ressaltada, é o objeto que identifica a **operação da interface**, ou seja, o objeto que possibilita habilitar e desabilitar o seu funcionamento, ligar ou desligar sua operação. Todas as interfaces de telecom pesquisadas podem ser habilitadas e desabilitadas. Muitas vezes cada porta de determinada interface possui essa facilidade, podendo-se habilitar o funcionamento de algumas portas e deixar outras desabilitadas, de acordo com o uso e os mapeamentos já existentes em determinada interface.

Para identificar qual o modelo das interfaces que estão sendo acessadas pelo sistema de gerência, todas as interfaces pesquisadas (ver tabela 5.1) possuem um objeto que identifica o **modelo ou tipo da interface**. Muitas vezes o sistema de gerência recebe um evento identificado por *hostname* e *slot*, e através da consulta do objeto que identifica o modelo da interface, o gerente toma medidas diferentes para a resolução do problema informado pelo evento. Através desse objeto, também são identificados os outros objetos que devem ser consultados no *polling* do equipamento/interface.

Objetos responsáveis por iniciar e terminar **testes nas portas das interfaces** também foram encontrados em quase todas as interfaces pesquisadas (como mostra a tabela 5.1). As interfaces diferem nos testes possíveis de serem realizados, como *loops* analógicos, *loops* digitais, testes de laser ou testes de BERT. A maioria das interfaces pesquisadas pode sofrer testes analógicos e digitais. Um software de gerência precisa demonstrar ao usuário que interfaces e equipamentos estão passando por testes, sendo, portanto, desejável que os objetos de testes sejam monitorados. Além disso, é necessário que possam ser executados testes remotamente com o auxílio do software gerência.

Todas as interfaces pesquisadas possuem uma determinada **taxa de transmissão**, podendo essa ser configurada algumas vezes, e em outras vezes apenas verificada através dos softwares de gerência. Torna-se fundamental para um software de controle de equipamentos de rede, verificar a taxa de transmissão sendo exercida por determinada interface, pois algumas podem sofrer queda na taxa de transmissão quando ocorrem muitos erros de transmissão, e esse tipo de erro deve ser automaticamente verificado pelo gerente de rede.

Algumas interfaces possuem as suas taxas de transmissão fixas, como interfaces E1, E3 ou STM-1, outras disponibilizam apenas dados como o número de bytes ou pacotes com erros.

Todos os equipamentos e interfaces que são gerenciados através do protocolo SNMP podem ter a configuração de envio de **traps SNMP**. Essas configurações de envio de traps do agente SNMP, podem ser basicamente de dois tipos: configuração de envio de *trap* por tipo ou configuração de envio de traps para a interface toda. A habilitação de *traps* SNMP faz com que o gerente possa receber as informações de alteração na configuração, alteração no hardware do equipamento ou alterações no *status* do equipamento/interface no momento em que a alteração é detectada por parte do agente SNMP.

A gerência de alarmes, como mostrado anteriormente, é outro fator primordial na hora de se decidir por um sistema de gerência. Um bom sistema de gerência precisa saber dos alarmes no equipamento/interface no momento em que esses alarmes ocorrem, tornando possível a correção do erro de forma rápida. Todas interfaces pesquisadas possuíam ou uma lista de alarmes ativos na interface ou um objeto que identificasse os números dos alarmes ativos.

A verificação do **estado dos links** das portas de uma interface é de vital importância para as redes de telecomunicação, posto que com a queda de um link pode ser interrompida uma importante linha de voz e/ou dados, que muitas vezes implica no pagamento de multas por parte das operadoras de telecom. O estado do link é possível de ser verificado em todas as interfaces pesquisadas, como mostra a tabela 5.1.

Todos os equipamentos que possuem um agente SNMP, ou mesmo um agente que responda a um outro protocolo de gerência, possui um *firmware* relacionado com esse agente. *Firmware*, nada mais é do que uma programação em hardware, programa ou dados de computador que são armazenados permanentemente em um chip de memória de hardware como uma ROM ou EPROM. **A versão de *firmware*** que está sendo executada no equipamento/interface é outra informação muito importante, pois muitas vezes as informações disponíveis para gerência diferem de uma versão para outra, ou mesmo o funcionamento do dispositivo pode ter diferenças significativas. Através do modelo e da versão de *firmware*, identifica-se um equipamento quando este apresenta problemas, junto às empresas que desenvolvem equipamentos de telecomunicações.

A **data de release** de um *firmware* é outro dado importante para identificarmos uma versão de software de uma interface, pois uma vez identificado um problema no software, é interessante buscar na rede da empresa de telecom outras interfaces que possuem a mesma data de *release*, pois o problema pode voltar a acontecer.

O tempo de **Up Time** de determinado equipamento, informa o tempo de operação, permitindo verificar alguma eventual parada na transmissão de dados ou mesmo verificar desde quando o equipamento/interface está em funcionamento. Essa informação é vinculada ao equipamento, mas permite deduzir informações do tempo de uso das interfaces contidas no equipamento.

O **número serial** de uma interface possibilita identificá-la de forma única. Dessa maneira é possível saber a proveniência de uma determinada placa, data de sua compra, desde quando está em produção e até mesmo buscar um lote inteiro de interfaces com problemas. Nem todas as interfaces pesquisadas possuíam essa informação disponível para a gerência, mas todos os equipamentos PDH e SDH pesquisados possuíam esse objeto.

Outro objeto que constou várias vezes nas listas de objetos respondidos pelas interfaces foi o objeto que identifica a **versão de hardware** da interface. Através deste, o gerente pode identificar as funcionalidades que podem existir a partir de uma determinada versão de hardware, e pode identificar um lote completo de interfaces com problema na sua rede.

Objetos que apresentam as **estatísticas de erro** também são comuns, principalmente entre as interfaces que utilizam o protocolo *Ethernet* como *Bridges* ou tributários *Ethernet* PDH. Algumas placas SDH também possuem objetos de estatísticas. Porém os objetos de estatística diferem muito entre cada interface de rede, impossibilitando que o software de gerência seja automaticamente alimentado com a informação do objeto correto a ser recuperado.

Com o desenvolvimento de interfaces que operam em altas frequências, utilizando processadores com clock que também operam em frequências altas, a **temperatura da interface** passa a ser um aspecto importante a ser monitorado. Muitas vezes ocorre degradação da performance ou até a perda de uma interface devido à sua operação em temperaturas altas.

Normalmente, o objeto que monitora a temperatura de uma determinada placa possui um outro objeto que informa os **limites de temperatura** que essa placa pode operar sem gerar degradação do sinal ou dano à mesma. Podem ser configurados alarmes para quando a temperatura superar esse limite, ou mesmo, configurar o desligamento da placa quando a temperatura chegar a valores perigosos.

Outro objeto que passa a ser importante devido a interfaces que operam na velocidade de gigahertz, é o de **estado de operação das fans** (ventiladores) que dissipam o calor gerado em cada placa. Às vezes, existe mais de um ventilador acoplado na placa e, portanto, um objeto de estado para cada um desses ventiladores. Outras vezes existe outro objeto associado que informa a velocidade de operação desse ventilador que aparece na gerência na forma gráfica.

6 DEVICE COMPARE 1.0

No desenvolvimento de softwares de gerência de telecom, são identificados objetos que serão considerados para derivar a situação de cada interface, objetos que possibilitam alterar as configurações de operação, objetos que disponibilizam testes remotos para o usuário e objetos que ajudam a identificar cada interface e cada equipamento.

O trabalho de encontrar esses objetos é feito pelos engenheiros que desenvolvem cada novo equipamento ou nova interface. Esses profissionais devem ter o cuidado de disponibilizar os objetos que podem ser configurados com os seus valores possíveis e os objetos que vão apresentar as falhas em cada interface do equipamento.

Cada interface possui suas características e peculiaridades como foi visto no capítulo anterior, porém, existe um grupo de objetos que estão presentes em todas as interfaces ou em um grupo grande delas.

Esses objetos são cadastrados na base de dados dos softwares de gerência para serem recuperados durante o *polling* periódico, ou durante o *polling* acionado através de eventos enviados pelos equipamentos. Muitas vezes, um mesmo objeto, comum a várias interfaces de telecom ou a vários equipamentos, é cadastrado mais de uma vez.

Buscando evitar esse tipo de inserção desnecessária na base de dados dos softwares de gerência, e buscando facilitar o desenvolvimento do suporte a novas interfaces nos sistemas de gerência, foi realizada uma pesquisa com o intuito de identificar as semelhanças entre as interfaces de redes de telecomunicação e os objetos aos quais comumente essas interfaces respondem, para que, dessa maneira, os engenheiros possam preocupar-se em passar aos programadores as informações das novidades que a nova interface/equipamento apresenta, e o software de gerência já recupere esse grupo de objetos em comum automaticamente.

Visando auxiliar na detecção dos objetos gerenciáveis de cada interface, e buscando essas semelhanças entre os objetos respondidos em cada uma delas, foi desenvolvido um software utilizando a linguagem java e um banco de dados preenchido com as interfaces suportadas pelo software de gerência dos equipamentos da empresa DATACOM.

A ferramenta de comparação desenvolvida, batizada de ***Device Compare***, compara os objetos de configuração e estado de dois dispositivos selecionados pelo usuário, podendo mostrar todos os objetos gerenciáveis ou apenas as diferenças e semelhanças entre eles. O software ainda compara os alarmes cadastrados para ambas as interfaces, mas não será objeto de estudo desse trabalho.

6.1 Descrição

Para auxiliar na procura por semelhança entre os objetos gerenciáveis das interfaces de rede pesquisadas, foi desenvolvido a ferramenta *Device Compare*. O software foi desenvolvido visando auxiliar no desenvolvimento dessa dissertação, mas também possui cunho comercial, pois visa facilitar a inserção de novas interfaces gerenciáveis através da comparação com interfaces já suportadas pelo software DmView e desenvolvidas pela DATACOM. Portanto, atinge outros campos de gerência de redes, como visualização das traps cadastradas na base de dados, possibilidade de inserção de novas traps, visualização dos alarmes cadastrados e possibilidade de inserção de novos alarmes, além dos objetos monitorados por modelo de interface e por equipamento que será utilizado nessa dissertação.

O software foi desenvolvido utilizando a linguagem Java 5.0 acessando uma base de dados do software de gerência DmView da empresa DATACOM. Foi preciso acessar a base deste software de gerência devido a necessidade de buscar objetos gerenciáveis por modelo de interface ou por equipamento. A base de dados do DmView possui os objetos separados entre objetos de configuração e objetos que derivam estado da interface.

Outra informação interessante recuperada através do *Device Compare*, é o protocolo utilizado para buscar o objeto gerenciável. No caso da base de dados utilizada, existiam objetos recuperados por SNMP e por PCGA (Protocolo proprietário da DATACOM e, portanto, confidencial).

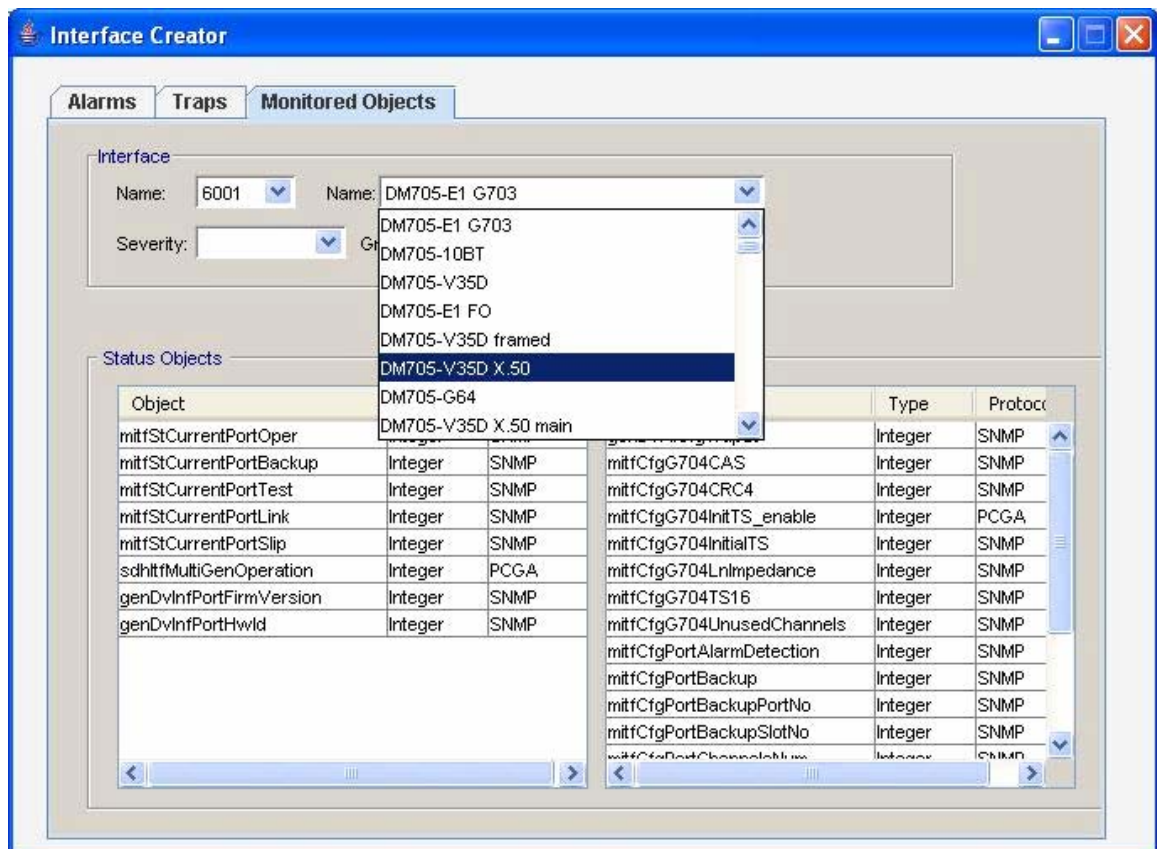


Figura 6.1: Ferramenta *Device Compare*

6.2 Apresentação do Software

Na primeira versão do software, este possui um painel com três abas, a primeira aba apresenta os alarmes já cadastrados no software na base de dados e a possibilidade de inserção de novos alarmes. Os alarmes normalmente são recebidos através de uma lista de alarmes nos softwares de gerência de equipamentos de telecomunicações, e informam várias situações de erro de equipamentos e interfaces.

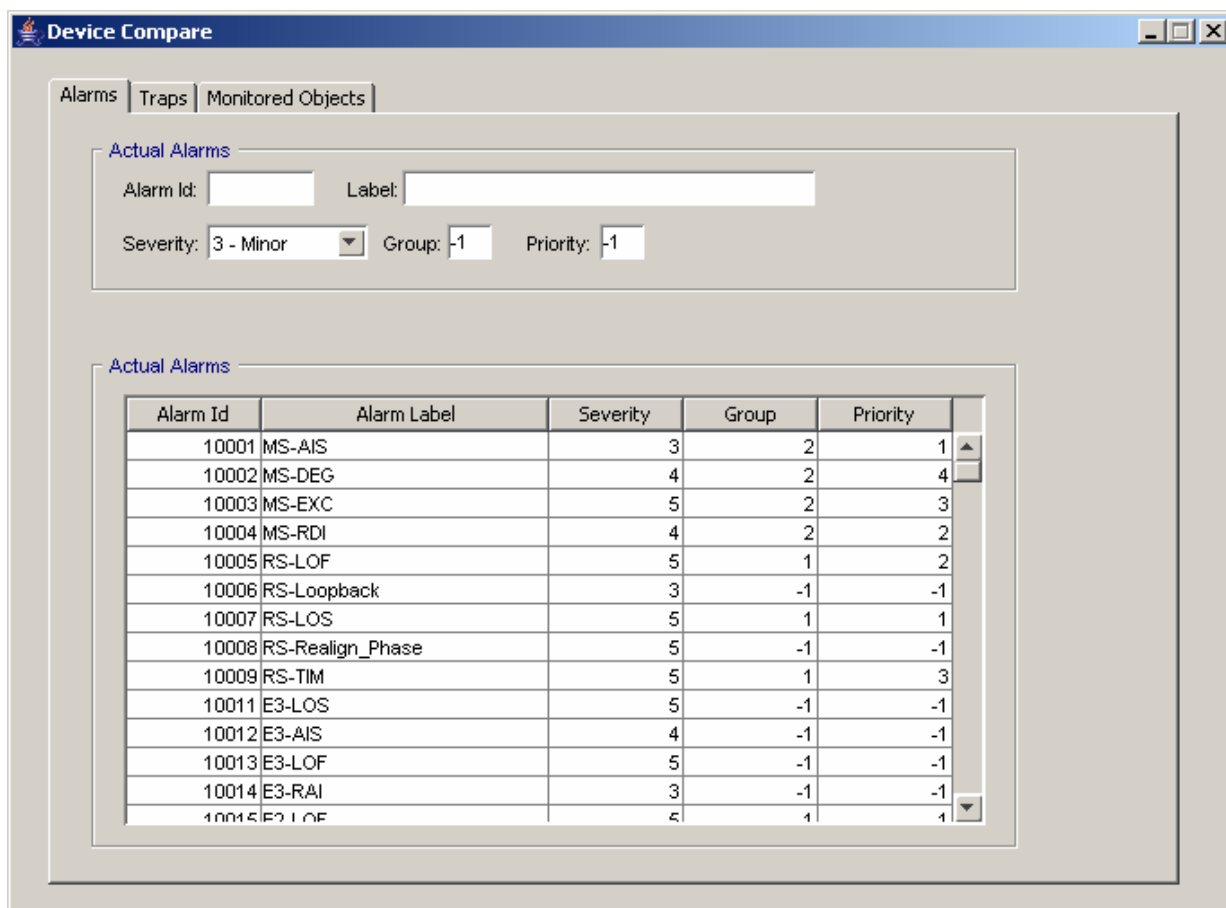


Figura 6.2: Cadastro de Alarmes no *Device Compare*

A segunda aba apresenta as traps cadastradas na base de dados, com os valores possíveis de serem assumidos por cada trap e a descrição do evento ocorrido no equipamento que deverá ser mostrado na janela de recepção de eventos do software DmView.

A terceira aba apresenta os objetos monitorados separados por interfaces, podendo mostrar as semelhanças entre cada interface em termos de objetos monitorados.

6.3 Estrutura do Software

O software foi desenvolvido de forma modular em quatro pacotes Java.

O pacote principal é responsável pela inicialização do sistema. A classe *MainClass* faz a inicialização dos vetores estáticos, faz a chamada dos métodos que acessam a base de dados do sistema de gerência para recuperar os objetos gerenciados por interface,

recupera os alarmes cadastrados, *traps* cadastradas e por fim apresenta a tela principal do software.

O pacote *GUI (Graphical User Interface)* é responsável pelas janelas gráficas do sistema. Na primeira versão do software existe uma classe responsável pela apresentação da janela de objetos monitorados para cada interface do sistema de gerência, possibilitando também a entrada de novos objetos gerenciados. Nessa janela, é possível visualizar os objetos gerenciados de duas interfaces ao mesmo tempo, possibilitando a comparação entre elas. Essa facilidade foi muito utilizada na verificação das semelhanças e diferenças entre as interfaces, objeto principal dessa dissertação.

Outra classe é responsável pela janela de visualização das *traps* cadastradas no sistema de gerência. No sistema de gerência *DmView* (sistema de gerência dos equipamentos Datacom), as *traps* são registradas independente de interface ou equipamento, fazendo com que a entrada de uma nova *trap* na base de dados possibilita a recepção e entendimento dessa *trap* independente do equipamento responsável pelo seu envio.

Por fim, a terceira janela disponível apresenta os alarmes cadastrados no sistema de gerência, e, da mesma forma que o cadastro de *traps*, os alarmes são cadastrados independente de equipamento ou interface no sistema de gerência *DmView*

Existe uma quarta classe (*GuiUtils*) que provê métodos que facilitam a disposição e apresentação de componentes gráficos nas janelas do sistema.

O pacote *Network* contém as classes que fazem a abstração dos elementos das redes de telecomunicação. Na primeira versão do software o pacote possui duas classes. A classe *MngObject* que faz a abstração dos objetos gerenciáveis das interfaces e equipamentos, e a classe *NetworkInterface* que faz a abstração das interfaces de cada equipamento da base de dados.

O pacote *Utils* possui a classe *Database* responsável por todos os acessos à base de dados, a classe *DefaultTableModel* responsável pela estrutura das tabelas que são apresentadas no software (tabela com os objetos gerenciáveis por interface, tabela de alarmes cadastrados no sistema de gerência e a tabela de *traps*) e a classe *UIDefaults* que apresenta os valores padrão para cores, tamanho de botões e valores de funcionamento geral do sistema.

Para facilitar o entendimento das associações entre as classes, foi desenvolvido um diagrama de classes UML, como mostra a figura 5.3. Os atributos gráficos foram removidos para facilitar a visualização das classes e atributos que pertencem às regras de negócio do software. As classes *GuiUtil*, *Database*, *DefaultTableModel* e *UIDefaults* são utilizadas nas três janelas gráficas (janela de alarmes, *traps* e de objetos monitorados por interface), mas não tiveram suas associações apresentadas também para facilitar a visualização.

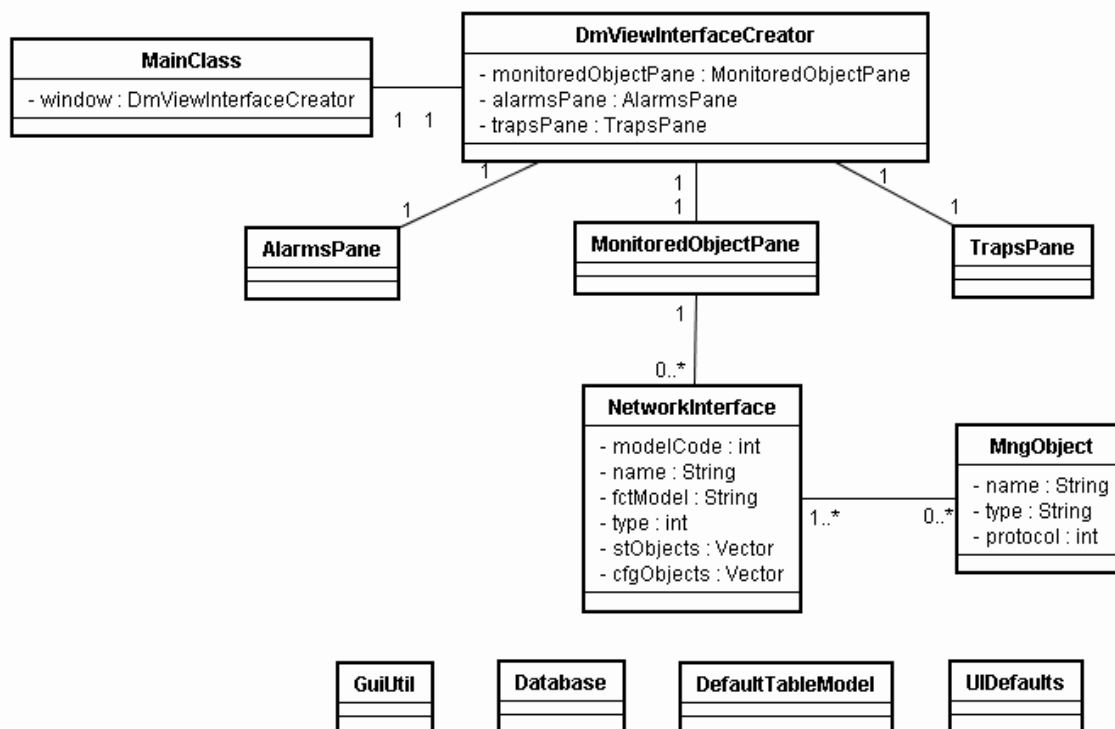


Figura 6.3: Diagrama de Classes UML

Com base nas descrições e recomendações das interfaces pesquisadas e com o auxílio da ferramenta (*Device Compare*), foram encontradas várias características e possíveis maneiras de configurá-las em comum e que na maioria das vezes são transformadas em objetos remotamente gerenciáveis via protocolos de gerência como SNMP. Esses objetos que devem ser monitorados para facilitar o monitoramento de redes de telecom por parte de gerentes de rede, através dos softwares de gerência de redes, ou NMSs (*Network Management Systems*).

Buscando facilitar o desenvolvimento do suporte de novas interfaces nos softwares de gerência de redes de telecom, iremos demonstrar o resultado da pesquisa que tentou relacionar as semelhanças entre as interfaces de telecom utilizadas atualmente, ou seja, objetos que podem ser verificados ou configurados por todas as interfaces ou na sua maioria. De posse desses dados, será possível identificar falhas e efetuar modificações na configuração de novas interfaces nos softwares de gerenciamento, bastando inserir na base de dados desses softwares, os objetos que, com certeza, a interface possui nas suas bases de gerenciamento.

6.4 Estudo de caso - Suporte à interface Tr24E1

Para iniciar o desenvolvimento do suporte a uma nova interface no sistema de gerência, normalmente é solicitado para os profissionais que desenvolveram uma nova tecnologia, que especifiquem os objetos de configuração e de estado que deverão ser monitorados ou apresentados pelo software de gerência.

Existe um problema histórico nesse processo que é a falta de conhecimento de gerência de equipamentos de rede por parte dos profissionais de engenharia que

desenvolvem as interfaces de telecom, resultando numa falha de comunicação que ocasiona o esquecimento de objetos fundamentais para a gerência do equipamento, ou o acesso à objetos muitas vezes desnecessários para a configuração desse equipamento.

Para evitar esse tipo de problema, é necessário fazer a filtragem da informação passada pelos engenheiros aos desenvolvedores do software de gerência. Esse trabalho é realizado por alguém que trabalha diretamente no desenvolvimento do software de gerência, verificando um a um os objetos que foram passados como importantes para derivar o estado do equipamento ou para configurá-lo.

Como exemplo de suporte de uma nova interface no sistema de gerência, vamos citar aqui o desenvolvimento do suporte ao tributário 24E1 elétrico do equipamento DmSTM-1 desenvolvido recentemente pela empresa Datacom-Telemática. Após o desenvolvimento da interface (parte de hardware, lógica programável e software embarcado), foram passados às pessoas que desenvolvem o sistema de gerência todos os objetos respondidos pela interface. Porém, uma boa parte dos objetos que foram passados, não são interessantes de serem monitorados pelo software de gerência.

Muitas vezes, são criados documentos que descrevem o funcionamento de uma interface para ser utilizado dentro da empresa. Esses documentos sempre auxiliam no desenvolvimento da gerência, pois apresentam as configurações possíveis e algumas coerências a serem verificadas na configuração, mas de um modo geral, eles não possuem os objetos que devem ser monitorados, gerando sempre um trabalho de pesquisa por parte dos desenvolvedores do sistema de gerência.

Com o auxílio da lista de objetos padrão que foi criada a partir das pesquisas realizadas durante este trabalho, já temos um grupo básico de objetos que a interface deverá responder para o sistema de gerência. No primeiro teste da interface na gerência, foi constatado que o objeto de habilitação de operação da interface e o objeto onde são feitos os testes na interface não estavam sendo respondidos. Após a correção por parte do profissional que desenvolveu o software embarcado da interface, passamos para a monitoração dos objetos específicos da nova tecnologia.

Com a ferramenta desenvolvida, é possível verificar os objetos gerenciáveis para as outras interfaces já suportadas para o equipamento DmSTM-1 e, verificar os objetos gerenciados de interfaces que possuam portas E1 (já que a nova interface tem basicamente 24 portas E1 que são *cross-conectadas* em um agregado STM-1), ou mesmo, interfaces que trafegam sinais elétricos já suportadas, para verificar os tipos de testes que possam ser feitos, já que a maioria das interfaces do equipamento DmSTM-1 utiliza sinais óticos.

Na figura 6.4, são apresentados os objetos gerenciados pela interface Tr-Eth do mesmo equipamento, e os objetos gerenciados pela interface E1 de um equipamento PDH (Dm705), sendo comparados no software *Device Compare*.

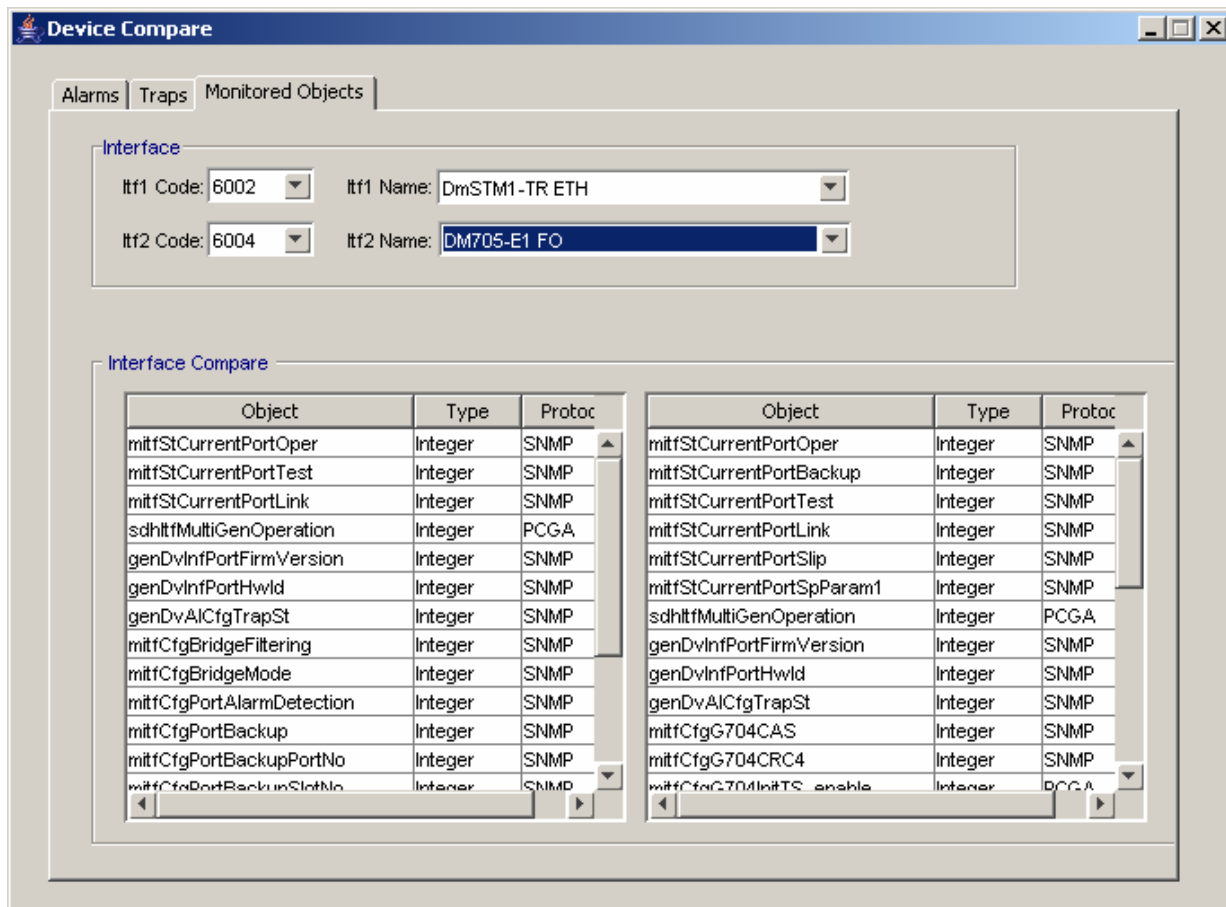


Figura 6.4: Objetos da interface Tr-Eth do equipamento DmSTM-1 e interface E1 do Dm705 sendo comparados

Os objetos em comum identificados entre as interfaces Tr-Eth (tributário ethernet) e a interface E1 elétrica de outro equipamento, são inseridos na base de dados do sistema de gerência para que possam ser monitorados para a nova interface Tr 24E1

A utilização da ferramenta elimina a utilização de um especialista no desenvolvimento da gerência das interfaces de telecom. O processo passa a ser mais automático e menos subjetivo, já que o desenvolvimento do suporte na gerência agora está baseado na comparação direta entre interfaces semelhantes através do *Device Compare*, e, principalmente, nos objetos indispensáveis na monitoração dessas interfaces obtidos através da pesquisa entre várias interfaces utilizadas no mundo de telecom no Brasil.

7 CONCLUSÃO

Através das pesquisas entre as diferentes interfaces de redes de telecomunicações, foi possível identificar características físicas e lógicas. As características físicas mostraram-se pouco aproveitáveis em termos de gerência de redes por serem, muitas vezes, inalteráveis e próprias da recomendação e da implementação da interface, mas, foram fundamentais para que fosse entendido o funcionamento de cada uma das interfaces, suas peculiaridades de configuração e as possibilidades de uso real de cada tecnologia.

As características lógicas e passíveis de serem alteradas através de um software de gerência ou objetos que sofriam alteração durante o uso da interface, acabaram sendo o objeto principal de estudo do trabalho. Identificando os objetos que denotavam falhas e que eram configurados pelos usuários através de softwares de gerência, foi possível identificar uma gama bastante razoável de objetos comuns entre as interfaces e equipamentos de telecom, com o auxílio do software desenvolvido para concretizar essa dissertação.

Foram encontrados vários objetos de configuração em comum nas interfaces pesquisadas. Porém as configurações de cada interface e de cada equipamento precisam passar por uma verificação de coerência, visto que algumas configurações não podem ser efetuadas concomitantemente com outras configurações. O levantamento das coerências necessárias para efetuar uma alteração na configuração de um equipamento, e até mesmo o levantamento das possibilidades de configuração de cada objeto configurável, abre uma brecha para futuros estudos, pois notou-se que outra dificuldade na atualização dos sistemas de gerência é justamente atualizar as coerências para novos objetos e interfaces, que normalmente são feitas pelos desenvolvedores a cada nova versão dos softwares de gerência.

O software desenvolvido para a concretização dessa dissertação de mestrado (*Device Compare 1.0*), já está sendo utilizado de forma prática na empresa Datacom-Telemática, que desenvolve tanto equipamentos de telecomunicação quanto o seu próprio sistema de gerência e, atualmente já está suportando a gerência de interfaces e dispositivos de telecomunicações de outros fabricantes.

Existem melhorias latentes a serem feitas no software desenvolvido. A mais importante delas é identificar a partir de dados fornecidos pelo usuário a semelhança de uma nova tecnologia em relação às interfaces já existentes. Hoje, a identificação é realizada pelo usuário do software, necessitando do conhecimento de especialista.

Utilizando o software, foi possível desenvolver o suporte de gerência de falhas para a interface 32E1 de um equipamento SDH, utilizando os objetos gerenciados da interface tributária G. 703 E1 de um equipamento PDH e os objetos conhecidos na gerência de falhas da interface tributária 24E1 de outro equipamento SDH. O software

também pode ser utilizado no setor de suporte da empresa, já que através dele é possível verificar os objetos que podem levar uma interface a aparecer em estado de falha no software de gerência e o protocolo que deverá ser usado para recuperar o valor dos objetos.

A falta de padronização de MIBs SNMP e até de protocolos de acesso aos equipamentos na área de telecomunicações também foi uma descoberta feita a partir das pesquisas realizadas no início desse trabalho. Pela quantidade de portas e objetos que os equipamentos SDH possuem, (por exemplo), o protocolo SNMP torna-se inviável, fazendo com que as empresas que desenvolvem esses equipamentos acabem também desenvolvendo protocolos proprietários, para que seja possível transmitir uma quantidade maior de informação sem muitas trocas de pacotes entre a gerência e o equipamento de telecom.

Embora existam softwares de gerência de telecom há bastante tempo e existam alguns trabalhos publicados sobre boas práticas na área de gerência de telecom, os primeiros esforços no sentido de facilitar a utilização desses softwares de gerência estão sendo feitos há pouco tempo. Estão surgindo os chamados “softwares de gerência de nível superior”, que mostram os dados de vários softwares de gerência dos mais diversos fabricantes e não se preocupam com o protocolo que vai ser utilizado para ativar configurações nos equipamentos. Eles fazem chamadas de API dos softwares de gerência dos fabricantes, podendo configurar redes heterogêneas com múltiplos protocolos de acesso aos equipamentos.

Hoje a idéia de padronizar objetos e protocolos utilizados em telecom é um sonho antigo, devido, principalmente ao parque de equipamentos instalados e em produção no país e no mundo. Grandes empresas como a Cisco, tentam fazer as suas interfaces com o usuário tornarem-se um padrão de fato, outras tentam fazer um esforço em conjunto no sentido de padronizar pelo menos as MIBs utilizadas na representação dos dados. Enquanto isso, ferramentas como a desenvolvida nesse trabalho e estudos a partir de objetos básicos utilizados nas interfaces, são fundamentais na tentativa de tornar mais fácil o suporte de novas tecnologias nos softwares de gerência, diminuindo o tempo de desenvolvimento e o tempo de lançamento de novas versões no mercado.

REFERÊNCIAS

- ADDPAC TECHNOLOGY. **E&M Guide**. Disponível em: <www.addpac.com>. Acesso em: set. 2005.
- ARTOLA, E. **OlhoVivo: Sistema Especialista para Gerência Pró-Ativa Remota**. 1996. Dissertação (Mestrado em Ciência da Computação) - Instituto de Informática, UFRGS, Porto Alegre.
- ASGA. **Manual do Multiplexador STM-1 MMO 63E1**. Disponível em: <www.asga.com.br> Acesso em: set. 2005.
- BATEMAN, A. **Digital Communications: Design for the Real World**. Reading, MA: Wesley, 1999.
- BEN-ARTZI, A.; CHANDNA, A.; WARRIES, R. U. Network Management of TCP/IP Networks: Present and Future. **IEEE Network Magazine**, New York, v. 4, n. 4, p. 35-43, July 1990.
- BIERMAN, N. **Network Management Observations**. [S.l.]: IETF, 2002.
- CISCO SYSTEM INC. **Analog E&M Voice Signaling Overview**. Disponível em: <http://www.cisco.com/warp/public/788/signalling/e_m_overview.html>. Acesso em: jan. 2006.
- DATACOM. **Dm705-Cpu32 - MuxE1: Manual de Instalação e operação**. [S.l.], 2000.
- DIAS, B. **Protocolo de Gerenciamento SNMP**. Disponível em: <http://mesonpi.cat.cbpf.br/naj/snmp_color.pdf>. Acesso em: out. 2005.
- DIGITEL. **Manual do Access Mux AD**. Disponível em: <www.digitel.com.br> Acesso em: set. 2004.
- DUARTE, E. P. **Desafios de Gerência e Segurança de Redes**. [S.l.]: DInfo, UFPR, 2003.
- HUNT, C. **TCP/IP Network Administration**. [S.l.]: ÓReilly & Associates, 1992.
- INFO WESTER. Disponível em: <<http://www.infowester.com/adsl.php>>. Acesso em: fev. 2006.
- KLERER, S. The OSI Managements Architecture: an Overview. **IEEE Network**, New York, v.2, n.2, p.20-29, Mar.1988.
- NASCIMENTO, M.; TAVARES, A. **Tecnologia de Acesso em Telecomunicações**. São Paulo: Berkeley, 2002.
- NATIONAL SEMICONDUCTOR. **LM75 Digital Temperature Sensor and Thermal Watchdog with Two-Wire Interface**. [S.l.], 2005.
- OPENNMS. Disponível em: <www.opennms.org> Acesso em: jan. 2006.
- PAN, H. **SNMP-Based ATM Network Management**. [S.l.]: Artech House, 1998.

PROJETO de cabeamento e conexão. Disponível em: <http://www.projetoderedes.com.br/novas_dicas_cabeamento.html> Acesso em: out. 2004.

ROCHOL, J. Notas de Aula da disciplina de Redes de Computadores. 2002. Instituto de Informática, UFRGS, Porto Alegre

SAUVÉ, J.; NICOLLETTI, P.; LOPES, R. **Melhores Práticas para a Gerência de Redes de Computadores**. Rio de Janeiro: Campus, 2003.

SILVA, A. Introdução ao Gerenciamento de Redes TCP/IP. **Boletim Bimestral sobre Tecnologia de Redes**, Rio de Janeiro, v 1, n. 3, ago. 1997.

SOARES, L. F. **Redes de Computadores: das LANs, MANs e WANs às Redes ATM**. 2. ed. Rio de Janeiro: Campus, 1995.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2**. 3rd ed. Reading: Addison Wesley, 1999.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

TAROUCO, L. M. R.. Notas de Aula da disciplina de Gerência de Redes. 2005. Instituto de Informática, UFRGS, Porto Alegre.

TUTORIAL Redes ópticas. Disponível em: <<http://www.teleco.com.br/>>. Acesso em: jun. 2006.