Universidade Federal de Santa Catarina
Centro Tecnológico
Curso de Engenharia de Controle e Automação Industrial - UFSC

UM AGENTE SNMP PARA CENTRAIS TELEFÔNICAS DE PEQUENO PORTE

Monografia submetida à Universidade Federal de Santa Catarina como requisito para a Aprovação da disciplina:
EEL 5901: Projeto de Fim de Curso

Frederico Rabello de Moraes

Florianópolis, Fevereiro de 1998

UM AGENTE SNMP PARA CENTRAIS TELEFÔNICAS DE PEQUENO PORTE

Frederico Rabello de Moraes

Esta monografia foi julgada no contexto da disciplina EEL 5901: Projeto de Fim de Curso e aprovada na sua forma final pelo Curso de Engenharia de Controle e Automação Industrial

Banca Examinora:

Eng. Guido Garcia D'Angelo
Orientador da empresa

Eng. Wilson Libanio da Costa Junior
Orientador da Empresa

Professor Carlos Alberto Maziero
Orientador do Curso

Prof. Augusto Humberto Bruciapaglia
Responsável pela disciplina e Coordenador do Curso

Prof. Werner Kraus Junior
Avaliador

Aluno Daniel Albino
Debatedor

Aluno Daniel M. Kamers
Debatedor

Agradecimentos

Gostaria de primeiramente agradecer aos meus pais, irmãos e toda a minha família pela oportunidade que me deram de estar vivo e de poder cursar um curso superior, dando-me todo o a apoio e amor necessário para tornar-me hoje o que sou.

Da mesma forma gostaria de agradecer a Liege e sua família por terem me acompanhado de perto por todo este período de fim de curso.

Em especial gostaria de agradecer ao Wilson Libanio e a Guido D'Angelo e a todos aqueles com quem trabalhei na Telesc por terem me auxiliado no trabalho e desde a idealização até a sua redação final.

Por fim gostaria de agradecer ao Prof. Maziero e Prof. Augusto por terem me acompanhado e instruído por todos os meses de trabalho e é claro a todo a Curso de Automação desde seus alunos até os professores e a UFSC por ser uma Universidade pública gratuita e de qualidade, rogando que as próximas gerações tenham a mesma oportunidade que eu tive.

Sumário

Simbologia

ASN.1	*Abstract Syntax Notation One*
ARMC	*Armação - Pântano do Sul*
BA	*Boletim de Anormalidade*
BECZ	*Bairro Bela Cruz*
BNU	*Blumenau*
BRLG	*Barra da Lagoa*
BSC3	*Binary Synchronous Communication 3*
CCO	*Chapecó*
CCT	*Central de Comutação Telefônica*
CGIR	*Centro de Gerência Integrado de Rede*
CMIP	*Common Management Information Protocol*
CMU	*Carnegie Mellon University*
CPA	*Controlada por Programa Armazenado*
CPA-T	*Comutação Temporal Controlada por Programa Armazenado*
CPqD	*Centro de Pesquisa e Desenvolvimento*
CRC	*Cyclic Redundancy Code*
CRDR	*Costeira do Ribeirão*
CTPP	*Centrais Telefônicas de Pequeno Porte*
CUA	*Criciúma*
FM	*Frequency Modulation*
FNS	*Florianópolis*
FTP	*File Transfer Protocol*
GNU	*GNU is Not UNIX*
GPL	*GNU Public License*
IEA	*Itapema*
IPC	*Inter Process Comunication*

ISO	*International Organization for Standardization*
JVE	*Joinville*
LAN	*Local Area Network*
LGDC	*Lagoa da Conceição*
LGS	*Lages*
MIB	*Management Information Base*
MIT	*Management Information Tree*
MOPS	*Morro das Pedras*
NE	*Network Element*
NMS	*Network Management Station*
NTSP	*Nova Telessupervisão*
OS	*Sistemas de Operação*
OSI	*Open Systems Interconnection*
PAC	*Palhoça*
PC	*Personal Computer*
PDU	*Protocol Data Unit*
PFRA	*Praia de Fora*
PPP	*Point to Point Protocol*
RFC	*Request for Comment*
SDH	*Synchronous Digital Hierarchy*
SGBD	*Sistema Gerenciador de Banco de Dados*
SIORE	*Sistema de Operações Remotas*
SNMP	*Simple Network Management Protocol*
SNT	*Sistema Nacional de Telecomunicações*
SO	*Sistema Operacional*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TELESC	*Telecomunicações Santa Catarina*
TFTP	*Trivial File Transfer Protocol*
TMN	*Telecommunications Management Network*
TSP	*Telessupervisão*

WAN	*Wide Area Network*
ZTX-CTZ	*Centralizado Zetax*

LISTA DE FIGURAS

Resumo

Este projeto está inserido na área de Gerência de Redes de Telecomunicações e consiste de uma aplicação agente SNMP para gerenciamento de falhas em centrais telefônicas de pequeno porte.

Palavras-chave: Gerência de Redes de Telecomunicações, Supervisão de Equipamentos, Gerenciamento de falhas, Centrais telefônicas de pequeno porte .

Abstract

This project is inserted at Telecommunications Management Network area and consists of an agent management aplication for Failure Management in Small Sized Switchs.

Keywords: Telecommunications Management Network, Equipments Supervision, Failure Management, Small Sized Switch.

Introdução

A multiplicidade de equipamentos e a exigência por qualidade nos serviços prestados pelas concessionárias de Telecomunicações alavancam a necessidade de gerência integrada da rede e dos serviços de Telecomunicações.

Os serviços de Telecomunicações são suportados por três elementos básicos, os equipamentos de transmissão, os equipamentos de comutação e de acesso ao assinante e as instalações físicas e equipamentos de infra-estrutura.

Existe um grande esforço no sentido de padronização destes equipamentos para que a supervisão dos mesmos não seja limitada a um sistema ou plataforma de gerência específicos. A interoperabilidade deve ser garantida e implementada de acordo com a arquitetura TMN (*Telecommunications Management Network*), independente do modelo de gerenciamento adotado.

A monitoração e o controle de recursos são atividades inerentes à gerência de redes. Estas atividades de gerenciamento devem ser realizadas de forma padronizada, de acordo com o modelo de gerência adotado.

Toda concessionária de serviços de Telecomunicações tem como um dos objetivos a manutenção dos serviços dos seus usuários e de seus equipamentos, sob pena de perda de receita e insatisfação de clientes.

As linhas de assinantes constituem os pontos de acesso aos serviços de Telecomunicações. Estes pontos são interligados por meio de equipamentos de comutação, como as centrais telefônicas, e transmissão, e estes devem ser monitorados para detectar falhas eventuais, ou possibilidades de falhas futuras, com o objetivo de efetuar as correções no tempo mais rápido possível.

Além dos equipamentos de comutação e transmissão, as concessionárias de Telecomunicações possuem equipamentos como grupos geradores, condicionadores de ar, além de vários outros, que também podem e devem ser gerenciados. Detectando as falhas às quais estes equipamentos estão sujeitos, e corrigindo-as em tempo hábil, não

haverá transtorno nos serviços prestados e nem um comprometimento preocupante com a perda de receitas e com o desempenho do sistema de Telecomunicações.

A padronização de serviços se faz necessária na medida em que o uso dos recursos torna-se incompatível ou específico. Esta padronização servirá também como um meio de estimular fabricantes a utilizarem um padrão de desenvolvimento de seus equipamentos, tendo em vista a vasta gama de equipamentos que existem e que surgem no mercado.

O modelo de gerenciamento OSI (*Open Systems Interconnection*) é um modelo definido pela ISO (*International Organization for Standardization*). Bastante completo e robusto, foi projetado para solucionar problemas, especialmente aqueles do porte exigido pelos sistemas de telecomunicações. Possui funções bem definidas e é baseado no paradigma de orientação a objetos.

A filosofia de gerenciamento de redes apresentada pela comunidade Internet é baseada no modelo conhecido como SNMP (*Simple Network Management Protocol)*, cuja funcionalidade reside basicamente na leitura e alteração de valores de variáveis em equipamentos remotos gerenciáveis e em alguns relatórios de evento para situações específicas.

É comum utilizar o termo SNMP como referência a uma coleção de especificações para gerenciamento de redes que incluem o próprio protocolo, a definição de uma base de informações e conceitos associados.[Stalling 93]

O SNMP foi o primeiro protocolo usado. Foi rapidamente desenvolvido como solução para protocolos de gerenciamento Internet e possibilitou uma resposta para os problemas de comunicação entre diferentes tipos de redes.

A maior vantagem do SNMP é que ele é extremamente simples, o que o torna facilmente implementável para a maioria das redes. Outra vantagem do SNMP é que ele é amplamente utilizado atualmente. O resultado disso pode ser visto na maioria dos produtos, que são projetados para suportar SNMP. Pela sua simplicidade, a atualização deste protocolo torna-se bastante fácil.

Alguns fabricantes de equipamentos já incluem em seus produtos agentes SNMP, para que a gerência sobre seus produtos seja feita de forma padronizada. Mas muitos equipamentos ainda não possuem nenhum tipo de gerência ou não estão sendo gerenciados de forma padronizada, impossibilitando o uso das informações de modo interoperável pelas ferramentas especialmente desenvolvidas para este fim.

Com base nessas constatações e percebendo a necessidade crescente de estruturar, uniformizar e automatizar os procedimentos de gerência de falhas em sua rede de telecomunicações, a TELESC S/A iniciou em 1996 o projeto SIORE - Sistema de Operações Remotas. O objetivo traçado para esse projeto é especificar e desenvolver um sistema de gerenciamento de equipamentos de telecomunicações seguindo o modelo de gerência SNMP, isto é, desenvolver um agente SNMP que execute as tarefas relacionadas a cada equipamento e apresente as informações que estes produzem de modo padronizado, não de modo proprietário, garantindo, desta forma, a interoperabilidade entre os equipamentos da rede e a aplicação de gerenciamento.

A aplicação agente deve possuir capacidade de comunicar-se com a aplicação gerente, que monitorará e controlará os equipamentos da rede de Telecomunicações de Santa Catarina - TELESC S.A., além de coletar as informações que são produzidas pelos elementos de rede.

Com objetivo de ampliar a já extensa gama de equipamentos que o SIORE alcança, este documento trata da criação de um agente SNMP para centrais telefônicas que não tem condições de realizar os serviços do SIORE, analisando a viabilidade da criação de um canal de comunicação adequado, que permita assim, a monitoração ininterrupta destas centrais.

O projeto consiste em analisar centrais de pequeno porte e se possível implementar um sistema de telecomunicações entre estas centrais e o SIORE, disponibilizando através deste sistema, que qualquer PC (*personal computer*) com acesso a rede interna da Telesc, tenha a disposição aos serviços de telesupervisão que o projeto SIORE implementar.

Sobre o Conteúdo

Este trabalho está dividido em 6 capítulos. O capítulo 1 apresenta aspectos teóricos inerentes à rede e centrais telefônicas. O capítulo 2 explana sobre diversos aspectos teóricos que servirão como embasamento para o projeto, bem como as referências bibliográficas citadas. O capítulo 3 coloca o contexto da empresa Telesc e seus sistemas de modo a ilucidar onde se enquadra o projeto neles. O capítulo 4 diz respeito à especificação do projeto em si, os elementos envolvidos e uma descrição das ferramentas que podem ser usadas para concluir a aplicação de gerenciamento. No capítulos 5 e 6 é descrita a implementação da aplicação agente nas centrais telefônicas do tipo Trópico R e Zetax respectivamente.

Ao leitor sem muita intimidade com os sistemas de telecomunicações de uma empresa de telefonia, recomenda-se que seja lido todo o documento, desde o primeiro capítulo, onde encontram-se os conceitos básicos para uma melhor compreensão deste trabalho.

O leitor especializado no domínio da aplicação e interessado na análise e especificação do sistema pode ater-se a terminologia específica, e em seguida ler os capítulos 2 e seguintes da obra.

Para leitores mais técnicos e práticos, a última parte do documento, sendo essa os capítulos 5 e 6, contém aspectos relativos à implementação propriamente dita do agente SNMP.

Nos Anexos podem ser encontrados um artigo referente a ASN.1 (*Syntax Abstract Notation One*).

CAPÍTULO 1 - Redes e Centrais Telefônicas

O Objetivo deste capítulo é introduzir os conceitos básicos necessários à compreensão dos sistemas de telefonia, no que diz respeito aos aspectos abordados neste trabalho. Serão introduzidos conceitos referentes a redes de telefonia, centrais telefônicas (estrutura, tipos, tamanhos) e a telesupervisão.

1.1- Definições

1.1.1 - Rede Telefônica

A rede telefônica se destina basicamente a permitir a conversação telefônica entre dois usuários quaisquer desta rede e a qualquer tempo. O usuário deseja atingir qualquer um dos outros usuários ligados nesta rede (que pode ser de âmbito mundial) e que a conexão seja rápida e realizada com o número mínimo possível de tentativas [Ribeiro 80]. A F*igura 1.1.1* ilustra a conexão entre dois usuários, sendo as centrais "A" e "B" locais e "T" uma central trânsito.

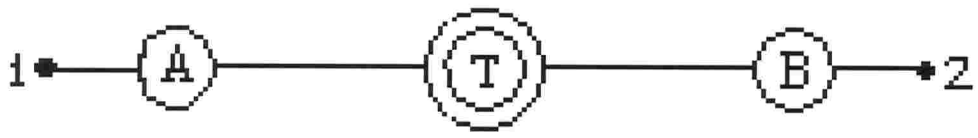

Figura 1.1.1 - Conexão entre dois usuários

Ela é composta por um conjunto de centrais de comutação ligadas entre si através de grupos de circuitos telefônicos. Intrinsecamente associado a qualquer rede telefônica, existe um conjunto de regras que estabelecem a forma pela qual as chamadas telefônicas originadas pelos assinantes devem ser escoadas através da mesma, e que constituem o Plano de Encaminhamento da rede [SIEMENS 75].

O Plano de Encaminhamento de uma rede telefônica determina a forma como devem ser encaminhadas as chamadas telefônicas, permitindo a determinação do volume de tráfego por rota. Desta forma, é possível dimensionar os grupos de circuitos que interligam as centrais de comutação, definindo o que se denomina de estrutura da rede.

1.1.2- Central Telefônica

Em uma rede telefônica não há interligação permanente entre os assinantes e sim entre eles e um centro de comutação ou central telefônica. À medida que cada assinante deseja uma conexão, transmite a solicitação à central e esta realiza uma conexão temporária entre os mesmos, que ficará mantida durante todo o tempo necessário para a comunicação desejada [Ribeiro80].

Entende-se por *comutação* a operação que permite realizar esta interligação temporária entre os dois usuários da rede[Ribeiro80].

A estrutura de hardware das centrais telefônicas pode se dividido em:

1) Módulo de Comutação: É a parte da central que executa a comutação de voz e dados dos terminais da central, e o controle das vias de sinalização entre processadores, bem como a geração e distribuição dos sinais de sincronismo.

2) Módulo de Operação e Manutenção: É a parte da central responsável pela realização das funções de operação, manutenção e supervisão, relacionando-se com o meio externo através de periféricos de entrada e saída que conectados ao módulo de operação e manutenção permite a comunicação entre o operador e o sistema. Estas funções de operação e manutenção são realizadas por placas microprocessadas chamadas placas TSP (*Telesupervisao*). As placas TSP são placas de alarmes, telecomandos e telemedidas. As placas de alarmes capturam sinais elétricos gerados por contato-seco, as de telecomandos geram comandos, acionam relês e as de telemedidas adquirem medidas elétricas analógicas e as

digitalizam. Todas essas placas se comunicam com um microcomputador via uma rede serial *token-bus*.

3) Módulo de Infra-estrutura: É a parte da central mais autônoma, que oferece aos outros módulos meios para tornar suas funções operacionalizáveis. Trata-se dos equipamentos que realizam a distribuição de energia e, caso o fornecimento externo falhe, a geração dela ocorre através sistemas de *no-breake* que contém geradores e baterias, os sistemas de transmissão de dados podendo ser por microondas, rádio ou outros. Além deste equipamentos há uma enorme gama de outros como sistemas de ar condicionado, sistemas de refrigeração mais específicos, antenas e cabos, multiplexadores, segurança, etc..

A F*igura 1.1.2.a* a seguir ilustra as diferentes partes que constituem uma central telefônica.

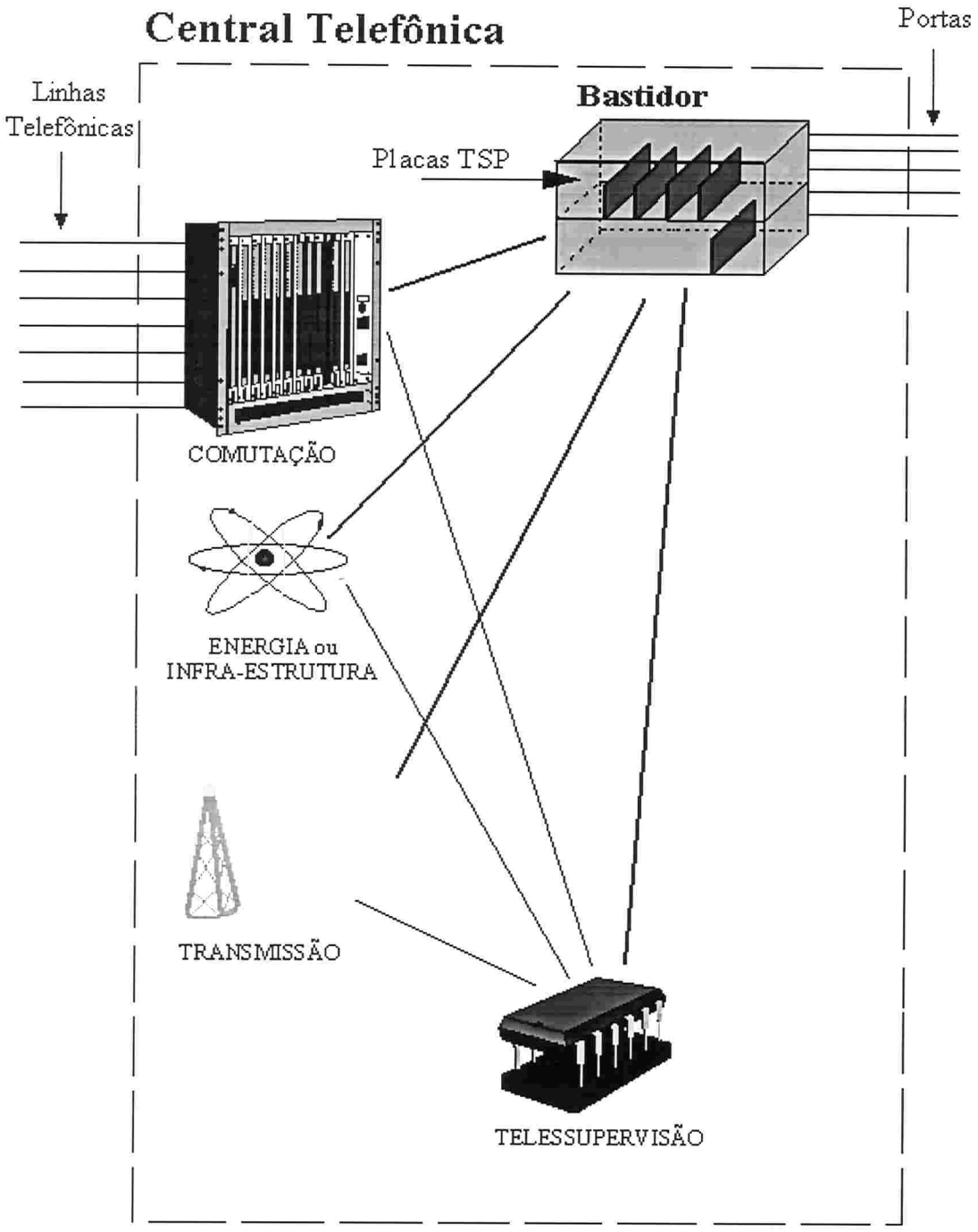

Figura 1.1.2 (a) - Ilustração de uma Central Telefônica

As centrais telefônicas podem ser de dois tipos:

1) Central local: Central de comutação à qual se ligam linhas de assinantes localizados dentro de sua área de ação. Tipicamente, em áreas urbanizadas, uma central local serve a assinantes dentro da área de um círculo de raio da ordem de 5 a 6 Km a partir da central.

2) Central trânsito: Em uma rede telefônica o ideal seria que as centrais locais estivessem todas ligadas entre si (F*igura 1.1.2.b*), mas devido ao grande número de centrais este esquema é inviável. Este problema é resolvido interligando-se as centrais locais a uma central específica, que provê as interligações desejadas entre as centrais locais (F*igura 1.1.2.c*). A central que interliga outras centrais é dita *central trânsito*, porque as chamadas apenas transitam por ela, não sendo terminadas em assinantes [Ribeiro80].

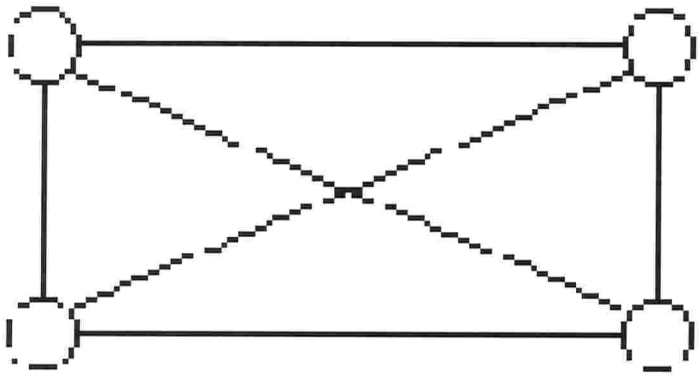

Figura 1.1.2 (b) - Ligações possíveis entre centrais locais

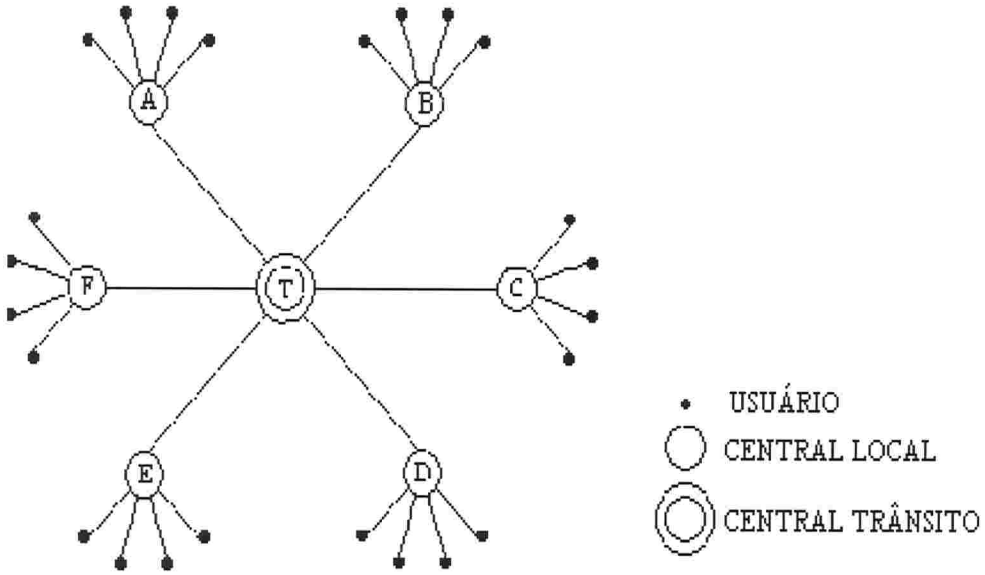

Figura 1.1.2 (c) - Uso da central trânsito

1.1.3- Centrais de Grande Porte

Existem na rede telefônica algumas centrais que são consideradas de grande porte, aproximadamente centrais que possuam mais de 4000 terminais. Estas centrais são poucas em relação ao número total de centrais existentes, e recebem um tratamento diferenciado.

Entre duas centrais locais quaisquer, pertencentes a áreas fechadas diferentes, o tráfego geralmente não justifica a abertura de rota direta. Mas, poderá vir a ocorrer que entre duas centrais locais de grande porte se justifique abrir uma rota direta.

As centrais de grande porte possuem diversas portas permitindo a sua comunicação por diversos meios e já possuem para si diversos sistemas desenvolvidos pelos fabricantes e pelas empresas usuárias para operacionalizá-las e automatizá-las.

1.1.4 - Centrais de Pequeno Porte

As CTPP existem em grande número, mas com apenas poucas centenas de terminais. Sendo muitas vezes comparáveis com grandes PABX, as CTPP são caixas fechadas com pouco material de apoio desenvolvido para elas e poucas vias de acesso, muitas vezes apenas uma, a velha e lenta linha discada.

Este trabalho tem por objetivo desenvolver software de apoio ao gerenciamento de algumas centrais de pequeno porte. As CCTP que serão alvo deste trabalho são as do tipo Zetax, Trópico R e SPX2000. As três são de fabricantes diferentes tendo características bem diferentes entre elas, o que nos levou a estudá-las em separado no decorrer dos capítulos deste trabalho.

1.1.5 - A Telesupervisão

O papel da Telessupervisão é extrair informações dos diversos elementos de uma rede de telecomunicações (NE - *network element*) por meio de equipamentos de supervisão remota, denominados TSP-20.

Estas informações que são extraídas de forma remota, são utilizadas durante o processo de tomada de decisões de que ações devem ser realizadas diante de determinado problema ou alarme. No caso dos alarmes o sistema decodifica-os e determina sua prioridade, sendo então o sistema responsável por definir se é necessário ou não abrir um boletim de anormalidade (BA) acionando-se assim, imediatamente, o técnico responsável de plantão para a central que possui o defeito.

Ainda hoje, mesmo que equipamentos modernos possuam mecanismos próprios para fornecimento de dados (de forma padronizada ou não) implementados pelo fabricante, existem certas informações necessárias à supervisão de sistemas que são coletadas de forma redundante, como é o caso das centrais e equipamentos SDH (*Synchronous Digital Hierarchy*). Esta coleta é feita usualmente através de placas de

aquisição de dados. Estas placas são desenvolvidas para que se possa fazer uma supervisão, ainda que "burra" (tipo contato-seco), dos equipamentos de telecomunicações.

Os seguintes NEs são assistidos:

- Equipamentos de transmissão como rádio UHF, rádio SHF, rádio digital, multiplexadores, elo (interface do cabo ótico com outro meio de transmissão), transmissor e receptor de TV, etc.

- Componentes de centrais de comutação analógica (registrador, marcador, avaliador) e de centrais digitais (alarmes concentrados).

- Equipamentos de energia (AC, DC, bateria, grupo gerador e ar-condicionado).

CAPÍTULO 2 - Gerência de redes de telecomunicações

Neste capítulo são descritos conceitos necessários ao entendimento dos sistemas de gerência de rede de telecomunicações, no que diz respeito aos aspectos abordados neste trabalho. Serão introduzidos conceitos referentes ao modelo TMN, do protocolo SNMP, da base de dados do sistema - MIB.

2.1 - Modelo TMN (*Telecommunications Management Network)*

O modelo TMN visa prover uma estrutura organizada para interconectar vários tipos de Sistemas de Suporte à Operação e equipamentos de Telecomunicações para a troca de informação de gerenciamento utilizando interfaces padronizadas que incluem a definição de protocolos e mensagens [Brisa 93].

Ainda, segundo [Brisa 93], neste contexto, a TMN pode gerenciar:

a) redes públicas e privadas, incluindo redes de telefonia móvel, redes virtuais, redes inteligentes, redes de longa distância, redes metropolitanas e redes locais;

b) a própria TMN;

c) terminais de transmissão tais como multiplexadores, roteadores e equipamentos de transmissão síncrona (SDH - *Synchronous Digital Hierarchy*);

d) sistemas de transmissão digital e analógica baseados em cabo coaxial, par trançado, fibra óptica, rádio e satélite;

e) *mainframes*, processadores *front-end*, controladores de *cluster* e servidores de arquivo;

f) serviços de suporte e telesserviços;

g) PABX, acessos de PABX e terminais de usuário;

h) softwares providos por ou associados a serviços de telecomunicações; por exemplo, software de comutação, de diretórios e de base de dados de mensagem;

i) sistemas de suporte e infra-estrutura, tais como módulos de testes, sistemas de energia, unidades de ar condicionado e sistemas de alarme de edifício;

j) entidades distribuídas e serviços oferecidos pelos agrupamentos dos itens anteriores.

Neste escopo, o projeto inclui-se nos itens c), f) e i), onde teremos serviços de suporte aos elementos de rede, detectando, por exemplo, falhas nas centrais digitais, ar condicionado, sistema de alarme, etc.

2.1.1 - Funcionalidades Associadas à TMN

Dentro da TMN podemos identificar cinco áreas funcionais de gerenciamento:

a) *Gerenciamento de Configuração*

Habilita ao usuário criar e modificar o modelo de gerenciamento de recursos físicos e lógicos da rede de telecomunicações. As principais funções deste gerenciamento são:

- Gerenciamento de Ordem de Serviço: possibilita a identificação e o controle do provisionamento de novos recursos necessários para a rede de telecomunicações. A Ordem de Serviço pode ser utilizada para solicitar novos recursos, físicos ou lógicos;

- Configuração de Recursos: são funções que têm como finalidade possibilitar que os recursos da rede possam ser criados, roteados, controlados e modificados;

- Informação de Recursos: são funções que têm como finalidade apresentar a lista de recursos aloucados, verificar a consistência da informação e obter informações sobre os recursos disponíveis.

b) *Gerenciamento de Falhas*

É um conjunto de funções que possibilita a detecção, a isolação e a correção de uma operação anormal da rede de telecomunicações. A monitoração de desempenho e o gerenciamento de falhas são conceitualmente similares, podendo ser distinguidos pelo fato de que o gerenciamento de falhas está relacionado a falhas que afetam o serviço prestado, mesmo que elas tenham sido causadas como conseqüência de uma degradação do desempenho. As principais funções de gerenciamento de falhas são:

- Supervisão de Alarmes: está relacionado ao gerenciamento da informação sobre as degradações de desempenho que afetam o serviço;

- Teste: o usuário pode solicitar que um teste específico seja executado, podendo também estabelecer os parâmetros do teste solicitado. Em alguns casos, o tipo e os parâmetros de teste podem ser automaticamente designados;

- Relatório de Problemas: o relatório de problemas é utilizado para rastrear e controlar as ações tomadas para liberar alarmes e outros problemas.

c) Gerenciamento de Desempenho

Deve prover funções para avaliar e relatar o comportamento dos equipamentos de telecomunicações e a eficiência da rede. Estas funções estão divididas em dois grupos:

- Medidas de Tráfego: estas funções capacitam ao usuário definir e controlar a entrega de relatórios de medidas de tráfego;

- Monitoração de Desempenho: são informações que permitem ao usuário obter, avaliar e relatar parâmetros de desempenho da rede. Tais informações podem ser utilizadas pelo usuário como apoio ao diagnóstico de falhas, ao planejamento da rede e à qualidade do serviço.

d) Gerenciamento de Segurança

As principais Funções de Segurança são: segurança de acesso, alarmes de segurança, rastreamento para auditoria no caso de violação e serviço de recuperação após violação. As informações que são trocadas dentro da TMN podem ser utilizadas por mais de uma área funcional de gerenciamento. Dentro deste contexto, definem-se funcionalidades da TMN como sendo a capacidade de:

- trocar informações de gerenciamento através do limite entre o ambiente de telecomunicações e o ambiente TMN;

- converter informações de gerenciamento de um formato para outro; desta maneira, as informações de gerenciamento que circulam dentro do ambiente TMN tem uma consistência natural;

- transferir informações de gerenciamento entre diferentes localizações no ambiente TMN;

- analisar e reagir apropriadamente às informações de gerenciamento;

- manipular informações de gerenciamento para uma forma útil e/ou significativa para o usuário de informações de gerenciamento;

- entregar informações de gerenciamento ao usuário de informações de gerenciamento e apresentá-las de uma maneira apropriada;

- garantir o acesso seguro de informações de gerenciamento aos usuários de informações de gerenciamento autorizados.

e) Gerenciamento de Contabilização

O Gerenciamento de Contabilização provê um conjunto de funções que possibilite determinar o custo associado ao uso da rede de telecomunicações, mediante medição da utilização dos serviços.

2.2 - SNMP (*Simple Network Management Protocol*)

O protocolo SNMP (*Simple Network Management Protocol*) foi desenvolvido para proporcionar uma ferramenta de gerenciamento para redes TCP/IP, básica e fácil de implementar.

O protocolo de gerenciamento é visto sob o paradigma de observação remota, isto é, ele não transporta simplesmente operações de gerenciamento que devem ser executadas pelos objetos gerenciados, mas também os identificadores destes objetos e seus valores.

O modelo atual para gerenciamento de redes baseadas em TCP/IP, está descrito nos seguintes documentos:

- RFC 1155 (SMIv1) / RFC 1902 *Draft* (SMIv2) - Estrutura de identificação da Informação de Gerenciamento, que descreve como os objetos gerenciados contidos na MIB são definidos;

- RFC 1213 (MIB-II) - Base de Informação de Gerenciamento, que descreve os objetos gerenciados definidos na MIB;

- RFC 1157 (SNMPv1) / RFC 1906 *Draft* (SNMPv2) - Protocolo de Gerenciamento de Redes Simples, que define o protocolo usado para gerenciar estes objetos.

O protocolo de gerenciamento SNMP consiste de dois "atores": um agente e um gerente. O agente mantém informações locais de gerenciamento em uma base de dados própria denominada MIB (*Management Information Base*) e responde às requisições de informação vindas do gerente. A comunicação entre um agente e um gerente é normalmente feita pela troca de primitivas *request* e *response*. O gerente requisita informações do agente usando uma primitiva *get-request* para o qual o agente responderá com uma primitiva *get-response*. O gerente pode também enviar uma primitiva *set-request* instruindo o agente para atualizar algumas informações da sua base de dados com o valor enviando por ele, e o agente também responde com uma primitiva *get-response* para o gerente.

Além das trocas de primitivas descritas acima um agente pode ainda enviar informações não solicitadas por meio de *traps*. Os *traps* são objetos escalares não solicitados que o agente envia para uma estação de gerenciamento de rede [Perkins 97], ou seja, quando o agente identifica um alarme, ele tem a capacidade de enviar uma mensagem alertando o sistema mesmo sem esta ser solicitada pelo gerente. Porém, *traps* têm um inconveniente: não possuem confirmação. Sendo assim, se alguma conexão falhar no meio do caminho, *traps* que foram enviadas ao gerente serão perdidas e ele não receberá a mensagem de aviso.

Todas as funções de agentes de gerenciamento são modeladas como inspeção ou alteração de variáveis na MIB. Portanto, a entidade de protocolo, em um *host* lógico remoto (possivelmente o próprio elemento de rede), interage com o agente de gerenciamento residente no elemento de rede, com o objetivo de recuperar (*get*) ou alterar (*set*) valores de variáveis solicitadas pelo gerente.

A estratégia implícita no SNMP é que a monitoração do estado da rede é feita preferencialmente por *polling*. Um número limitado de mensagens não solicitadas (*traps*)

guia a temporização e a direção do *polling*.

A comunicação entre entidades de gerenciamento é realizada através da troca de mensagens do protocolo. Esta troca de mensagens requer apenas um serviço de datagrama e, toda mensagem é completa e independentemente representada por um único datagrama de transporte, denominado de PDU (*Protocol Data Unit*).

A estrutura do protocolo SNMP admite um gerenciamento distribuído, com estações configuradas para exercer o papel de gerentes e agentes, e com possibilidade de comunicação entre gerentes para a troca de informações de gerenciamento.

Cada gerente pode gerenciar diretamente um conjunto de agentes e, quando o número de agentes cresce ao ponto de causar problemas relativos ao desempenho da rede de comunicação, a estação gerente pode delegar a tarefa de gerenciamento a gerentes intermediários. O gerente intermediário exerce o papel de gerente para monitorar e controlar os agentes sob sua responsabilidade e exerce o papel de agente para enviar e receber informações de controle de seu gerente hierarquicamente superior. A confirmação feita por este gerente intermediário será uma primitiva *inform-request*.

A união de um agente SNMP com algum conjunto arbitrário de entidades de aplicação SNMP, é chamada de *comunidade SNMP*. Cada comunidade SNMP é nomeada por um *string* de octetos que define um *nome de comunidade* para aquela comunidade.

Uma mensagem originada por uma entidade de aplicação SNMP que pertence à comunidade nomeada pelo componente de comunidade desta mensagem, é chamada *mensagem SNMP autêntica*. O conjunto de regras pelas quais uma mensagem é identificada como autêntica, é denominado *esquema de autenticação*. Uma implementação de função que identifica mensagens SNMP autênticas, de acordo com um ou mais esquemas de autenticação, é chamada *serviço de autenticação*.

Um subconjunto de objetos da MIB, que pertencem a um determinado elemento de rede, é chamado *visão da MIB SNMP*. Os nomes dos tipos de objetos representados em uma visão da MIB SNMP não precisam pertencer a uma única sub-árvore do espaço de nomes de tipos de objetos.

Um elemento do conjunto { *READ-ONLY*, *READ-WRITE* }, é chamado *modo de acesso SNMP*. [Stallings 93]

A união de um modo de acesso SNMP com uma visão da MIB SNMP é chamada *perfil da comunidade SNMP*. O perfil da comunidade SNMP representa privilégios de acesso específicos à variáveis em uma visão da MIB especificada. Os acessos às variáveis são representados pelo perfil, de acordo com as seguintes convenções:

- se a variável é definida com "*Access: none*", então ela não está disponível, como operando, para nenhum operador;

- se a variável é definida com "*Access: read-write*", ou "*Access: write-only*", e o modo de acesso do perfil é *READ-WRITE*, a variável está disponível como operando para as operações de *get*, *set* e *trap*;

- nos outros casos, a variável está disponível apenas como um operando para as operações *get* e *trap*;

- nos casos em que a variável "*write-only*" é um operando usado para as operações *get* e *trap*, o valor fornecido para a variável é específico da implementação.

A união de uma comunidade SNMP com um perfil de comunidade SNMP, é chamada *política de acesso SNMP*. Uma política de acesso representa um perfil específico de comunidade, estabelecido por um agente SNMP para os outros membros da comunidade. Todos os relacionamentos entre entidades de aplicação SNMP, são arquiteturalmente definidos em termos de políticas de acesso.

Se o elemento de rede, no qual o agente SNMP reside, não fornece a mesma visão

da MIB, definida no perfil especificado para aquela comunidade, então a política é chamada *política de acesso proxy*. O agente SNMP associado com uma política de acesso proxy é chamado *agente proxy*.

A política de acesso proxy permite a monitoração e o controle de elementos de rede que normalmente não podem ser acessados pelos protocolos de gerenciamento e de transporte. Na verdade, um agente proxy provê uma função de conversão de protocolo, permitindo que uma estação de gerenciamento execute um gerenciamento consistente sobre todos os elementos de rede, incluindo equipamentos tais como modems, multiplexadores e outros equipamentos que suportam diferentes estruturas de gerenciamento. [Stallings 93]

2.2.1 - A MIB (Management Information Base)

Existem várias interpretações para o termo MIB. Uma MIB SNMP pode ser descrita como uma coleção de definições de módulos que podem estar contidos em um ou mais arquivos. Ela também pode ser vista como a união de todas as informações de gerenciamento como "a MIB". Entretanto, a maioria das pessoas usam o termo MIB para referenciar um ou mais módulos que contém definições de informação de gerenciamento declaradas [Perkins 97].

Uma MIB pode ser vista, ainda, como uma área de armazenamento de informações, porém, deve-se tomar cuidado com este tipo de referência, pois nem todos os equipamentos gerenciados possuem certos dispositivos de armazenamento de dados.

O termo MIB pode também ser confundido com o termo MIT (*Management Information Tree)*. Na verdade, as definições de módulos contidos em um ou mais documentos, normalmente chamados de RFC (*Requests for Coments*), são feitas em ASN.1 (*Abstract Syntax Notation One*, ver anexo 1), uma notação usada para descrever as estruturas de dados, que serão enviadas por um protocolo de gerenciamento, e a informação contida nestas estruturas. A informação declarada nos identificadores e tipos

de objetos nestes documentos especifica uma estrutura em árvore. Esta estrutura (MIT) define o acesso aos objetos de uma MIB.

A MIB do agente especificada para os equipamentos (objetos) constantes no sistema pode ser visualizada na *Figura 2.2.1*.

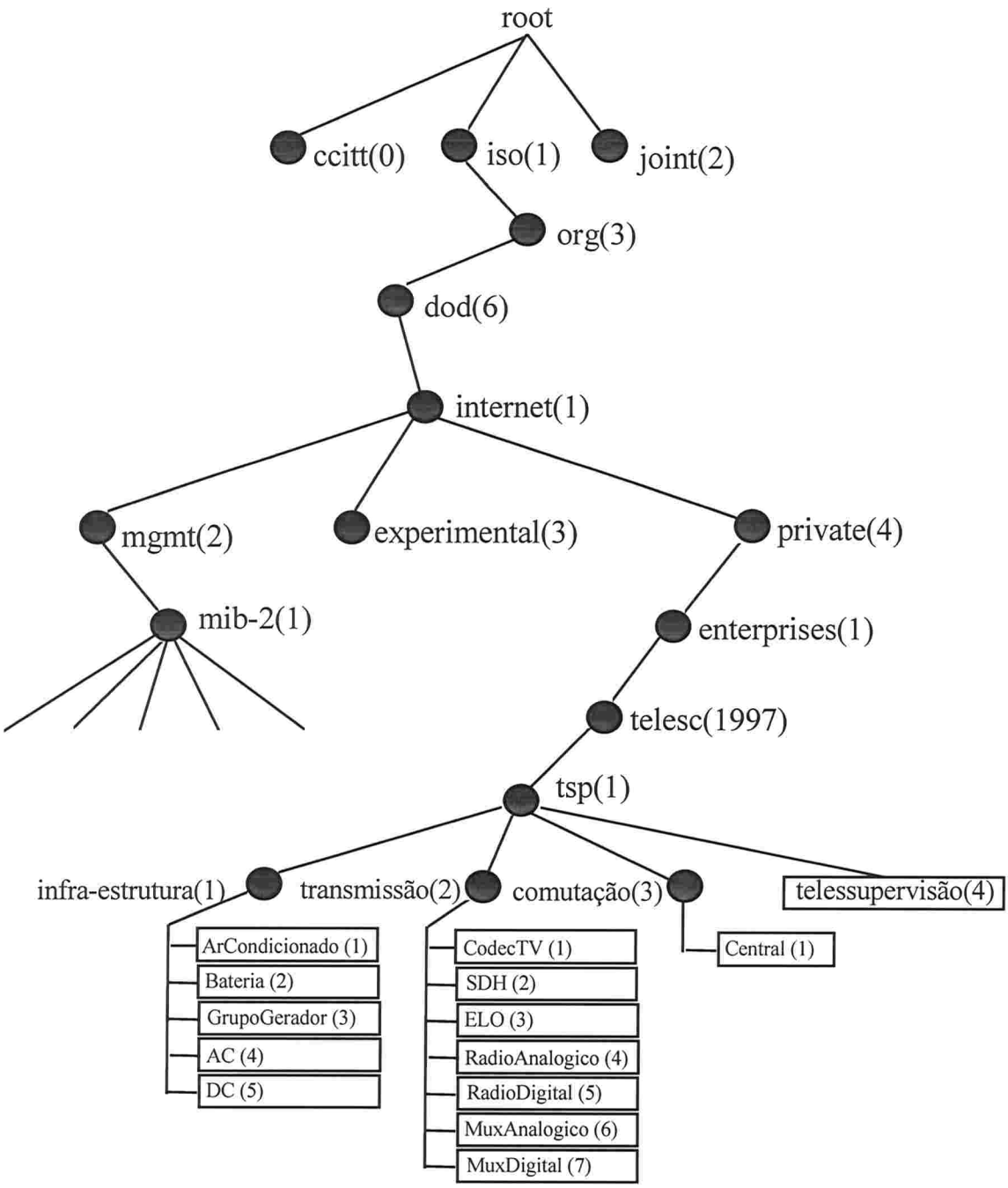

Figura 2.2.1 - MIB SNMP desenvolvida e padronizada para a TELESC, com detalhe dos objetos gerenciados.

CAPÍTULO 3 - O contexto da Telesc

Neste capítulo são descritos os sistemas que compõem a rede de Telecomunicações da Telesc, de forma a descrever o contexto em que foi desenvolvido este projeto.

3.1 - A rede de Telecomunicações da Telesc

A busca constante do incremento no número de terminais por habitante no estado de Santa Catarina fez com que o parque instalado aumentasse de 166.026, em 1985, para 348.417 terminais em 1993, e 714.637 terminais (convencionais e celulares) em 1997.

Em um período tão grande, ocorreram mudanças radicais na tecnologia e nas conquistas geográficas. Como a evolução da planta se faz de forma paulatina ao longo do tempo, é natural que esta tenha diversos equipamentos de gerações tecnológicas diferentes, como por exemplo:

- Transmissão: analógica (linha física, rádio analógico em UHF, VHF, SHF) e digital (fibra ótica, rádio digital);

- Comutação: centrais fixas analógicas, centrais fixas digitais e centrais celulares;

- Infra-estrutura: variedade de sistemas de climatização e energia.

Além das diferenças tecnológicas, existem as de padronização, pois os equipamentos são fornecidos por um grande número de fabricantes devido a dois motivos principais: diversidade de tecnologia e legislação vigente sobre a aquisição de equipamentos por empresas estatais.

A supervisão ou gerenciamento de falhas é vista na sua maioria isoladamente, dificultando uma visão global do que acontece na planta. Surge aqui a necessidade de um

sistema para integrar todos os eventos (falhas, exceções) que ocorrem na planta e que são fornecidos pelos diversos sistemas de operação e supervisão.

Porém, nas redes tradicionais, o conceito de gerência de rede, via de regra, se confunde com o conceito de supervisão, que é uma forma de gerência muito limitada e, portanto, insuficiente para tornar possível o oferecimento de serviços modernos, com qualidade e produtividade.

Estes sistemas de supervisão, que atualmente encontram-se em funcionamento na TELESC, serão substituídos gradativamente por sistemas padronizados de gerência de redes.

O sistema desenvolvido neste trabalho, deverá substituir funcionalmente os chamados sistemas de Supervisão F-80 e Supervisão FB-200, em uso atualmente.

3.1.1 - A Organização da Telesc

Há algum tempo que esforços estão sendo dispendidos para que os chamados CGIRs (Centros de Gerência Integrada de Rede), atuando em cada concessionária de serviços de telecomunicações, possam ser capazes de controlar toda a rede de telecomunicações sob sua jurisdição a partir de um único ponto, caracterizando uma postura centralizada nos serviços de gerência.

Atualmente a TELESC S.A. possui seis centros regionais, denominados superintendências, que situam-se dentro da área geográfica do estado de Santa Catarina.

A TELESC S.A. possui seis superintendências:

- Superintendência Leste (Florianópolis);
- Superintendência do Vale (Blumenau);
- Superintendência Sul (Criciúma);

- Superintendência Planalto (Lages);

- Superintendência Oeste (Chapecó);

- Superintendência Norte (Joinville).

O CGIR, atualmente localizado no bairro do Itacorubi, em Florianópolis, é o centro responsável pela gerência da rede de telecomunicações de Santa Catarina. Existem vários projetos de gerência sendo desenvolvidos atualmente. Entre eles, temos o SIORE - Sistema de Operações Remotas, que é o responsável pelo controle de equipamentos de telecomunicações, e no qual está envolvido diretamente este projeto, no que diz respeito com o gerenciamento de falhas de centrais de pequeno porte.

Já existem atualmente equipamentos com dispositivos que possibilitam o seu gerenciamento. Como exemplo, temos o ar condicionado, onde os mais modernos possuem agentes SNMP. Porém, existem equipamentos bem mais robustos e capazes de gerar informações mais complexas, nos quais o protocolo SNMP não é suportado. Para estes equipamentos, tais como centrais telefônicas, é necessário utilizar um modelo mais elaborado, baseado no modelo OSI, como o CMIP (*Common Management Information Protocol*).

Como os equipamentos a serem gerenciados não possuem interface própria para geração de certas informações, foram desenvolvidas placas proprietárias de coleta destas informações. Estas informações produzidas pelos equipamentos e traduzidas por estas placas são do tipo contato-seco, ou seja, sabe-se a priori se o estado da informação coletada é *ligado* ou *desligado*.

Em cada superintendência estima-se que deverão existir aproximadamente mil placas de coleta de informações. Com a utilização do protocolo SNMP, soluciona-se os principais problemas causados no processo de varredura, que depende, não só do protocolo, como do meio físico de transmissão ao qual o sistema tem acesso. O modelo

que foi tomado como referência de arquitetura foi o OSI, mas na verdade, o modelo OSI é raramente implementado por inteiro, o que freqüentemente ocorre, por motivos de simplicidade e viabilidade de custos, é optar-se por uma alternativa mais barata e com menos complexidade na implementação. Dessa forma optou-se pelo SNMP.

A *Figura 3.1.1.a* representa o *backbone* da rede SIORE na TELESC. Os micros representam as superintendências, que estarão ligadas por meio de roteadores. Futuramente, estas LANs (*Local Area Network*) estarão ligadas aos anéis óticos do SDH (*Synchronous Digital Hierarchy*), que funcionarão a uma velocidade de 155 Mbits/s.

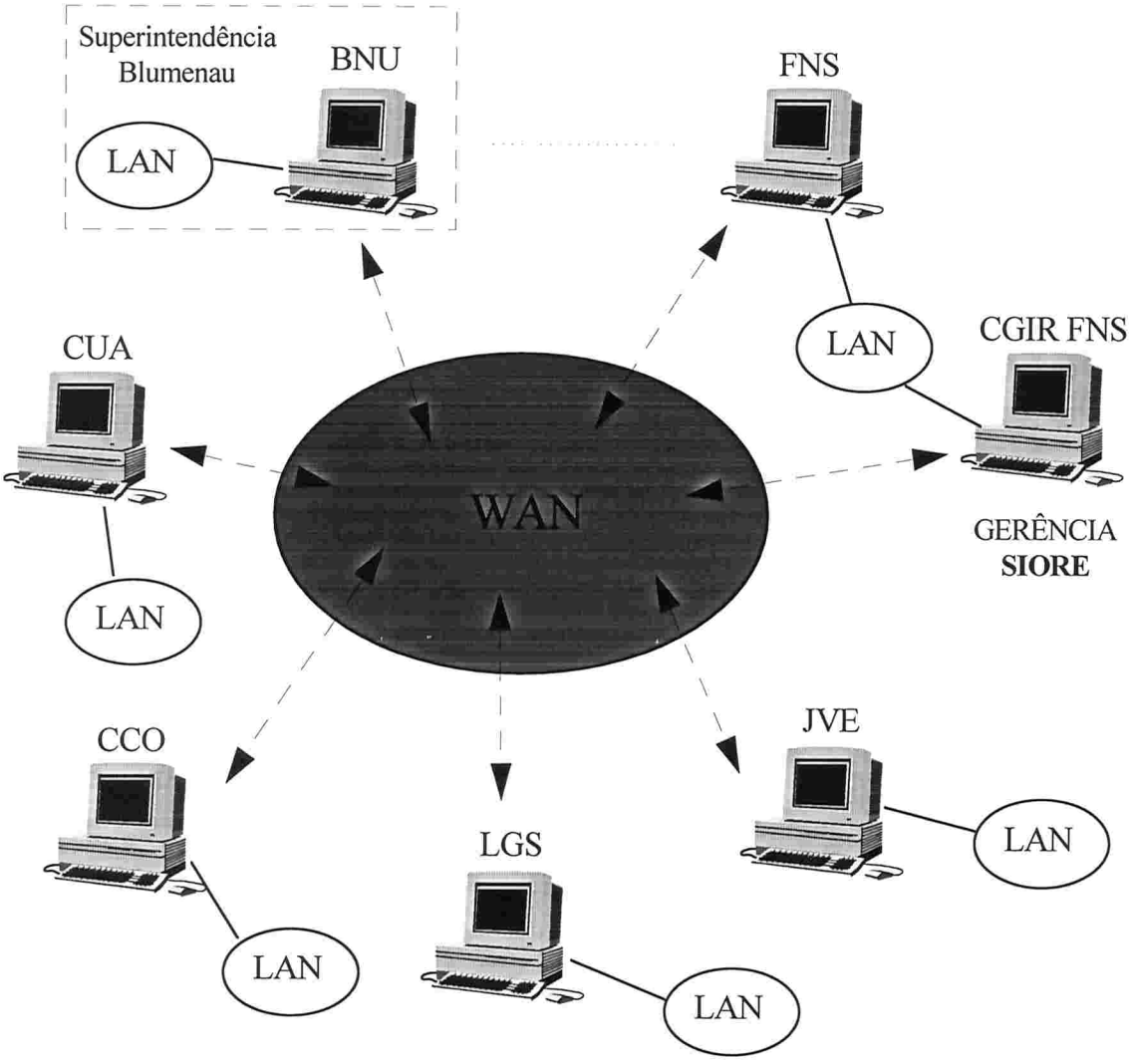

Figura 3.1.1 (a) - Backbone da rede gerenciada.

Para ficar mais claro e entender onde estão os agentes, a F*igura 3.1.1.b* detalha uma das superintendências (no caso, a superintendência do Vale - Blumenau). Cada superintendência pode ter várias estações de gerenciamento, onde agentes SNMP deverão monitorar e controlar os elementos de rede (*NE - Network Element*).

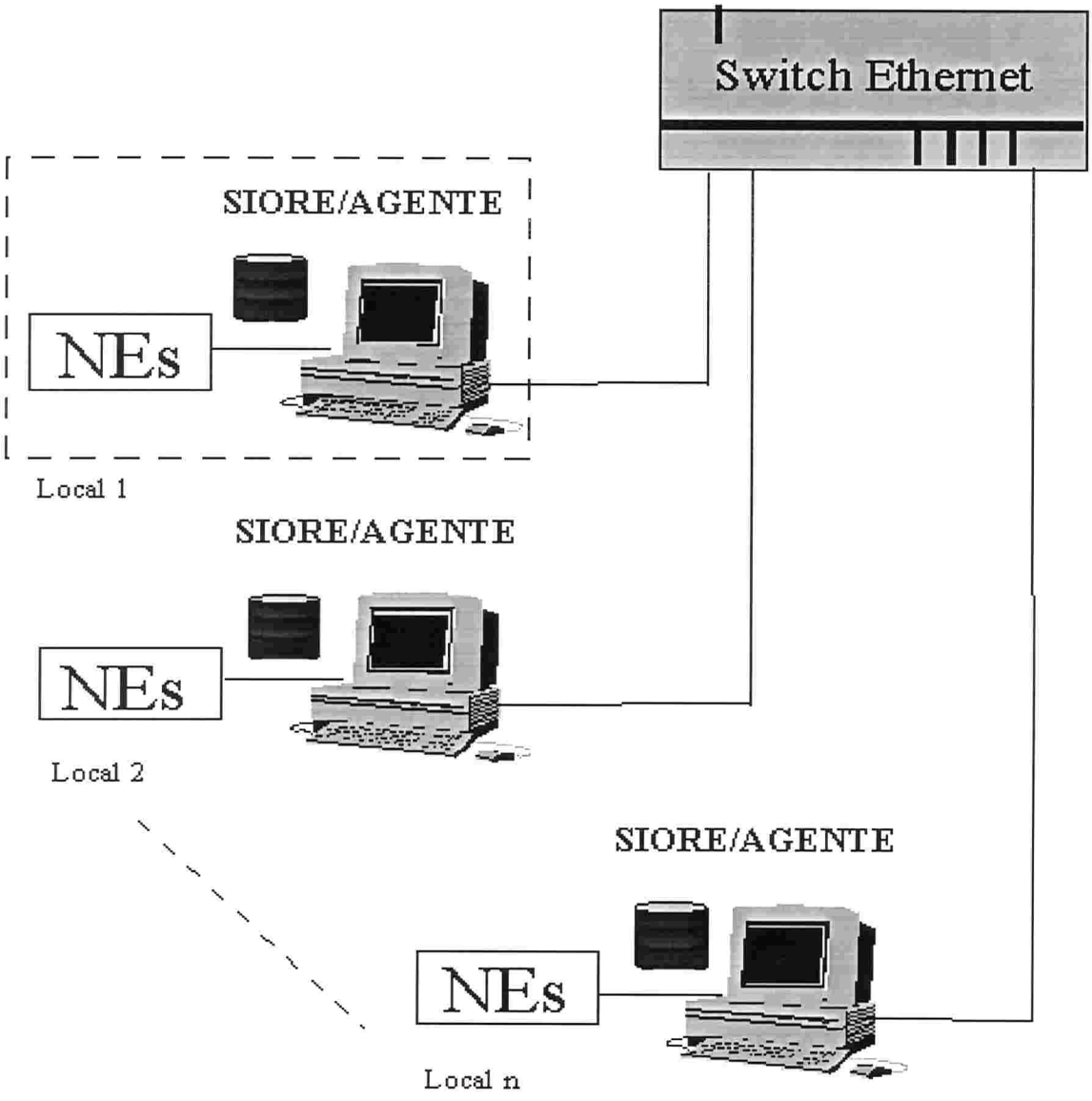

Figura 3.1.1 (b) - Backbone das Superintendências (BNU).

Cabe lembrar que a Superintendência do Vale (Blumenau) possui localidades agregadas a ela, não só no próprio perímetro urbano de Blumenau, mas também em outras cidades, a exemplo Itajaí e Balneário Camboriú. Estas cidades também estão incluídas no dimensionamento do projeto e também terão agentes SNMP para seus elementos de rede. Entretanto, a configuração das estações, quanto aos equipamentos que serão gerenciados, irá variar bastante, inclusive nas formas de comunicação entre NEs e NMS (*Network Management Station*), pois nem em todo local poderá haver uma estação de gerenciamento, devido às características deste local. Para estas situações, outros tipos de comunicação serão feitas, via *modem*, em uma linha dedicada.

A configuração da localidade pode ser visualizada na *Figura 3.1.1.c*, onde encontra-se o agente SNMP, lendo informações das placas contidas em um bastidor, e estas, por sua vez, ligadas aos elementos de redes, que estão representados por seus grupos de agregação.

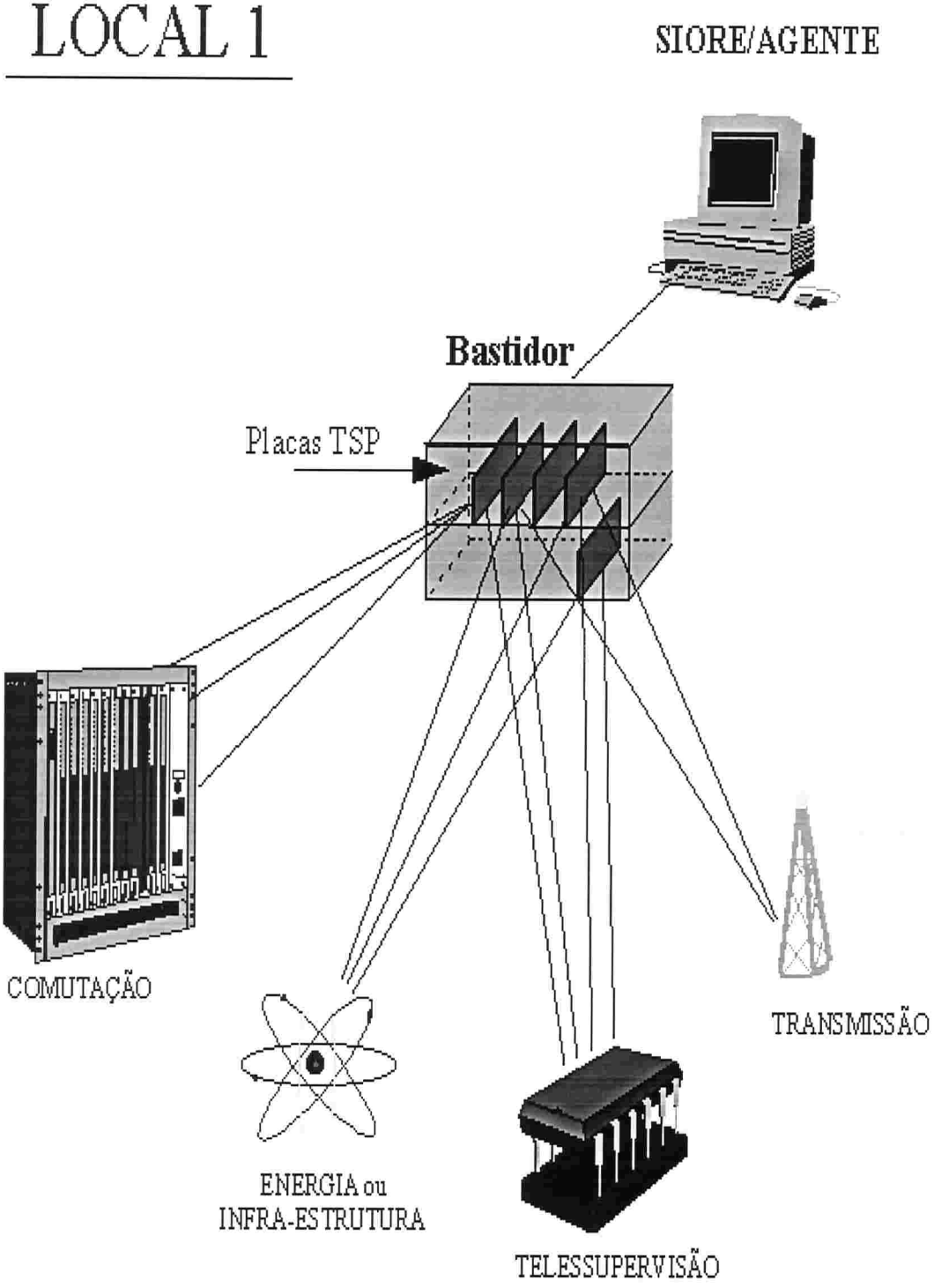

Figura 3.1.1 (c) - Detalhe da Estação de Gerenciamento (NMS).

3.1.2 - Gerência de Rede na TELESC

A TELESC planejou a gerência de suas redes de telecomunicação em quatro etapas:

1ª etapa:

- Criação do CGIR (Centro de Gerência Integrada de Rede), com o objetivo de centralizar os sistemas de monitoração;
- Definição de objetos gerenciados a nível de gerência de falhas;
- Automação de processos de supervisão de falhas.

2ª etapa:

- Telessupervisão de centrais analógicas.

3ª etapa:

- Implantação da rede de comutação de pacotes;
- Migração do suporte do CGIR do *mainframe* IBM para a rede de pacotes.
- Integração dos sistemas de operação (nos quais inclui-se o SIORE) e bases de dados para a arquitetura TMN (*Telecommunications Management Network*), que vem sendo definida a nível mundial, baseada no modelo OSI e que tem como objetivo o gerenciamento de redes especificamente para sistemas de telecomunicações.

3.1.3 - CGIR - Centro de Gerência Integrada de Rede

O CGIR é composto por equipamentos de monitoração e controle, e alguns centralizados. Um centralizado é um equipamento dedicado que, constantemente, supervisiona um ou mais elementos de rede. Os centralizados estão agrupados fisicamente (em um mesmo local), sem qualquer interoperação (integração) entre eles.

As informações são recebidas pelos centralizados de diversas maneiras: no monitor de vídeo, em painéis, em relatórios, em arquivos, etc. Especialistas estudam e interpretam estas informações para tomar atitudes cabíveis na solução das falhas.

Na situação atual, o principal problema encontrado é a falta de integração entre os centralizados e a falta de análise das informações em tempo real, ocorrendo casos em que um especialista atende a mais de um sistema.

Os sistemas de operação ou supervisão do CGIR sofrem certas deficiências, tais como:

- Má utilização de recursos (pessoas e equipamentos);

- Alarmes não padronizados (cada fabricante utiliza protocolo proprietário e formatos diferentes);

- Os analistas, devido à não padronização das formas de operação e acesso às centrais, têm visão parcial da situação da planta digital, isto é, visão restrita aos modelos de centrais aos seus cuidados;

- Dificuldade para detecção de alarmes (em alguns casos, somente são conhecidos após seu desaparecimento);

- Falta de supervisão sobre o desempenho do sistema;

- Predomina a abertura manual dos boletins de anormalidades (BAs).

3.1.4 - Sistemas de Supervisão da Telesc

A busca constante do incremento no número de terminais por habitante no estado de Santa Catarina fez com que o parque instalado aumentasse de 166.026, em 1985, para 348.417 terminais em 1993, e 714.637 terminais (convencionais e celulares) em 1997.

Em um período tão grande, ocorreram mudanças radicais na tecnologia e nas conquistas geográficas. Como a evolução da planta se faz de forma paulatina ao longo do tempo, é natural que esta tenha diversos equipamentos de gerações tecnológicas diferentes, como por exemplo:

- Transmissão: analógica (linha física, rádio analógico em UHF, VHF, SHF) e digital (fibra ótica, rádio digital);

- Comutação: centrais fixas analógicas, centrais fixas digitais e centrais celulares;

- Infra-estrutura: variedade de sistemas de climatização e energia.

Além das diferenças tecnológicas, existem as de padronização, pois os equipamentos são fornecidos por um grande número de fabricantes devido a dois motivos principais: diversidade de tecnologia e legislação vigente sobre a aquisição de equipamentos por empresas estatais.

A supervisão ou gerenciamento de falhas é vista na sua maioria isoladamente, dificultando uma visão global do que acontece na planta. Surge aqui a necessidade de um sistema para integrar todos os eventos (falhas, exceções) que ocorrem na planta e que são fornecidos pelos diversos sistemas de operação e supervisão.

Porém, nas redes tradicionais, o conceito de gerência de rede, via de regra, se confunde com o conceito de supervisão, que é uma forma de gerência muito limitada e,

portanto, insuficiente para tornar possível o oferecimento de serviços modernos, com qualidade e produtividade.

Estes sistemas de supervisão, que atualmente encontram-se em funcionamento na TELESC, serão substituídos gradativamente por sistemas padronizados de gerência de redes.

O sistema desenvolvido neste trabalho, deverá substituir funcionalmente os chamados sistemas de Supervisão F-80 e Supervisão FB-200, em uso atualmente.

3.2 - O SIORE

O SIORE - Sistema Integrado de Operações Remotas - é uma interface que vai possibilitar aos Sistemas de Operação (OS) interagir com os equipamentos de Telecomunicações (NEs) através de chamadas padrão.

Esta interface prevê a coleta de informações e execução de ações sobre os equipamentos através de solicitações remotas ou não.

Este projeto está baseado no desenvolvimento de um agente que situa-se entre os OSs e os equipamentos de telecomunicações

Entre as cinco funções de gerenciamento (falhas, desempenho, configuração, segurança e contabilização), são identificadas diretamente neste projeto três funções essenciais que deverão estar implementadas: gerência de falhas, configuração e segurança.

A primeira etapa foi alcançada e se ateve à gerência de falhas. A próxima etapa na continuação do desenvolvimento do projeto SIORE, que não foi atingida por completo, deve atentar para a gerência de configuração, e, por último, gerência de segurança.

A principal função de gerenciamento de falhas é a supervisão de alarmes, pois está diretamente relacionada ao gerenciamento da informação sobre as condições de operação que afetam os serviços prestados por uma concessionária de Telecomunicações.

A supervisão de alarmes e telemedidas é uma função de monitoração de equipamentos da rede, enquanto a emissão de telecomandos é uma função de monitoração e controle desses equipamentos.

Este projeto se concentra exatamente neste ponto do sistema, sendo que tratará do gerenciamento de falhas nas centrais telefônicas de pequeno porte. As centrais de pequeno porte são centrais pequenas, com poucos assinantes, geralmente localizadas em localidades com poucas residências e muitas vezes em localidades remotas do estado.

Deve-se deixar claro que esta é uma iniciativa inovadora, pois não havia até agora empresa nenhuma que se dispunha a oferecer tais serviços a este tipo de clientes, sendo que a Telesc é a única do sistema Telebrás que se voltou para este lado dos seus serviços e não há noticia de empresa no mundo, que tenha feito qualquer trabalho nesta área. Primeiro porque é retorno financeiro direto seria pequeno, devido a ser um serviço que não pode ser cobrado diretamente, ao pouco número de assinantes que atingiria e a considerável infra-estrutura que exige e também porque as centrais deste tipo não foram projetadas visando fazer parte de tais sistemas, sendo que não apresentam nenhum tipo de facilidade ou preparo para fazer parte se um sistema como o SIORE.

Os próximos capítulos deste trabalho se concentrarão exatamente nestas centrais de pequeno porte e nas soluções encontradas para a sua absorção pelo SIORE.

CAPÍTULO 4 - Um Agente SNMP para Centrais de Pequeno Porte

O capítulo 4 entra em conceitos mais diretamente ligados ao projeto dos agentes para as CTPP, sendo que numa primeira parte explana sobre a estrutura geral, seguindo então para os sistemas de suporte, em especial do sistema operacional para o gerenciamento da rede e após isto trata de um rápida especificação dos componentes sistemas e de suas formas de interconexão.

4.1 - Estrutura Geral

Consiste em um esquema centralizado, onde uma estação (*host*) é configurada como **gerente** e os demais elementos da rede desempenham o papel de **agentes** ou **proxy agents**. Um **proxy agent** serve de procurador para aqueles equipamentos que não implementam o SNMP. Cada agente possui uma MIB que contém as variáveis relativas aos objetos gerenciados.

O modelo usado para o gerenciamento de redes TCP/IP (*Transmition Control Protocol / Internet Protocol*) inclui os seguintes elementos-chaves:

- Uma **estação de gerenciamento**;
- Um conjunto de objetos gerenciados, correspondente a um **agente** de gerenciamento e uma **MIB** associada, que é a base de informações de gerenciamento;
- Um protocolo de gerenciamento de redes, que é usado pela estação gerente e pelos agentes na troca de informações de gerenciamento.

Um **objeto gerenciado** representa um recurso que estará sujeito ao gerenciamento. Estes recursos podem ser vistos como objetos, onde cada objeto corresponde a um elemento de rede envolvido no sistema. Cada objeto é visto como uma coleção de variáveis cujo valor pode ser lido ou alterado, possibilitando, assim, a monitoração e o controle de cada elemento da rede.

A **estação gerente** pode ser vista como um sistema hospedeiro ou *host*, que executa as aplicações de gerenciamento e o protocolo de gerenciamento de rede, tomando decisões de acordo com as informações obtidas junto ao agente. Seu propósito geral é fazer *polling* para os agentes para coleta de informações através de primitivas *request*.

O **agente**, quando solicitado pelo gerente, encaminha informações ou altera valores das variáveis que representam os objetos gerenciados. Os agentes rodam em cada nodo da rede e coletam informações em cada dispositivo que se deseja gerenciar. Monitorando, desta forma, aplicações e recursos, os agentes podem notificar ao gerente de duas formas: instantaneamente, ao ocorrer um problema, através de *traps*; ou através de requisições do gerente, por meio de *gets* ou *sets*.

O modelo de gerenciamento adotado para o projeto possui inconvenientes quando o número de objetos gerenciados é muito grande, pois o tráfego de informações de gerenciamento pode sobrecarregar a rede, causando uma situação indesejada na rede real. Não se sabe ainda qual será o tráfego na rede para o número de agentes que teremos em cada localidade de cada superintendência.

Portanto, se um tráfego muito elevado ocorrer, será delegada a cada superintendência a responsabilidade de possuir um gerente na sua rede local, que fará papel de agente para o gerente principal, que estará em Florianópolis, no CGIR, e fará papel de gerente dos agentes de sua superintendência.

Um aplicativo chamado *mestre* é o responsável direto pela coleta de informações das placas de alarme (*escravo*) que estarão nos bastidores, através de varredura. O mestre será implementado como um *daemon*, ou seja, um programa que ficam rodando em *background*, entrando em funcionamento sempre que o agente for inicializado. O mestre possui variáveis de memória compartilhada com o agente SNMP. O agente lê os dados coletados pelo mestre, armazenando-os na MIB, para a futura requisição e alteração de informações realizada pelo gerente.

4.2 - Suporte de execução

4.2.1 - O Sistema Operacional para Gerenciamento da Rede

O desenvolvimento de um agente SNMP (*Simple Network Management Protocol*) depende diretamente do sistema operacional em que o mesmo irá funcionar. Em cada SO (Sistema Operacional) irá variar o ambiente de desenvolvimento do programa e sobretudo a forma de interação entre o agente e o sistema operacional em uso. Já o programa em si, será relativamente parecido de uma plataforma para outra, principalmente no que diz respeito as funções que executa. Existe uma variedade de sistemas operacionais para uso em estações de gerenciamento como, por exemplo, MS-DOS, Windows, UNIX, OS/2 e Windows/NT. Estes sistemas variam de acordo com suas potencialidades e desempenho para uso em uma estação de gerenciamento de rede - NMS (*Network Management Station*).

O UNIX é provavelmente o sistema operacional mais popular para estações de gerenciamento. Por ser um sistema operacional multitarefa, provê maiores facilidades para *background* e escalonamento de processos, e é bem mais robusto quando rodando múltiplas aplicações concorrentes. Como disse Doug Gwyn [Welsh 93]: "UNIX foi projetado para fazer com que as pessoas não pudessem fazer coisas estúpidas, porque seu sistema de policiamento mantêm as pessoas afastadas das funções de nível mais elevado de segurança".

O UNIX geralmente roda em máquinas mais caras, e consequentemente, o software de gerenciamento de rede para UNIX também fica mais caro. Devido às características deste sistema operacional, ele é ideal para redes maiores e mais complexas.

Pelo fato de possuir características e recursos considerados essenciais para o funcionamento do agente no sistema em questão, a plataforma de desenvolvimento do agente será UNIX. Por questões de custo, optou-se por uma máquina barata, como um PC, levando-se em consideração o número de estações que farão parte do sistema. Por

isso, será utilizada uma versão de sistema operacional UNIX para PCs, chamada Linux. Existem versões de Linux, a disposição na Internet, inclusive de graça. A gratuidade desse sistema e a possibilidade de rodá-lo sobre plataformas de hardware modestas não implica em uma menor robustez ou confiabilidade, ao contrário. As implementações atuais do Linux têm confiabilidade e robustez comparáveis à de versões comerciais do Unix, como Solaris, AIX e HP-UX.

4.2.2 - Sistema Operacional LINUX

O LINUX, uma versão do sistema operacional UNIX, alcançou notoriedade ao ser identificado como "o UNIX para PC". Foi anunciado pela primeira vez em novembro de 1991, desenvolvido por Linus Torvald, 23 anos, estudante de Ciência da Computação da Universidade de Helsinki, Finlândia. Torvald preparou o sistema para rodar em computadores com processador Intel 386 em diante.

Criado no final dos anos 60, o UNIX vem sendo desenvolvido em C desde a década de 70, com o objetivo de se tornar um ambiente portável. Isso ajuda a entender porque ele existe até hoje, ao contrário dos outros sistemas que morrem quando as máquinas ficam obsoletas.

Algumas versões do LINUX são comerciais, como o Solaris (Sun) e o AIX (IBM). Outras são de livre distribuição, como o próprio Linux, o FreeBSD e o NetBSD. Na verdade, o LINUX é um *freeware*. Pode ser distribuído obedecendo-se o "GNU Public Licence" (GPL).

O LINUX possui diversas distribuições, desenvolvidas por grupos de pessoas diferentes, onde variam, em geral, a maneira de instalar, o número de *softwares* que acompanham o sistema básico e a facilidade de manutenção do sistema.

4.2.3 - Linguagem de Programação C

O uso da linguagem C para implementação do agente justifica-se no fato das características desta linguagem estarem diretamente ligadas à portabilidade, eficiência e conveniência. Como o sistema operacional que estará nas estações agentes de gerenciamento é o LINUX, é natural pensar que a aplicação de gerenciamento também pode ser melhor configurada e desenvolvida com esta linguagem, permitindo assim utilizar os recursos deste sistema operacional.

Fatores de tendência também influenciam a escolha desta linguagem como construtora do agente, visto que a maioria dos sistemas de gerenciamento estão feitos em C/C++.

4.2.4 - Versão SNMP - CMU SNMP

O SNMP é um protocolo do modelo Internet para gerenciamento de redes. O CMU (*Carnegie Mellon University*) é uma implementação do SNMP, desenvolvida em linguagem C, portável para Linux, desenvolvido por Juergen Schoenwaelder e Erik Schoenfelder.

A versão atual do CMU SNMP é a 2.1.2, e a versão do Linux atualmente a disposição da Telesc é a Slackware 3.2.0, juntamente com a versão kernel 2.0.0 .

Estas são as versões do sistema operacional e da versão SNMP que são usadas para implementar os objetos gerenciados.

4.2.5 - Protótipo CMU-SNMP-LINUX

De posse dos códigos fontes do CMU, estudou-se toda a estrutura do programa, e foram identificados os módulos e funções que deveriam ser acrescentados para implementar as funcionalidades dos objetos gerenciados.

A primeira atitude foi fazer uma simples implementação para verificar o funcionamento e o comportamento do CMU. Foram acrescentadas na MIB duas variáveis ou *object-types*: localidade e alarme. Abaixo encontra-se uma parte da especificação da MIB para o teste inicial do protótipo, descrita em ASN.1.

```
tspLocalidade OBJECT-TYPE
        SYNTAX          DisplayString
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
                "The identification of the local of agent siore started."
        ::= { TspMIBObjects 1 }


tspAlarme OBJECT-TYPE
        SYNTAX          Integer
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
                "The number of alarm read from BAS."
        ::= { TspMIBObjects 2 }
```

4.3 - Estrutura do agente

4.3.1 - O Mestre

É um programa em PC, rodando LINUX, que controla, via porta serial, uma rede de placas microcontroladas que estão nos bastidores (NTSP) ou nas estações da TSP-20 (TSP). Ele implementa uma varredura para busca de alarmes, máscaras de telecomandos ou telemedidas e envia os comandos, recebidos do agente que roda em outro processo no mesmo PC, para a placa que o executa. A comunicação, para maior segurança, entre mestres e escravos é feita através de um protocolo proprietário da TELESC inspirado no BSC3 (*Binary Synchronous Communication 3*). A taxa de transmissão é de 9.600 bps. Devido às características é *half-duplex* e pode ser a dois (RS-485) ou quatro fios (RS-232C).

4.3.2 - O Agente

O *Agente SNMP* encontra-se como disposto na *Figura 4.3.2*, e é o responsável pela padronização do sistema para gerenciamento dos elementos de rede anteriormente descritos.

Uma observação importante deve ser feita. Por definição, um agente é um elemento que se encontra diretamente em um elemento de rede. Os elementos de rede que neste trabalho são descritos, não possuem agentes próprios. Na verdade, o agente aqui descrito é um agente procurador ou *proxy-agent* para esses equipamentos. Porém, pelo fato do agente estar rodando em um PC, e por este poder ser gerenciado através da MIB-II (parte integrante da MIB, ver figura 2.2.1), neste texto, adota-se a convenção de chamá-lo de agente ao invés de referenciá-lo como *proxy-agent*.

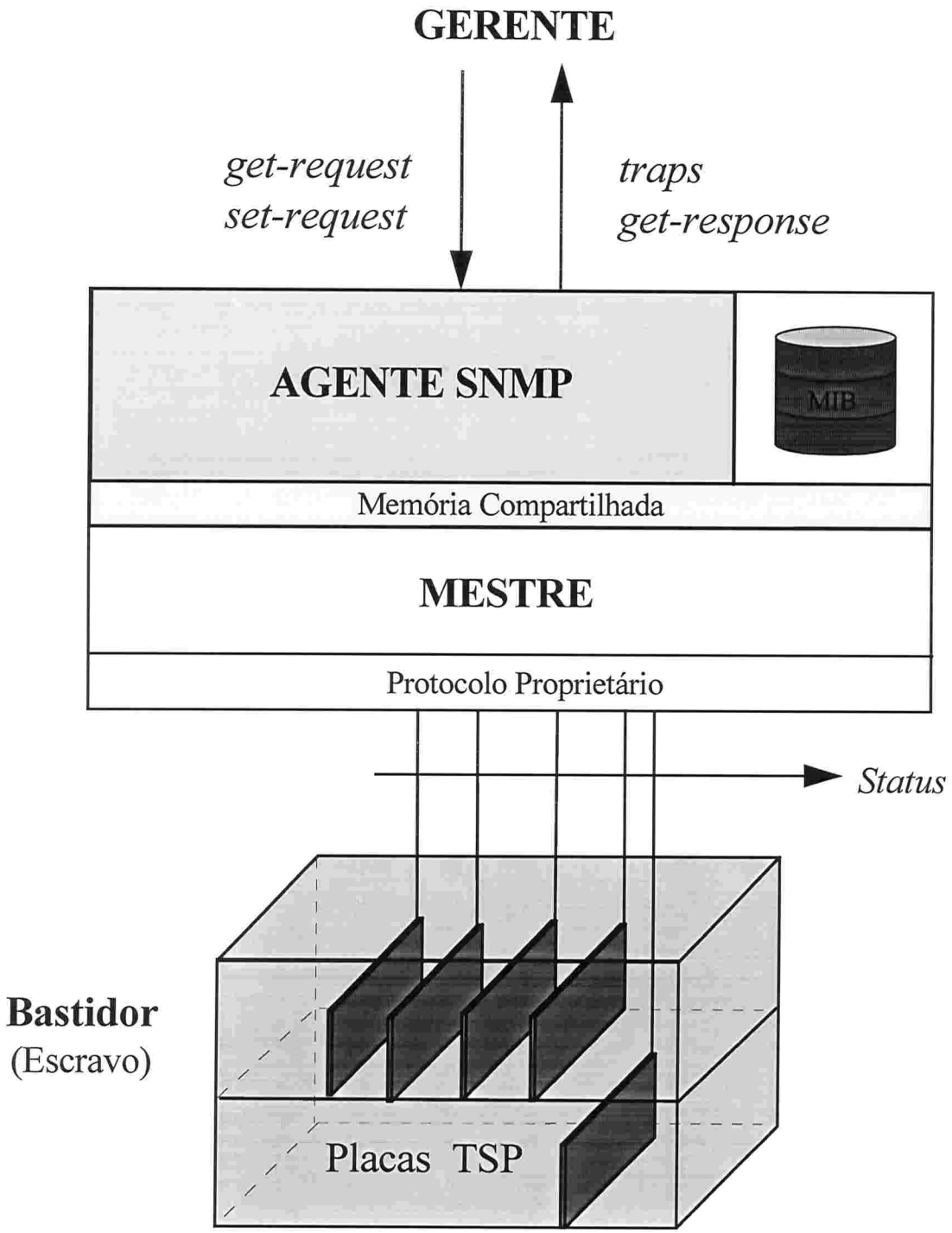

Figura 4.3.2 - Visão geral do sistema de Telessupervisão.

A taxa de transmissão é variável de acordo com o NE, podendo ser 1200 até 9600 bps.

4.3.3 - O Escravo

São um conjunto de placas microcontroladas (placas TSP), rodando um programa monitor em ROM que carrega um programa de operação em RAM. São basicamente de quatro tipos, a saber:

- Placas coletoras de alarmes (PCA), com capacidade de coletar 64 pontos.
- Placas de telecomandos (PTC), com capacidade de operar 32 pontos de contatos-secos.
- Placas de telemedidas (PTM), com capacidade de 8 pontos de entradas de sinais analógicos, como tensões, correntes, temperatura ou umidade, que são digitalizadas e armazenadas para serem enviadas ao mestre quando requisitadas.
- Placas controladoras da TSP-20 (AR21 e SPR2), controlam as funções de coletas de alarmes e operação de telecomandos das estações da antiga telessupervisão. Implementam o mesmo protocolo que as placas anteriores e se integram na mesma rede, se necessário.

4.3.4 - Comunicação Entre Processos - IPC

Existem várias formas de comunicação IPC (*Inter-Process Communication*). Este tipo de recurso possui métodos para múltiplos processos comunicarem-se uns com os outros. Existem vários métodos de comunicação entre processos que podem ser feitos através de:

•Pipes

•Queues

- Semáforos

- Memória compartilhada

- Sockets

Entre estes métodos, a utilização de memória compartilhada foi escolhida para a comunicação entre agente e mestre por esta ser a forma mais rápida de IPC, pois não há intermediações, como no caso *pipes* e *queues*.

Memória compartilhada pode ser descrita como um mapeamento de uma área ou segmento de memória que pode ser mapeada e compartilhada por mais de um processo. A informação é mapeada diretamente de um segmento de memória, e dentro de um espaço de endereçamento de um processo chamador. Um segmento pode ser criado por um processo e, subseqüentemente, ser escrito e lido por qualquer quantidade de processos.

Uma observação quanto à segurança deste tipo de IPC deve ser lembrada. Como o segmento de memória compartilhado pode ser lido por qualquer processo, um processo *intruso*, que saiba o segmento de memória que está sendo utilizado pela aplicação, poderá causar sérios danos às informações que o agente estará armazenando em sua memória. Estas informações expressam o estado do objeto, que está sendo coletado.

Entretanto, o sistema operacional provê mecanismos de segurança que dificultam este tipo de "atentado". O uso de memória compartilhada só pode ser realizado por um super-usuário. Ora, se um super-usuário cometer tal delito, desconfie. Um super-usuário tem acesso a todas as operações legais do sistema operacional a nível usuário.

A segurança pode ser aumentada protegendo-se os arquivos fontes, ou através de autenticação do segmento aloucado, no momento da aloucação. Porém, questões de segurança não estão sendo levadas em consideração neste projeto.

A IPC ocorre entre o *daemon* SNMP, que corresponde à aplicação agente, e entre um processo mestre, que é disparado pelo agente SNMP no momento de sua inicialização.

Na implementação do agente, existem cinco áreas de memória compartilhada. Cada uma delas comporta formatos de informação diferentes, compatível com o tipo de placa a que esta se refere. Este motivo justifica o uso de segmentos de memória distintos.

Quando o agente é inicializado, um arquivo de configuração, que contém as informações da respectiva estação de gerenciamento, é lido, e estes valores são armazenados em memória. Em seguida, a memória compartilhada é inicializada. O processo mestre é então disparado, e inicia-se a leitura das placas (escravo), através de varredura. O mestre armazena os valores lidos das placas nas mesmas áreas de memória onde o agente irá lê-las, quando da requisição de alguma primitiva *get* ou *set* realizada pelo gerente da aplicação.

Quando o gerente solicita um *get* (1), o agente executa uma primitiva *Return_StatusValue* (2); o mestre escreve ininterruptamente na memória (3), e a primitiva retorna o estado da informação solicitada (*Figura 4.3.4.a*).

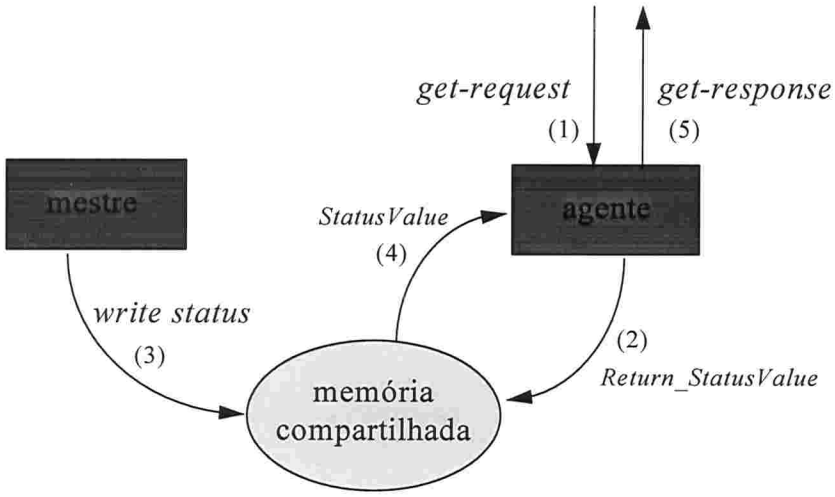

Figura 4.3.4 (a) - Agente realizando get com detalhe do funcionamento com memória compartilhada.

A informação poderá ser uma telemedida ou um alarme, que são atributos *READ-ONLY*, ou ainda o retorno de estado de um telecomando, que é um atributo *READ-WRITE*.

No caso do gerente solicitar um *set* (1), o agente realizará a escrita na memória compartilhada através da primitiva *Write_SharedMem* (2) (*Figura 4.3.4.b*).

O mestre, que estará lendo e escrevendo na memória compartilhada ininterruptamente, fará uma comparação de estados de telecomando toda vez que for escrever (3). Se o estado atual for diferente do estado anterior (4), enviará um telecomando para o escravo (5), que se encarregará de colocar o equipamento no estado requerido.

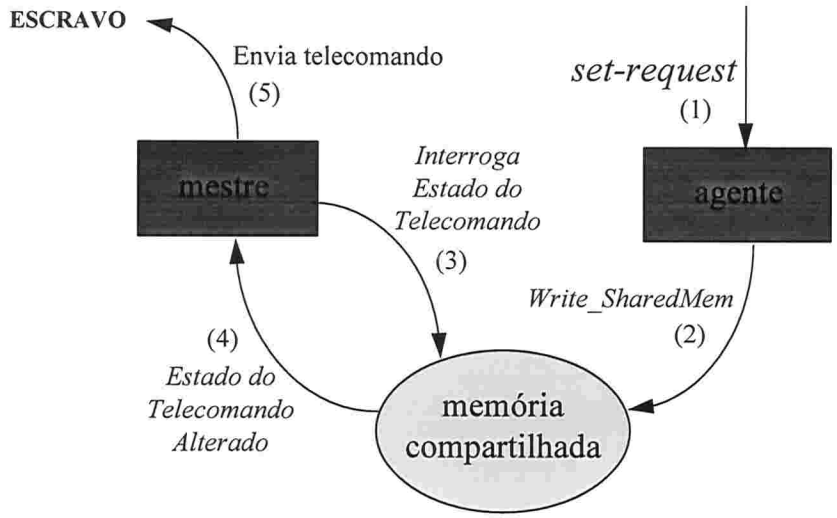

Figura 4.3.4 (b) - Agente realizando set com detalhe do funcionamento com memória compartilhada.

As primitivas *set* só serão atendidas para telecomandos. Não serão aceitos *set* para alarmes ou telemedidas.

4.3.5 - Tabela de Conversão

Por serem cinco os tipos de placa, cada uma com um formato de dados diferente, a configuração das placas nos *slots* dos bastidores deveria ser da maneira mais genérica possível, de modo que um técnico, em sua manutenção rotineira, pudesse retirar e colocar placas dos *slots* sem ter conhecimento da gerência de configuração do bastidor, que estaria disposta para um operador no CGIR em um painel gráfico adequadamente estruturado. Caso não ocorresse desta forma, certamente, com o passar do tempo surgiram

problemas graves e caros. Técnicos iriam fazer a manutenção dos bastidores e, se esses alterassem a configuração sem avisar a um operador do CGIR, alarmes trocados iriam começar a disparar sem nenhuma razão aparente e somente após uma investigação mais profunda, que poderia-se identificar o problema. Problemas como o alarme de central disparando, quando na verdade era de um grupo gerador, solicitação de envio de telecomando para um equipamento que nem requer este tipo de comando, entre outros problemas.

Outro fato importante para reforçar a idéia da variedade do sistema é que os tipos, a disposição e a quantidade de NEs a serem agregados a cada NMS é muito inconstante. Iriam existir lugares onde não poderíamos colocar um estação por motivos de ambiente e custos. Colocar um micro em algum lugar de difícil acesso ,como o topo de um morro, dentro de uma caixa de aproximadamente $2m^2$, para coletar alarmes de rádio-transmissão é, certamente, algo inadequado. Haveria dificuldades para alguém operar aquela estação, além da manutenção tornar-se acentuadamente complexa. A solução para este problema seria colocar, quando a disposição dos elementos de rede fosse bastante variada, mais de um bastidor para a mesma NMS. Por exemplo, equipamentos de ar-condicionado em prédios diferentes, próximos um do outro, seriam ligados a bastidores diferentes, mas a uma mesma NMS, reduzindo custos.

Além destes problemas, outro é bastante pertinente. Como fazer a interface entre agente e mestre de modo que *gets* e *sets* fossem realizados de maneira correta, no objeto correto, e na variável correta?

A solução encontrada foi montar uma tabela onde a coluna corresponde ao ponto de alarme na placa e a linha corresponde à posição do *slot* no bastidor. Estas informações estão em um arquivo de configuração, chamado siore.conf. Este arquivo possui informações para localizar exatamente um determinado estado de um equipamento em uma matriz bidimensional em memória.

Para localizar um *status* ou estado do objeto para uma determinada ocorrência, requerido em uma operação de *get* ou *set*, o agente localiza neste arquivo o tipo de placa, o número do bastidor, o número do slot e o número do ponto onde aquela informação está fisicamente ligada. Uma fórmula é aplicada para fazer as conversões necessárias e

localizar nesta tabela (matriz) o respectivo *status* para aquela respectiva ocorrência daquele objeto, dependendo do tipo de placa a qual aquele ponto estiver conectado.

O agente retorna uma informação *on* ou *off* para aquela ocorrência, que também está previamente definida no arquivo de configuração, se for placa de alarme. Se for placa de telecomando, a pedido do gerente o agente coloca um objeto nos seguintes estados: desligado, ligado no modo monoestável ou ligado no modo biestável. No caso de telemedida, retorna um valor inteiro.

4.3.6 - A MIB (ASN.1)

O CMU possui um *parser* para leitura da MIB. Possui os identificadores básicos da linguagem, mas é limitado a certas estruturas ASN.1.

Toda vez que o agente é inicializado este *parse* é realizado. Se houver algum erro na especificação da MIB, o agente acusará um erro e abortará o processo.

Na MIB especificada para a TELESC existem 14 identificadores de objeto. Os grupos transmissão e comutação são descritos com 14 tipos de objetos, enquanto que os grupos telessupervisão e infra-estrutura são descritos com 13 tipos de objetos. A diferença está baseada no campo rota, pois os objetos da telessupervisão e da infra-estrutura não necessitam este tipo de informação. Com exceção desta informação, todos os outros campos são idênticos.

Aqui identificamos uma limitação do SNMP. Como o modelo SNMP não possui conceito de herança, há a necessidade de se declarar todos os campos para cada um dos objetos, sendo que os campos dos objetos são todos idênticos.

4.3.7 - Arquivo de Configuração

Um agente deve possuir em algum dispositivo de armazenamento as informações inerentes a uma determinada configuração de uma estação. Esta configuração reflete a situação dos equipamentos da própria estação onde estará funcionando o agente.

Estas informações são lidas de um arquivo de configuração pelo agente no momento de sua inicialização, pois o sistema deve ser capaz de conhecer suas próprias configurações, e um meio volátil de armazenamento não garante a integridade das informações, devendo estas ficarem em um meio não-volátil, como é o caso de um arquivo.

As informações de gerenciamento as quais o agente irá monitorar pertencem às categorias estática e dinâmica. O arquivo de configuração irá conter informações estáticas, caracterizando a configuração atual dos elementos. As informações dinâmicas não necessitam estar neste arquivo, pois são informações ativas, geradas pelos NEs constantemente, e coletadas através de varredura. Exemplos de informações estáticas são a estação, o tipo de placa e identificação do equipamento. A informação dinâmica do sistema será o *status*, que pode ser um telecomando, telemedida ou alarme coletado.

Quando o agente for ativado, o arquivo de configuração será gerado e estará vazio, caso não exista este arquivo no sistema, e não haverá nenhuma informação estática. Através de *sets*, a configuração da estação será inserida.

Aqui encontra-se uma limitação do agente. Como não se sabe, a priori, quantas instâncias de um certo objeto existirão em uma determinada estação, e como a leitura do arquivo está condicionada a caracteres especiais para o reconhecimento das informações, quando houver a necessidade de se configurar um novo equipamento que for acrescentado na estação, haverá a necessidade de se criar uma nova linha no arquivo de configuração para que o agente reconheça, através dos caracteres especiais, que existe uma nova instância configurada. Atualmente, o agente não é capaz de realizar tal operação, visto que a gerência de configuração não foi implementada.

Para futuros aperfeiçoamentos do sistema, as sugestões seriam "ensinar" o agente a acrescentar uma nova linha no arquivo de configuração, ou, através de uma aplicação gerente, criar e configurar este arquivo com o auxílio de uma interface gráfica, onde uma opção faria uma baixa automática do arquivo por FTP ou TFTP para aquela estação, seguida da reinicialização do agente, através de uma gerência de configuração, que não foi abordada neste projeto.

CAPÍTULO 5 - Integração do Agente às Centrais Trópico R

Neste capítulo se descreverá a forma como foi desenvolvido o agente SNMP para as centrais do tipo Trópico R especificamente. Inicialmente haverá uma rápida descrição da peculiariedades da central em si, de seus problemas e então das soluções desenvolvidas.

5.1 - Trópico R

5.1.1 - Especificações da Central Trópico R

A Central Trópico R é uma central telefônica de comutação temporal controlada por programa armazenado (CPA-T) podendo ser utilizada como central tandem (trânsito) com multimedição ou combinada.

A central Trópico R é parte integrante de uma família de equipamentos de comutação temporal desenvolvida pelo Centro de Pesquisa e Desenvolvimento da Telebrás - CPqD, de acordo com o programa brasileiro de comutação temporal, que tem o objetivo de desenvolver equipamentos de comutação temporal para suprir as necessidades do Sistema Nacional de Telecomunicações - SNT.

A Telesc conta atualmente com 53 Centrais Trópico R no seu sistema, sendo que, estas centrais, somam um número de aproximadamente de 54500 telefones em todo o Estado de Santa Catarina.

A estrutura física da central, vide F*igura 5.1.1 abaixo*, é subdividida, do ponto de vista de manutenção, em: bastidores, sub-bastidores, placas de assinante e elementos não padronizados. Sendo os elementos não padronizados aqueles componentes da central que provêem a infra-estrutura que variam em dimensão e configuração, em relação aos demais elementos existentes na estrutura física da central.

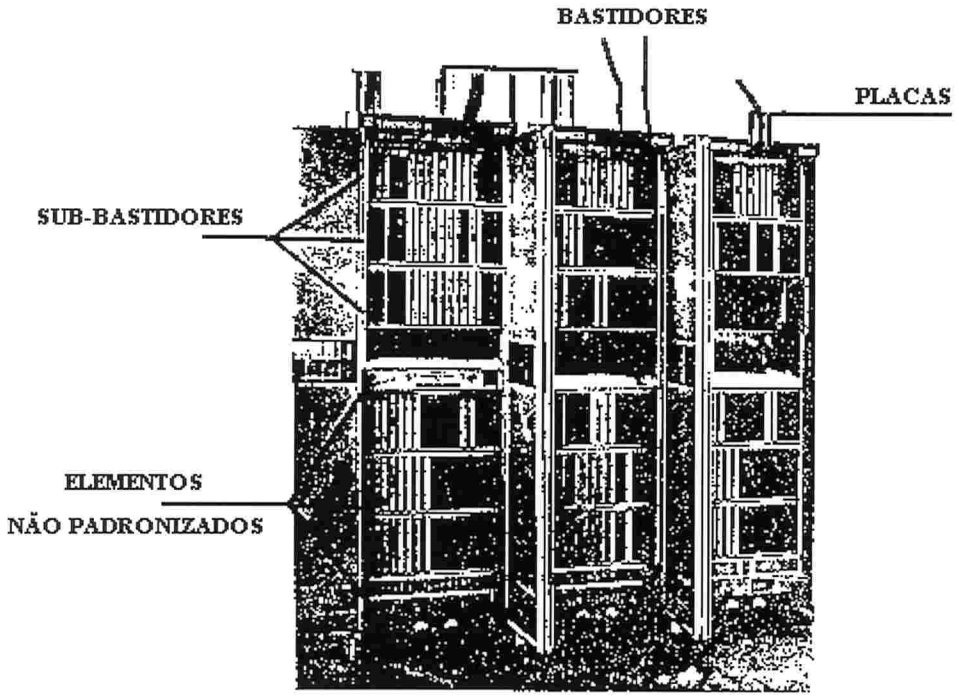

Figura 5.1.1 - Estrutura física da Central Trópico R

5.1.2 - O problema

O canal de comunicação entre a Trópico R e a Telesc até então era a linha discada. Os Técnicos da Telesc utilizavam-se de algum programa que discavam o número de acesso da central e implementava seu protocolo. Uma vez feita esta parte inicial enviavam comandos para a central, fazendo com que operações fossem realizadas por ela ou que emitisse algum tipo de relatório. Todos estes equipamentos e sistemas eram de tecnologia proprietária do fabricante, totalmente incapazes de passar informação para o SIORE.

Esta tecnologia proprietária era sigilosa, sendo que não havia documentação a respeito do protocolo ou dos meios de transmissão que a central teria para oferecer ao SIORE.

Além disso existe o problema devido a posição geográfica das centrais Trópico R, 51 ao todo, espalhadas por todo o Estado, desde São Lorenço D'Oeste até Canasvieiras, podendo haver dificuldades na hora da instalação do sistema no que condiz a parte física dele, mesmo porque, muitas alternativas tornam-se rapidamente inviáveis economicamente, devido ao enorme custo de colocar-se um PC rodando o agente para cada uma das centrais.

Desta forma pode-se relacionar vários problemas que devem ser resolvidos para que se crie um agente que de condições ao SIORE de comunicar-se com a central Trópico R. Os problemas devem ser resolvidos observando uma certa ordem lógica pois de outra forma o projeto teria que sofrer alterações constantes na sua forma e conteúdo.

5.1.3 - A solução

A seqüência de trabalho identificada foi:

1) Desenvolver um canal de comunicações com a Central Trópico R para substituição da comunicação via linha discada;

2) Descobrir qual o protocolo proprietário da Central Trópico R;

3) Desenvolver um Agente SNMP que tenha capacidade de comunicar-se com a Trópico R através do canal de comunicação desenvolvido e que implemente o protocolo previamente revelado;

4) Projetar a rede comunicações que disponibilizará a ligação entre os agentes desenvolvidos para a Trópico R e as centrais e entre os agentes e o SIORE propriamente dito.

5.1.3.1 - O canal de Comunicações

As centrais Trópico R tem cinco portas em sua estrutura, cada uma delas tem uma função definida (*Figura 5.1.3.1*), sendo que utiliza-se a porta RS232 para acessar-se a central via modem.

Os canais de comunicação são instalados de seguinte forma: a divisão de comunicação de dados instala uma ligação direta e permanente entre a central e o micro PC que tem o agente residente nele. Esta ligação é nada mais do que um para de fios trançados, o qual é composto de dois fios elétricos em cobre, isolados, e arranjados longitudinalmente de forma helicoidal, reduzindo os efeitos das induções eletromagnéticas parasitas. Esta linha é conectada ao micro através do modem. Dentre as opções disponíveis, o tipo de modem, que melhor se adequava as necessidades do projeto é o da Elebra, modelo EC3255.

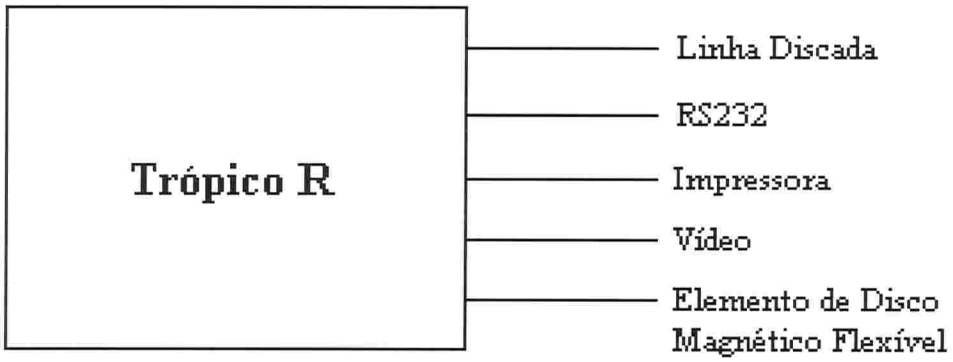

Figura 5.1.3.1 - Portas da Central Trópico R

O agente foi desenvolvido de forma a ter dentro dele os procedimentos para comunicar-se com o modem via porta serial COM1, sendo que as informações que a central envia são armazenadas em uma área de memória, ajustadas a uma forma adequada ao SIORE e enviadas a ele através da LAN ou de uma linha PPP, caso a LAN não esteja disponível entre o local onde se encontra o microcomputador e o SIORE.

A programação do modem necessária para conseguir-se comunicar-se com a central é 7E2 a 1200 bits por segundo, ou seja:

- O primeiro número define quantos são os bits de dados (*data bits*), os quais carregam as informações que estão sendo transmitidas. No caso deste agente o tamanho da palavra é sete.

- A letra define se existe ou não (*none*) o uso de paridade na comunicação e caso este procedimento esteja sendo utilizado, qual o tipo de paridade: se par (*even*) o valor da soma dos data bits com o stop bit deve ser par para a palavra estar correta, ou se impar (*odd*) a soma deve ser impar. O agente usa paridade do tipo par - E.

- O segundo número é a representação dos assim chamados *stop bits*, que representam o período mínimo de tempo em que a linha deve permanecer em uma condição determinada antes de uma nova palavra possa ser iniciada. O agente trabalha com um tempo de parada de dois bits.

- O último número representa a velocidade de transmissão dos bits durante a comunicação. O PC comunica-se com a central a uma velocidade de 1200 bits por segundo.

Por fim, deve-se configurar a porta da central Trópico R, que será utilizada para comunicar-se via modem com o agente, de forma assíncrona e com esta mesma velocidade de 1200, pois é a maneira que o programa comunica-se com a central.

5.1.3.2 - O Protocolo da Trópico R

O protocolo de comunicação da central do tipo Trópico R revelou-se bem simples, sendo basicamente uma abertura de comunicação seguido de um pedido de senha. Feito isto abre-se uma sessão de comunicação onde é feita a troca de comandos. Esgotadas as operações fecha-se a sessão e termina-se a comunicação entre a central e o PC.

O protocolo foi descoberto em grande parte pelo método da tentativa e erro, no processo também foi utilizada a ajuda de um analisador de protocolo e através da pesquisa nos manuais do fabricante da Trópico R, no caso o manual do fabricante que foi consultado foi o da Promom.

Sendo então que para obter comunicação com a central telefônica deve-se abrir uma sessão para comunicação, que seria nada mais do que um canal de comunicação. Para tanto segue-se um protocolo bem definido como descrito abaixo ou pode ser melhor visualizado na F*igura 5.1.3.2*:

1.Abre-se sessão enviando-se um "TAB" ou "CTRL I";

2. Recebe-se como resposta um pedido de envio de senha, da seguinte forma: "SENHA:";

3. Envia-se a senha correspondente a central que se quer comunicar. Estas senhas estão disponíveis nos manuais da Telesc.

4. A central identifica a senha enviada como válida ou não.

5a. Caso a senha seja identificada como válida pela central, a sessão é aberta e recebe-se o prompt "<" e a central fica aguardando os comandos do operador da Telesc.

5b. Caso a senha seja considerada invalida pela central, ela responde com a mensagem "SENHA INVALIDA" a central corta a comunicação e caso queira-se comunicar-se com a central, necessita-se reiniciar o processo desde o passo 1.

6. O operador envia os comandos que desejar e recebe as respostas, informações e relatórios correspondentes.

7. Fecha-se a sessão de comunicação com o comando "CTRL K", ou automaticamente, caso o operador permaneça mais de 6 minutos sem enviar nenhum comando para a central.

8. Em qualquer um dos dois casos a central envia a mensagem "FIM DE SESSÃO", caso o operador queira novamente comunicar-se com a central, necessita-se reiniciar o processo desde o passo 1.

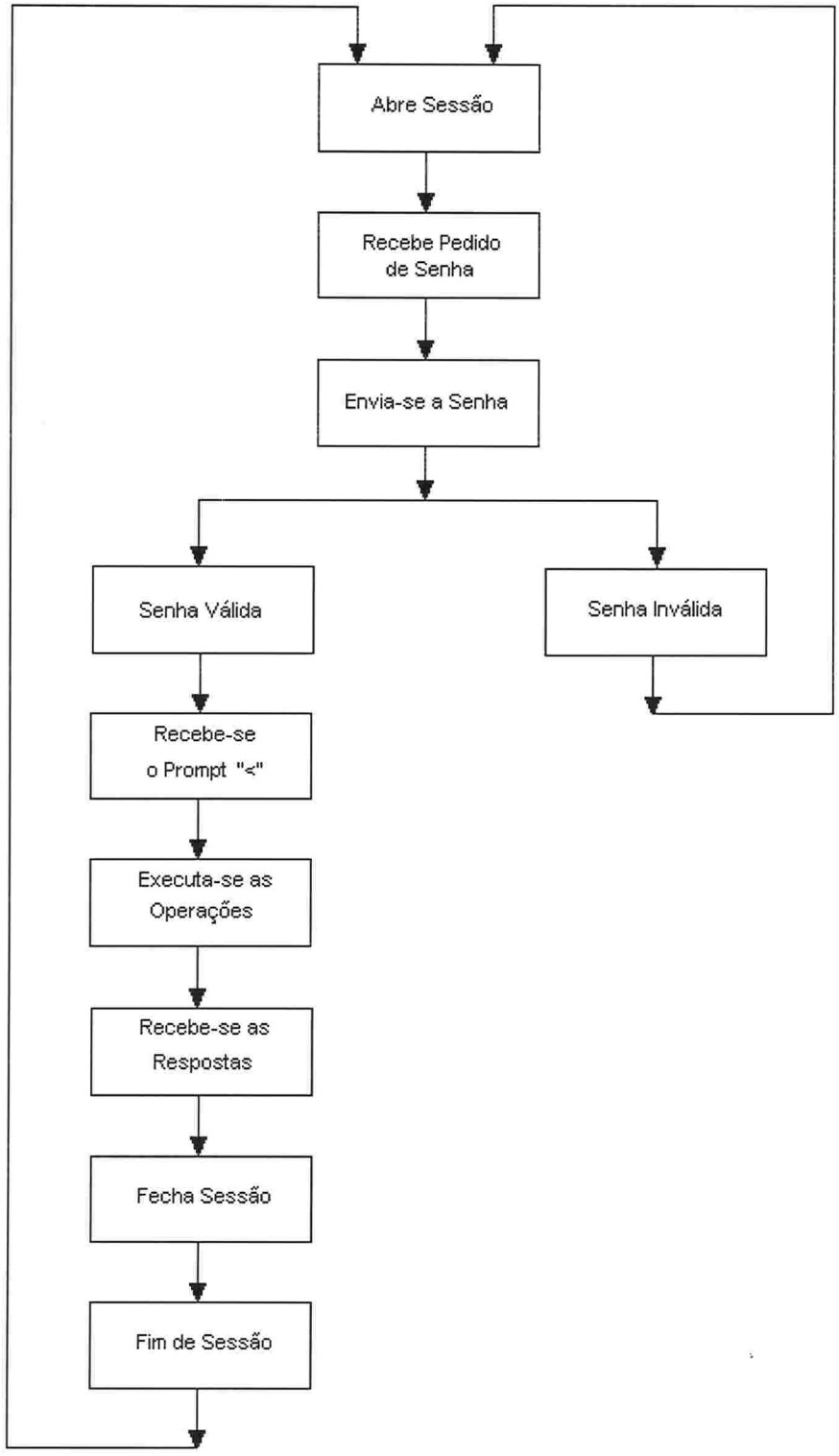

Figura 5.1.3.2 - Esquema do Protocolo da Trópico R

5.1.3.3 - O Agente para a Trópico R

Para tornar então, o SIORE capaz de comunicar-se com as CTPP do tipo Trópico R, um agente SNMP, doravante apenas chamado agente, foi desenvolvido. O agente foi implementado em C++ o qual esta disponível junto ao Linux para PC, sistema operacional que esta sendo usado pelo SIORE. Trata-se de um programa que habilita a comunicação entre o SIORE e a central Trópico R da seguinte forma. O agente foi desenvolvido dentro das especificações da programação orientada a objeto e é totalmente autônomo, não necessitando de nenhuma biblioteca ou programa de terceiros para rodar além do sistema operacional Linux.

O SIORE deseja enviar comandos para uma determinada central, o agente é identificado como responsável por comunicar-se com ela. Ele então é acionado e envia o comando do SIORE, recebe a resposta e a passa para o SIORE. O SIORE analisa a resposta e atualiza as informações no sistema, sendo assim, que dessa forma, a Trópico R é incorporada aquele painel com a visão geral do sistema, que o SIORE propõe-se a disponibilizar.

Independente disto, o agente de tempos em tempos emite o comando de IFALCE para a central. O comando nada mais é do que uma verificação se ela tem algum defeito em seu sistema, caso ela tenha a resposta ao IFALCE será algum código de alarme. Caso algum defeito seja identificado, o agente manda via *trap* (ver capítulo 2 - O Agente SNMP) o alarme para o SIORE que analisa a informação e toma a atitude adequada para resolução do problema.

5.1.3.4 - A Rede de Comunicações entre as Centrais Trópico R e o Siore

Devido ao grande número de centrais Trópico R, torna-se inviável economicamente colocar um PC dedicado para a monitoração de uma única central.

A solução encontrada foi instalar-se uma placa multiserial em um PC e ligar suas diversas portas uma em cada modem, sendo então que um único computador poderia fazer a varredura de alarmes em um número razoável de centrais. Cada um destes PCs

serão então ligados ao mestre (SIORE) pela LAN. A F*igura 5.1.3.4* ilustra o projeto da arquitetura da rede.

Deve-se deixar claro que esta é a arquitetura mais adequada para o caso das Trópico R e que para as Zetax e SPX 2000 serão consideradas outras alternativas, mais condizentes com a situação em particular de cada uma.

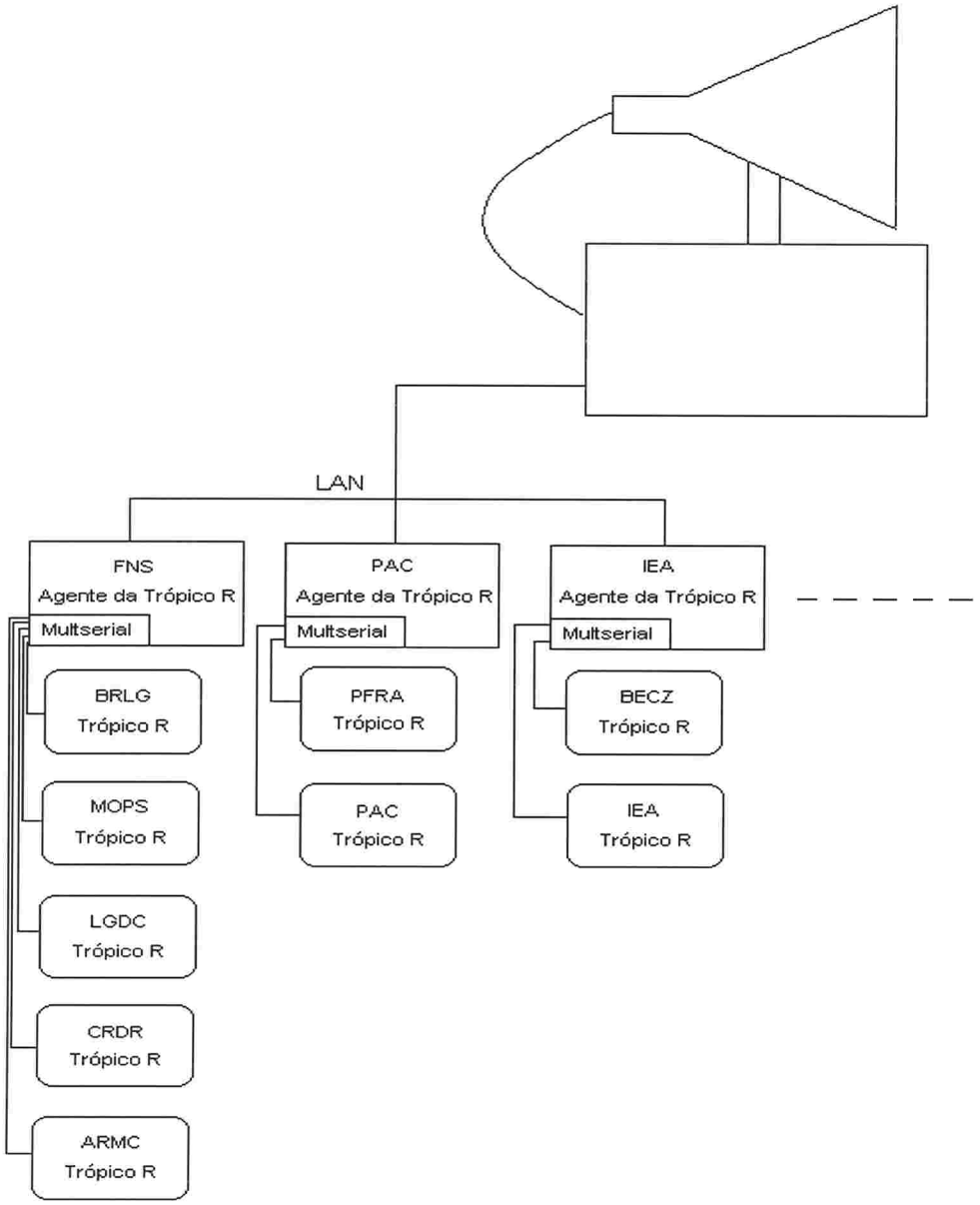

Figura 5.1.3.4 - Rede do SIORE para Telesupervisão Integrada da Trópico R

CAPÍTULO 6 - Integração do Agente às Centrais Zetax

No capítulo 6, seguindo o mesmo esquema do capítulo anterior, se descreverá a forma como foi desenvolvido o agente SNMP, agora para as centrais do tipo Zetax. Inicialmente haverá uma rápida descrição da peculiariedades da central em si, de seus problemas e, fianalmente das soluções desenvolvidas.

6.1 - Zetax

6.1.1 - Especificações da Central Zetax

Existem três modelos de centrais Zetax são chamadas ZTX-600, ZTX-610 e ZTX-632. Os três modelos tem basicamente a mesma forma e função para a Telesc, tanto que as diferenças entre eles nunca afetaram os processos de licitação para compra das centrais. Entretanto, estas diferenças afetaram em muito este projeto, como poderá ser visto no decorrer deste capítulo.

Mas estas diferenças afetaram em muito este projeto, como poderá ser visto em breve no próximo subtítulo *"6.1.2 - O problema"*, quando se voltará a este ponto.

Os dados que vem a seguir são genéricos e podem ser atestados nos três modelos da Central que existem.

Na Central Telefônica CPA Zetax, todos os procedimentos de operação são efetuados a partir de um microcomputador compatível com IBM-PC/XT ou AT equipado com o software ZTX-CTZ.

Este microcomputador, doravante denominado de ZTX-CTZ, poderá estar instalado local ou remotamente. Em qualquer das situações os procedimentos operacionais serão idênticos.

O ZTX-CTZ consiste de um conjunto de operação, manutenção e supervisão implementado em um microcomputador compatível, uma impressora paralela e um Modem CCITT/V22 com 1200 bits/s de velocidade, com discador e respondedor

automático. O ZTX-CTZ é compilado para ser executado sob sistema operacional com MS-DOS versão 2.1 ou mais recente.

Além de aceitar comandos teclados pelo operador, o ZTX-CTZ executa operações em paralelo, sem necessidade de intervenção ou comando explícito do operador.

Estas operações envolvem basicamente controle geral do sistema, com a execução das tarefas agendadas, como por exemplo, interrogação de contadores de tarifação, supervisão estatística, etc.

As centrais Zetax são as mais numerosas do sistema Telesc, sendo 81 instaladas por todo o estado. Devido ao fato de serem centrais pequenas, menos de 300 assinantes em média, geralmente localizam-se nas mais remotas localizações do Estado.

6.1.2 - O problema

Como foi visto acima, a única forma de comunicação entre as Centrais Zetax e a Telesc é através de um computador que possua o programa ZTX-CTZ. Os Técnicos da Telesc utilizam-se dele para realizar todas as funções de controle em geral. O programa realiza um procedimento de discagem do número de acesso a central e implementa seu protocolo. Uma vez feita esta parte inicial, envia-se comandos para a central, fazendo com que as operações desejadas sejam realizadas por ela, ou que emita algum tipo de relatório. O programa ZTX-CTZ é um software antigo, sendo que, a Telesc não tem acesso ao seu código fonte. O seu protocolo proprietário e incompatibilidade com outros sistemas, torna-o uma ilha inacessível para a base de dados da Telesc e totalmente incapaz de transmitir qualquer tipo de informação para o SIORE.

A Telesc possui três versões da Zetax a 600, 610 e 632. As do tipo 600 e 610 tem somente duas portas: uma remota e uma local. A *Figura 6.1.2* ilustra o problema acima descrito.

A porta local é utilizada para realizar-se operações na central in loco, geralmente pelo pessoal da manutenção que vai até a central propriamente dita para realizar algum conserto ou alteração.

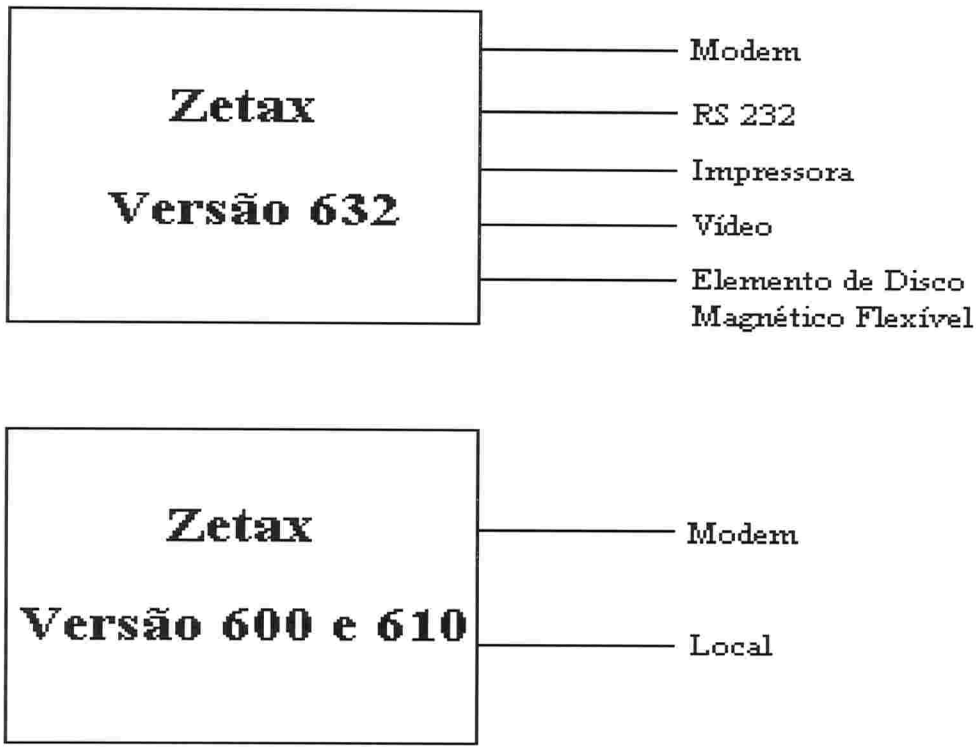

Figura 6.1.2 - Diferenças entre as portas disponíveis para as diversas versões das centrais do tipo Zetax

A porta remota é a ligação da central via modem com a Telesc. Esta porta é acessada via linha discada pelo programa ZTX-CTZ que foi anteriormente citado neste documento. Então caso se criasse um Agente para a Zetax que não falasse via linha discada e sim por qualquer outro meio, ocuparia-se a única entrada remota que a central dispõe e perderia-se todas as outras funções que o programa ZTX-CTZ implementa além da supervisão de falhas.

6.1.3 - A solução

Devido a inexistência de uma outra porta de acesso a centrais Zetax versão 600 e 610, optou-se por criar um canal de comunicações entre o agente e a Zetax via linha

discada, utilizando-se a mesma porta de entrada que é utilizada pelo programa ZTX-CTZ. Assim teremos a supervisão de alarmes da central implementado e agregado ao SIORE e manteremos os serviços que o ZTX-CTZ já oferecia.

Deve ficar claro que não há chance de haver quaisquer tipos de ações indesejadas entre os dois sistemas, pois as funções que continuaram a ser executadas pelo ZTX-CTZ são totalmente independentes do SIORE sem qualquer tipo de conexão tanto lógico como nos arquivos da central que utilizam.

A F*igura 6.1.3* ilustra a estrutura final do sistema descrito acima.

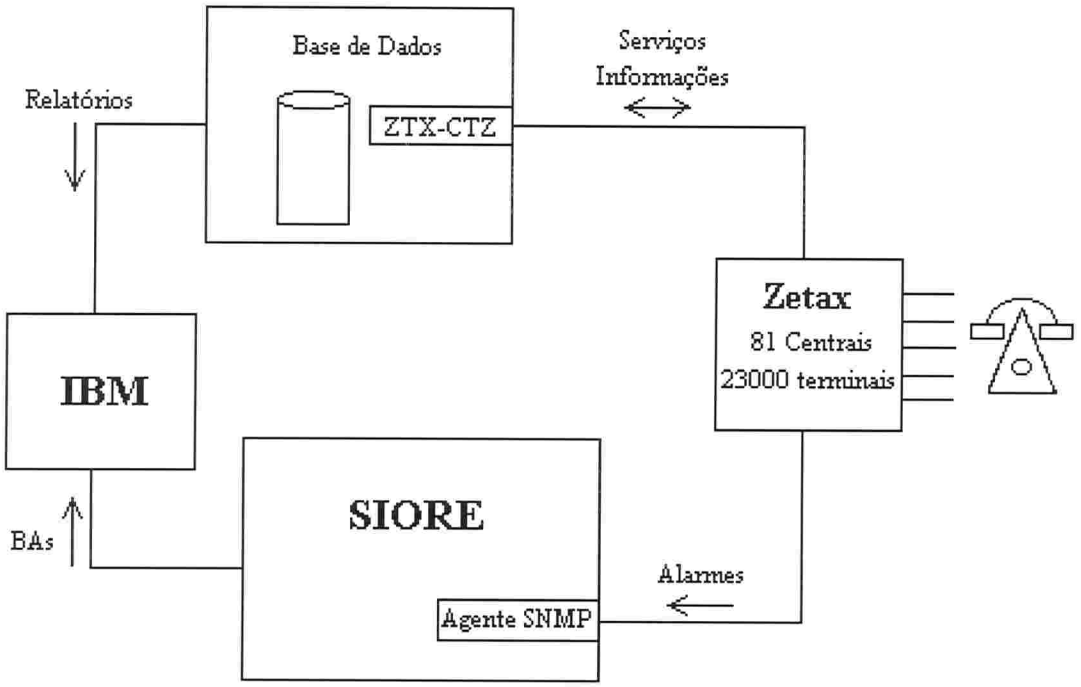

Figura 6.1.3 - Estrutura do sistema de gerenciamento das centrais do tipo Zetax

A seqüência de trabalho identificada foi:

1) Descobrir qual o protocolo proprietário da Central Zetax;

2) Desenvolver um Agente SNMP que tenha capacidade de interligar-se com as centrais do tipo Zetax através de um modem via linha discada, que identifique qual a

versão da Zetax com quem irá comunicar-se, implemente o protocolo previ revelado e envie os comandos adequados para cada versão diferente da Zetax;

3) Projetar a rede comunicações que disponibilizará a ligação entre os agentes desenvolvidos para a Zetax e as centrais e entre os agentes e o SIORE propriamente dito.

6.1.3.1 - O Protocolo da Zetax

O protocolo de comunicação da central do tipo Zetax revelou-se tremendamente complicado, sendo totalmente diferente de qualquer outro que a Telesc já teve contato.

A comunicação é feita através de quadros de informação, sendo que após ocorrida a discagem para a central e configurada as portas seriais, o agente pode imediatamente começar a enviar comandos de operações ou pedidos de relatórios em forma de quadros e receber as respectivas respostas desta mesma forma.

Os quadros tem um estrutura formal padrão, mas variam para cada versão da Zetax, causando isto, com que fosse necessário muito mais trabalho para descobrir os formatos dos quadros para cada uma das versões da Zetax que a Telesc possui.

Assomado a isto em cada quadro é emitido um par de bits detetor de erros que são calculados em função das informações existentes nos quadros. Devido a isto, o agente deve ser capaz de realizar o cálculo deste par de bits cada vez que um for enviar um quadro para a central.

O método de detecção de erros utilizado pele Zetax é um código polinomial, também denominado CRC (*cyclic redundancy code*). Nos códigos polinomiais, considera-se que os bits de uma cadeia de caracteres são os coeficientes de um polinômio, coeficientes estes, capazes de assumir apenas dois valores: 0 ou 1. Assim, um bloco de k bits é visto como uma série de coeficientes de um polinômio de k termos, indo de x^{k-1} a x^0. Por exemplo, a palavra 110001 contém 6 bits e representa o polinômio $x^5 + x^4 + 1$ (coeficientes contando da esquerda para a direita).

A utilização de códigos de detecção de erros polinomiais é baseada na escolha de um código especial que caracteriza um *polinômio gerador* G*(x)*. Uma exigência em relação a este polinômio é que os bits mais significativo e menos significativo (correspondendo, respectivamente aos coeficientes de mais alta ordem e de mais baixa ordem do polinômio) sejam de valor 1. A técnica consiste em adicionar um bloco de dados (caracterizando um polinômio de M*(x)*) um conjunto de bits de controle de modo que o quadro (dados + bits de controle) seja divisível por G*(x)*. Na recepção, a entidade de Enlace efetua a divisão dos bits compondo o quadro pelo polinômio gerador. Caso o resto seja diferente de zero, é caracterizado então a ocorrência de um erro de transmissão. [Stemmer 93]

O código polinomial adotado pela Zetax é um código bem conhecido comercialmente, assim chamado CRC-CCITT, que corresponde ao polinômio $x^{16} + x^{12} + x^5 + 1$.

A F*igura 6.1.3.1* ilustra um quadro padrão enviado e um recebido respectivamente durante uma comunicação entre o agente e uma central Zetax versão 600, sendo que os quadros das versões 610 e 632 aumentam em tamanho e complexidade.

A forma do quadro que o agente envia é o seguinte:

- Byte 1 : 00;

- Byte 2 : A senha da central que está cadastrada em arquivo que o agente consulta;

- Byte 3 : Não foi descoberto a função deste Byte, mas observou-se através do analisador de protocolo que seus valores eram sempre os mesmos e com uma seqüência fixa, então simplesmente o agente copia os valores que eram enviados pelo ZTX-CTZ;

- Byte 4 : Indica o número de Bytes de informações que o quadro contém;

• Byte 5 : Este Byte é um enumerador de comandos que o agente manda para a central, sendo que sempre é incrementado em um a cada novo comando enviado;

• Byte 6 em diante : Comandos do agente;

• Últimos dois Bytes : Código corretor de erros calculado em função dos Bytes anteriores.

A forma do quadro que o agente recebe da Zetax é o seguinte:

• Byte 1 : A senha da central;

• Byte 2 : 00;

• Byte 3 : Não foi identificado qual é o significado dos valores recebidos neste Byte;

• Byte 4 : Indica o número de Bytes de informações que o quadro contém;

• Byte 5 : Este Byte é 00 enquanto a central tiver um próximo quadro para ser enviado após este, sendo que é setado em FF quando for o último quadro que a central vai enviar;

• Byte 6 : Neste Byte é escrito o código da falha, sendo este o valor que o agente envia para o SIORE;

• Byte 7 em diante : Outros dados sobre a falha como data, hora, localidade, etc.;

• Últimos dois bytes : Código corretor de erros calculado em função dos Bytes anteriores.

00	Senha da central	?	Tamanho do quadro	Bit enumerador	... Dados ...	Código detector de erros

Forma dos quadros enviados pelo agente

Senha da central	00	?	Tamanho do quadro	Indica fim da lista de falhas	Código das falhas	... Outros dados ...	Código detector de erros

Forma dos quadros enviados pela central

Figura 6.1.3.1 - Quadros de comunicação da central Zetax

O protocolo foi descoberto eminentemente pelo método da tentativa e erro, tornando-se um processo muito lento baseado somente na observação através de um analisador de protocolo da comunicação entre as Zetax e o programa ZTX-CTZ

6.1.3.2 - O Agente para as Centrais Zetax

O agente SNMP que foi desenvolvido para tornar o SIORE capaz de comunicar-se com as CTPP do tipo Zetax foi implementado em C++ o qual esta disponível junto ao Linux para PC, sistema operacional que esta sendo usado pelo SIORE.

O agente foi desenvolvido dentro das especificações da programação orientada a objeto e é totalmente autônomo, não necessitando de nenhuma biblioteca ou programa de terceiros para rodar além do sistema operacional Linux.

O SIORE envia pedido de teste para uma determinada central Zetax, o agente é identificado como responsável por comunicar-se com ela. Quando o agente é acionado ele recebe o código identificador da central, com este código varre um arquivo de dados para obter também o número de acesso a central, sua senha e a versão da Zetax com qual entrará em contato. Feito isto ocorre a discagem via modem, caso a central não esteja disponível no momento, uma nove tentativa será feita em cinco minutos. Uma vez

acessada a central programa-se a porta serial para 8E1 a 1200 bps, velocidade da linha discada.

De acordo com a versão da Zetax que se está testando envia-se o comando do SIORE, ao receber o resultado o envia para o SIORE. O SIORE de posse destes dados atualiza as informações no sistema.

Independente disto, o agente tem um arquivo das centrais Zetax existentes na Telesc e realiza uma varredura das centrais emitindo o comando de IFALCE para cada uma das centrais. Caso algum defeito seja identificado, o agente manda via *trap* (ver capítulo 2 - O Agente SNMP) o alarme para o SIORE que analisa a informação e toma a atitude adequada para resolução do problema.

A F*igura 6.1.3.2* a seguir, vem ilustrar a seqüência de passos de um teste padrão da Zetax.

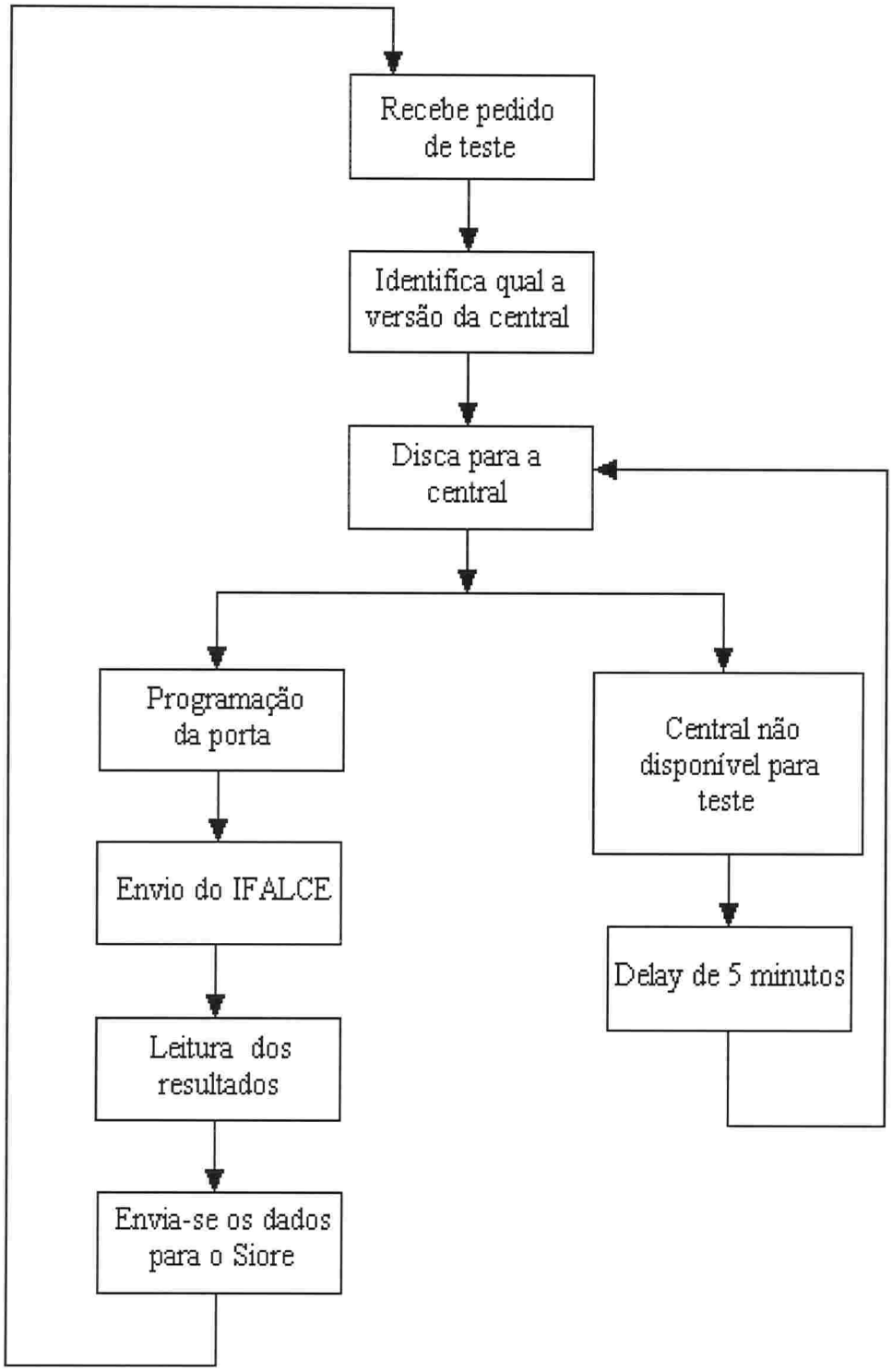

Figura 6.1.3.2 - Estrutura de um teste padrão nas centrais do tipo Zetax

6.1.3.3 - A Rede de Comunicações entre as Centrais Zetax e o Siore

Devido ao pequeno número de assinantes, menos de 23000, da Telesc que tem sua linha telefônica oferecida pelas centrais Zetax, designou-se apenas um PC, que fica localizado no CGIR, no Itacorubi, para ficar responsável por realizar os testes agendados pelo SIORE e realizar a varredura de todas as centrais no Estado.

A varredura é feita através da discagem via modem e demora em torno de 80 minutos para ser completada.

As informações obtidas pelo agente são transmitidas para o SIORE pela LAN da Telesc.

CONCLUSÃO

A Telesupervisão é uma das funções primordiais de uma companhia de telecomunicações. Sendo um processo de contínuo aperfeiçoamento de forma a melhorar o desempenho da planta de uma forma geral. O SIORE é um sistema de gerência que vem sendo desenvolvido pela Telesc para desempenhar esta função.

O agente da Telessupervisão, desenvolvido neste projeto, apresenta interface padrão para a comunicação com a futura plataforma de gerência da TELESC, o SIORE, característica que os outros sistemas desenvolvidos até então não possuem. Por isso, este é um sistema pioneiro no setor de telecomunicações em Santa Catarina, e o primeiro do porte em todo o país, desenvolvido "*in house*".

Muitas modificações ainda serão feitas no protótipo desenvolvido, pois a cada evolução no sistema, será acrescentada alguma funcionalidade a mais no agente, mas de qualquer forma, todo um sistema de suporte para esta evolução está desenvolvido e a disposição para acompanhar esta evolução.

Os agentes que foram desenvolvidos, o foram através de um estudo das centrais telefônicas em questão, de pesquisas no material encontrado sobre qualquer tentativa de comunicação com as centrais feitas até então e finalmente com a ajuda de ferramentas de hardware e software adequados ao contexto.

O desenvolvimento de *softwares* para gerenciamento de redes é um trabalho que exige associação dos conceitos de gerência com paradigmas de programação, para que a implementação reflita todas as definições e padrões adotados para a interoperabilidade entre sistemas.

O desenvolvimento deste tipo de sistema é muito proveitoso para as concessionárias de telecomunicações, pois gera facilidades que lhes possibilitam realizar com muito mais agilidade operações de elevada importância para a manutenção da qualidade dos serviços oferecidos pela empresa. Um exemplo disto é que, a velocidade de

comunicação entre o gerente e os equipamentos de telessupervisão, sai dos atuais 75 *bauds*, para uma taxa superior a 2.400 bps.

Outras vantagens da solução adotada é que é possível gerenciar o software do agente através da MIB-II, além de ser introduzida a recente supervisão de telemedidas, e a plataforma de hardware adotada é bastante barata comparada com outras arquiteturas que não são baseadas em PCs.

Neste primeiro passo foram os alarmes. Implementado os alarmes, partiu-se para a implementação dos telecomandos e telemedidas, estes dois últimos incompletos, e precisam ser revistos, pois foram implementados para se observar resultados imediatos.

Algumas considerações devem ser feitas para que este projeto não pare por aqui e evolua até atingir seu objetivo completo.

É importante lembrar que a aplicação gerente não faz parte deste projeto, mas este trabalho deve ser consultado como referência para a sua implementação, pois contém informações relevantes para o efetivo desenvolvimento da aplicação de gerenciamento.

Outro aspecto relevante que deve ser levado em consideração é a gerência de configuração e segurança, que devem ser implementados para que o agente seja funcionalmente completo.

Bibliografia

[Welsh 93]

WELSH, MATT - "Linux Installation and Getting Started". Linux Documentation Project, 1° edição, Agosto de 1993.

[Ribeiro 80]

RIBEIRO, MARCELLO - "Telecomunicações: Sistemas Analógicas - Digitais". EMBRATEL, Livros Técnicos e Científicos, Editora S.A. 1980.

[SIEMENS 75]

"Teoria do Tráfego Telefônico: Tabelas e Gráficos". Volume 1, SIEMENS AG. Editora Edgard Blucher Ltda. 1975.

[Stallings 93]

STALLINGS, W. - "SNMP, SNMPv2 and CMIP - The Pratical Guide to Network-Management Standards". Addison-Wesley, 1993.

[Perkins 97]

PERKINS, DAVID T. - "Understanding SNMP MIBs". 1997.

[Brisa 93]

BRISA - "Gerenciamento de Redes - Uma Abordagem de Sistemas Abertos". McGraw-Hill, São Paulo, 1993.

[Stemmer 93]

STEMMER, MARCELO RICARDO - "ELL 5184 Sist. Distribuídos e Rede de Computadores p/ A.I.". UFSC, Florianópolis, 1993.

[APOSTILA]

APOSTILA "Básico de Sistemas de Telecomunicações". Telecomunicações de Santa Catarina - TELESC S.A., Centro de Treinamento, 1996.

[Goldt]

GOLDT - "Sven et al, The Linux Programmer's Guide". Março, 1995.

[Montenegro]

MONTENEGRO, F. & Pacheco, R. - "Orientação a Objetos em C++". Editora Ciência Moderna, Rio de Janeiro, 1994.

Anexo 1 - A ASN.1 (Syntax Abstract Notation One)

A ASN.1 é uma notação usada para descrever as estruturas de dados, que serão enviadas por um protocolo de gerenciamento, e a informação contida nestas estruturas. Pode ser vista como uma linguagem formal abstrata, baseada em gramática, independente de máquina.

Para transmitir a ASN.1 através da rede são usados *Basic Encoding Rules* (BER). Isto é análogo a usar um compilador para converter código fonte para código objeto.

A ASN.1 é atualmente uma idealização feita pelo grupo OSI, e este grupo adotou uma política para que a ASN.1 pudesse ser usada pelo SNMP, prevendo futuramente uma fácil transição deste protocolo para protocolos de gerenciamento baseado no modelo OSI.

Até onde se sabe, a reservada comunidade Internet nunca se propôs a negociar com esta questão, e foi sutilmente forçada a adotar esta solução.

Entretanto, para manter tudo simples, de modo a não causar também impacto nos nodos gerenciados, somente um subconjunto da ASN.1 é usada pelo SNMP.

Uma coleção de descrições ASN.1 deve estar sempre contida em um módulo. Por exemplo:

<ModuleIdentifier> DEFINITIONS ::= BEGIN
[linkage]
[declarations]
END

O **ModuleIdentifier** pode ou não ser único (seria se estivesse sendo usado em uma biblioteca).

A seção **linkage** é onde se declara a ASN.1 para incluir informações de outros módulos (importação), ou para deixar estas informações acessíveis para outros módulos (exportação).

As seções **declarations** é onde vão as definições ASN.1. Estas definições podem ser tipos, valores ou macros. Por exemplo:

type-name ::= TYPE

value-name type ::= VALUE

- type-name é o nome do tipo.
- TYPE é o nome de um tipo existente.
- value-name é o nome de um valor (uma variável).
- VALUE é o valor atual a ser colocado em "value holder" (variável).