UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

ESCOLA DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

RELATÓRIO DE ESTÁGIO SUPERVISIONADO

ENG04497 – ESTÁGIO SUPERVISIONADO

DATACOM TELEMÁTICA

NOME: TIAGO DALL'AGNOL – 2877/98-0

SUPERVISOR: ENG. MARTIN A. F. MELLO

ORIENTADOR: PROF. MARCELO S. LUBASZEWSKY

PORTO ALEGRE, 12 DE MARÇO DE 2003.

Sumário

Folha de Avaliação

Lista de Figuras

Lista de Abreviaturas

ATM	Asynchronous Transfer Mode
DECnet	Digital Equipment Corporation Network
IEEE	Institute of Electrical and Electronic Engineers
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LUT	Look-Up Table
MAC	Media Access Control
MIB	Management Information Base
PC	Personal Computer
PPP	Point-to-Point Protocol
RAM	Random Access Memory
ROM	Read Only Memory
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

Resumo

Este relatório descreve as atividades desenvolvidas dentro da disciplina de Estágio Supervisionado III (ENG 04497), realizado entre os meses de dezembro de 2002 e fevereiro de 2003, na empresa DataCom Telemática, fabricante de equipamentos na área de telecomunicações.

A atividade desenvolvida consiste no projeto e desenvolvimento de um agente SNMP, que é, de um modo geral, o responsável pela coleta de informações do equipamento. O equipamento poderá ser qualquer equipamento de telecomunicações, como um modem, um conversor de interface, um multiplexador E1, etc. É o agente quem possibilita o acesso a informações pertinentes ao hardware e ao estado de funcionamento destes equipamentos.

Os objetos de estudo principal foram a linguagem C, o sistema operacional Linux e o protocolo SNMP.

1. Introdução

O estágio supervisionado proporciona ao graduando um amadurecimento necessário para sua conduta profissional futura, colocando-o frente a frente com os desafios e situações corriqueiras da profissão de Engenheiro.

No decorrer do estágio, é notório o amadurecimento do aluno, visto que pouco a pouco os problemas vão aparecendo, e precisam ser solucionados. Além da bagagem técnica adquirida, o lado profissional também é explorado, mostrando assim que além dos conhecimentos adquiridos na área técnica também é vivenciada a parte de organização, responsabilidade e intercomunicação com outros membros da empresa.

O presente relatório tem a finalidade de descrever as atividades desenvolvidas pelo estagiário Tiago Dall'Agnol durante o período de estágio supervisionado obrigatório, tendo como supervisor o Eng. Martin A. F. Mello e como orientador o prof. Marcelo S. Lubaszewski. Este relatório não se propõe a ser detalhista em sua abrangência, e sim dar uma visão geral dos aspectos considerados de maior importância durante o decorrer do estágio. Ele contém a apresentação da empresa, seguindo-se de uma descrição das atividades desenvolvidas, juntamente com comentários, resultados e conclusões a respeito dos trabalhos realizados.

2. Apresentação da Empresa

2.1. A Empresa

A DataCom Telemática desenvolve, fabrica e comercializa produtos e acessórios voltados para a área de telecomunicações. Fundada em 1996, seus principais segmentos de atuação são:

- Conversores de interface
- Multiplexadores E1 flexíveis com facilidade cross-connect
- Multiplexadores E3
- Conversores de velocidade para redes LAN e WAN
- Placas de gerenciamento SNMP para modems
- Modems profissionais de alta velocidade

A Empresa atua também na área de projetos de MLA (Multiplicadores de Linhas de Assinantes Digitais), Modems HDSL e no desenvolvimento de aplicativos integrados à plataforma de gerenciamento HP Openview para controle de equipamentos que suportem SNMP.

As placas de gerenciamento possibilitam que um agente SNMP, como por exemplo HP OpenView, possa gerenciar modems padrão Telebrás, permitindo dessa forma incorporar os modelos à rede de gerência centralizada. Muitos dos novos equipamentos já têm um agente SNMP "embutido".

O quadro funcional da empresa é composto por Engenheiros Eletricistas, Bacharéis em Ciências da Computação, técnicos em eletrônica, estagiários e funcionários administrativos.

Além de sua sede em Porto Alegre, a empresa também está presente na cidade de São Paulo, onde mantém um escritório comercial.

2.2. Informações diversas

Razão social:	Teracom Telemática Ltda
Nome Fantasia:	DataCom Telemática
CGC:	02.820.966/0001-09
IE:	096/2724084
Endereço:	Avenida França, 735
	Bairro Navegantes
	CEP 90230-220
	Porto Alegre – RS
Telefone:	(51) 3358 0100
Fax:	(51) 3358 0101
E-mail:	datacom@datacom-telematica.com.br
Web Site:	http://www.datacom-telematica.com.br

2.3. Principais Produtos

2.3.1. DM703-64S – Conversor de interface G.703 x V.25 – V.36

Figura 2.1: DM703-64S – Conversor G.703 x V.25-V.36

O DM703-64S é um equipamento que converte sinais do tipo G.703 codirecional a 64kbit/s para sinais das interfaces V.35 ou V.36/V.11. Constitui-se de uma placa padrão Telebrás que pode ser utilizada tanto em gabinetes quanto em sub-bastidores padronizados. A seguir são descritas suas principais características:

- Interfaces V.35 ou V.36/V.11, selecionáveis por estrapes.
- Apresenta-se em conector DB25 fêmea no gabinete ou sub-bastidor, com pinagem conforme ISO 2110 Amd. 1 - compatível com RS-530.
- Opção de interface Ethernet 100BaseTx com bridge remoto no modelo DM703-64SE.
- Velocidades de 64kbit/s, 128kbit/s ou 256kbit/s, utilizando a codificação definida na recomendação G.703 para 64kbit/s.
- Receptor G.703 suporta distâncias de até 1 km em par trançado 0,40mm.
- Operação com relógio interno, externo ou regenerado a partir do sinal G.703 recebido.
- Comutação automática para relógio interno na falta de relógio externo ou na falta de sinal G.703.
- Laço analógico local, laço digital local e laço digital remoto (V.54) através de teclas no painel frontal ou por CT140 e CT141.

- Gerador de padrão de teste com detector de erros, acionado por tecla no painel frontal.
- Leds indicadores de CT103, CT104, CT105, CT109, TESTE, ERRO e alimentação.
- Permite desabilitar as funções das teclas do painel.
- Gerenciamento padrão Telebrás, que em conjunto com o cartão de gerenciamento DMG20 da Datacom, permite que o conversor DM703-64S seja monitorado por um gerente SNMP. Também permite que o gerente ative laços de teste para verificação de desempenho e localização de falhas no enlace.
- Placa padrão, de acordo com Prática Telebrás 225-540-780

2.3.2. DM704CE - Conversor G.703 - G.704 x Ethernet 10BaseT

Figura 2.2: DM704CE – Conversor G.703 – G.704 x Ethernet 10BaseT

O DM704CE é um equipamento que converte sinais do tipo G.703 a 2048kbit/s, com estrutura de quadros conforme G.704, para um bridge remoto Ethernet. Apresenta-se em gabinete mesa (175x238x43mm) com alimentação 93 a 253 Vac ou 36 a 60 Vdc com seleção automática. A seguir são descritas suas principais características:

A função básica do Bridge é segmentar uma rede local, evitando que tráfego Ethernet local seja transmitido pelo canal E1, desperdiçando banda (capacidade). Filtra o tráfego da rede local e transmite para a interface G.703/G.704 apenas os pacotes correspondentes a endereços MAC não existentes na rede local, além de pacotes de broadcast e multicast. O atraso introduzido pelo processamento do Bridge é de 1 frame Ethernet.

O Bridge opera no nível MAC da interface Ethernet. Desta forma é totalmente transparente para os protocolos das camadas superiores, tais como TCP/IP, UDP, DECnet, etc.

O bridge pode operar em half-duplex ou full-duplex. A interface Ethernet do DM704C sII é do tipo 10BaseT (par trançado), conforme especificado pela IEEE 802.3. O conector RJ45 apresenta-se no painel traseiro.

Opera em velocidades múltiplas de 64kbit/s (n x 64k, n de 1 a 32) na comunicação com o bridge, com estrutura de quadros de acordo com G.704.

Operação com relógio interno ou regenerado a partir do sinal G.703 recebido, com comutação automática para relógio interno na falta de sinal G.703.

Programação utilizando terminal ou micro do tipo PC através de uma porta de controle com interface V.24/V.28 (RS232), disponível em conector DB9 fêmea no painel frontal.

2.3.3. DM705 – Multiplexador E1 Cross Connect Modular

Figura 2.3: DM705 – Multiplexador E1

O DM705 é um multiplexador E1 totalmente modular com capacidade de até 8 placas de interface e facilidade de cross connect entre qualquer timeslot de qualquer porta, onde o agregado máximo é de 2Mbit/s por slot.

Possui as seguintes interfaces:

- G.703/G.704
- V.35/V.36/V.28
- Fibra óptica
- Ethernet 10BaseT
- G.703 64k codirecional
- Roteamento (PPP/Frame Relay)
- Interfaces de voz FXS/FXO

Pode trabalhar como um cross-connect com várias portas E1. Os timeslots de cada porta podem ser mapeados em qualquer outra porta e em timeslots diferentes. Com isto é possível consolidar em um único canal, tráfego de vários canais E1 sub-utilizados, por exemplo, (os dados de portas V.35, bridge Ethernet, G.703 64kbit/s, etc, também podem ser mapeados em qualquer time slot de qualquer porta).

Permite definir uma porta E1 (ótica ou elétrica) como sendo backup de outra porta E1 (também ótica ou elétrica). Havendo interrupção no link principal, os dados passam a ser transferidos através do link de backup.

2.3.4. DM706C – MiniMux – Multiplexador E1 Cross Connect

Figura 2.4: DM706 – Multiplexador E1

O DM706C é um multiplexador E1 com capacidade de 6 portas podendo adicionar mais portas através de uma placa de expansão. Constitui-se de uma unidade básica com 6 portas e alojamento para 1 placa de expansão. A placa de expansão pode adicionar uma ou mais portas.

A unidade básica possui:

- 4 portas com interface V.35 - V.36/V.11 - V.28
- Uma porta de roteamento entre as interfaces WAN (Frame Relay/PPP) e Ethernet (10BaseT)
- Uma porta com interface G.703/G.704 (E1).

Como placa de expansão, podem ser instaladas interfaces do tipo: E1 elétrica - G.703/G.704 (para conexão de PABX digital, por exemplo), E1 em fibra óptica, interface de modem HDSL ou placa de voz com 4 canais do tipo FXS a 2 fios.

Permite definir uma porta E1 como sendo backup de outra porta E1. Havendo interrupção no link principal, os dados passam a ser transferidos automaticamente através do link de backup. Uma das interfaces E1 pode ser elétrica ou óptica.

A gerência remota é via SNMP, tornando a gerência simples e integrada. O equipamento pode conectar se ao gerente SNMP, diretamente pela porta Ethernet e in-

band pela porta WAN. Pelo link de agregado pode gerenciar equipamentos remotos, assim como ser gerenciado pelo equipamento remoto quando o Gerente SNMP não estiver conectado diretamente nele, tornando extremamente compacta a estrutura necessária para gerência remota.

A gerência local é feita por uma interface V.24/V.28 (RS232) disponível em conector DB9 fêmea, utilizando um terminal ou emulador VT100. Pelo terminal local pode-se configurar, ver status e gerar testes no equipamento local e no equipamento remoto.

Permite upgrade remoto de software, fazendo um download via TFTP pela porta Ethernet ou WAN.

3. Informações Preliminares

Aqui serão abordadas informações pertinentes às atividades desenvolvidas no estágio, no intuito de proporcionar uma melhor compreensão das mesmas. Primeiramente será exposto o porquê da necessidade de se gerenciar um equipamento de telecomunicações, sendo que ao desenrolar do texto serão expostas as tecnologias e as idéias que estão por trás do que é feito na prática.

3.1. Gerenciando equipamentos

Equipamentos de telecomunicações são cada vez mais complexos e mais numerosos nos dias de hoje. No que diz respeito ao fato de serem cada vez mais complexos, pode-se imaginar que suas funcionalidades estão sendo aumentadas, e o mesmo vale para as taxas de transmissão. É claro que não entraremos no mérito de quantos padrões de comunicação existem hoje em dia e como é possível conviver com esta "torre de babel".

Quanto ao fato de serem cada vez mais numerosos, podemos pensar em uma sala cheia de equipamentos, interligados uns com os outros, servindo a uma operadora de telefonia, por exemplo. Em geral, eles precisam passar por uma etapa de configuração antes de serem postos em funcionamento pleno. Além disso, seria muito interessante se fosse possível consultar parâmetros dos equipamentos, para saber se está tudo em ordem. Mais interessante ainda seria fazê-lo de uma forma automatizada, de maneira remota.

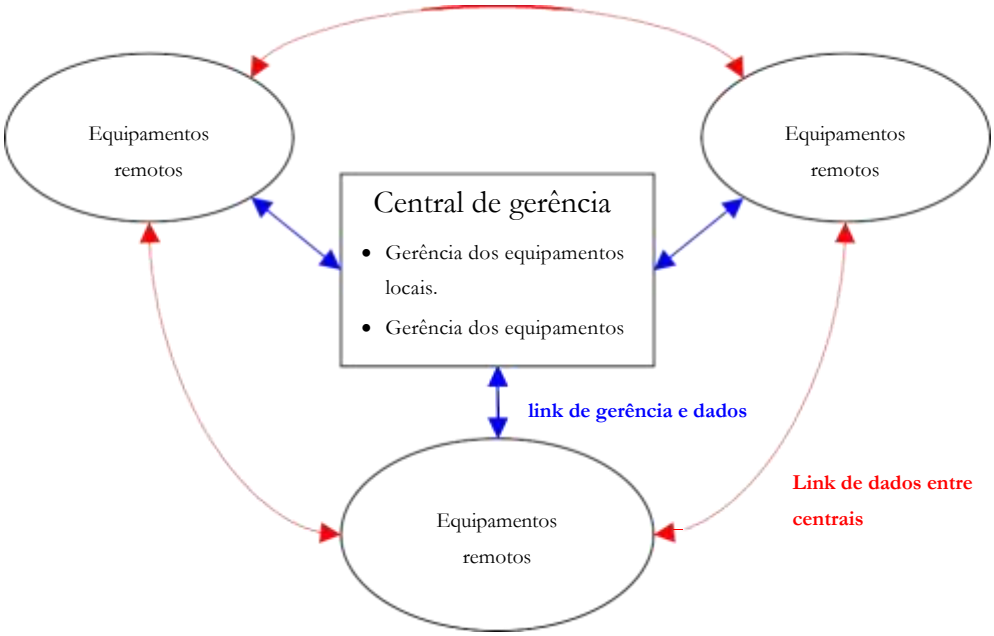

Figura 3.1: Idéia básica de gerência de equipamentos

É neste contexto que entra em cena a parte de gerência de equipamentos. Em suma, o fato de se gerenciar um equipamento consiste na supervisão do mesmo, para que se possa, local ou remotamente, obter informações de seu funcionamento, efetuar a configuração de seus parâmetros, verificar falhas, desempenho, etc.

3.2. Conceitos Básicos de Gerenciamento

Existem alguns conceitos básicos que são comuns a qualquer sistema de gerenciamento, que serão expostos aqui:

a) Objetos gerenciados: São elementos de interesse na rede, que podem ser dispositivos lógicos (software) ou físicos (hardware). Em suma, é qualquer objeto passível de ser monitorado numa rede para verificar certos parâmetros de funcionamento.

b) Agente: Elemento responsável pela coleta de informações dos objetos gerenciados, enviando-as ao gerente e executando comandos determinados por ele, baseados em tais informações.

c) Gerente: É quem concentra as informações passadas pelo agente e envia comandos de gerenciamento a este para serem executados sobre os objetos gerenciados.

d) MIB (Management Information Base): É a estrutura de dados básica de um sistema de gerenciamento. Consiste basicamente numa tabela onde se encontram os dados relevantes ao gerenciamento de um sistema. Seu formato é definido pela SMI (Structure of Management Information), que é descrita na linguagem ASN.1 (Abstract Syntax Notation One).

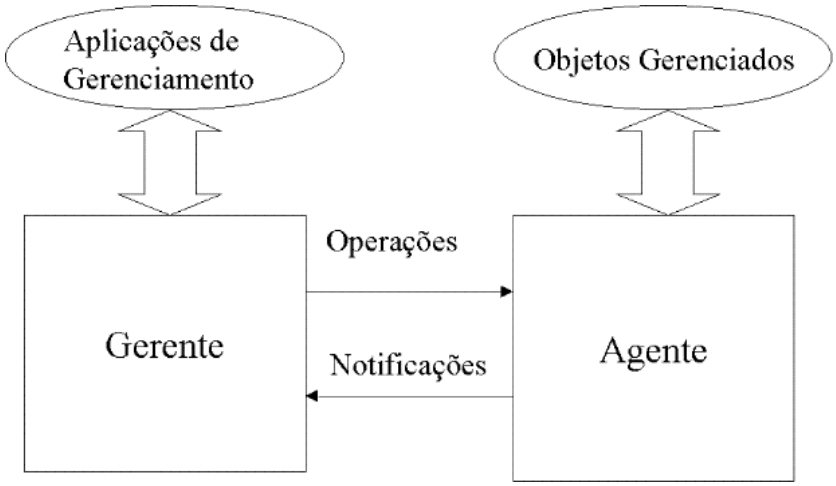

Figura 3.2- Cenário típico de um sistema de gerenciamento

3.3. Estabelecendo padrões

Uma vez estabelecido o propósito da gerência de equipamentos, nos vemos diante da necessidade de estabelecer uma forma de como "conversar" com o equipamento. Em outras palavras: queremos saber como será feita a comunicação entre o software gerente e o equipamento. Aqui entra em cena o protocolo SNMP (Simple Network Management Protocol).

Como no esquema de gerenciamento OSI, os processos que implementam as funções de gerenciamento Internet atuam como agentes ou gerentes. Os agentes coletam junto aos objetos gerenciados as informações recolhidas pelos clientes, com o objetivo de detectar a presença de falhas no funcionamento dos componentes da rede (hosts, gateways, processos executando os protocolos de comunicação, etc...), para que possam ser tomadas providencias no sentido de contornar os problemas que ocorrem como conseqüência das falhas. Um objeto gerenciado representa um recurso que pode ser um sistema hospedeiro (estação de trabalho, servidor de terminais, etc...), um gateway ou um equipamento de transmissão (modem, pontes, concentradores, etc...). Cada objeto gerenciado é visto como uma coleção de variáveis cujo valor pode ser lido ou alterado. O gerente envia comandos aos agentes, solicitando uma leitura no valor das variáveis dos objetos gerenciados (get e response), ou modificando seu valor (set). A modificação do valor de uma variável pode ser usada para disparar indiretamente a execução de operações nos recursos associados aos objetos gerenciados (por exemplo, uma mudança na configuração). Na troca de informações entre o gerente e o agente, são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede. A troca de mensagens entre o gerente e o agente é definida pelo protocolo SNMP.

O SNMP define o formato e a ordem que deve ser seguida no intercâmbio de informações de gerenciamento. As informações sobre os objetos gerenciados são armazenadas na MIB (Management Information Base), que contém informações sobre o funcionamento dos hosts, dos gateways, e dos processos que executam os protocolos de comunicação (IP, TCP, ARP, ...). O funcionamento do SNMP baseia-se na troca de operações que permitem que o gerente solicite que o agente lhe informe, ou modifique, o valor de uma variável de um objeto na MIB. O SNMP define também uma operação

(trap), que permite que um agente informe ao gerente a ocorrência de um evento específico.

3.3.1. SNMP v.1

O protocolo SNMP foi inicialmente idealizado em 1989. Sua arquitetura é baseada no modelo Internet para redes, e sua localização é equivalente à da camada aplicação, no modelo OSI. A camada inferior na pilha de protocolos é a UDP (User Datagram Protocol), que é protocolo de transporte padrão da Internet com serviço do tipo datagrama.

O sistema de gerenciamento de rede da arquitetura Internet TCP/IP opera na camada de aplicação e baseia-se no protocolo SNMP. Os padrões que definem a estrutura de gerenciamento de redes Internet são descritos nos documentos RFC-1155 (Structure of Management Information), RFC-1156 (Management Information Base) e RFC-1157 (Simple Network Management Protocol). Uma descrição mais profunda do SNMP vem nos RFC-2570 e 2571, sendo que este último se refere à sua arquitetura. A pilha de protocolos do SNMP é mostrada a seguir:

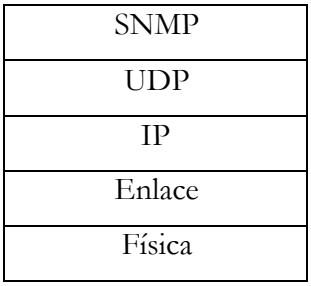

Figura 3.3- Pilha de Protocolos do SNMP

Sua operação é bastante simples, sendo as seguintes mensagens (primitivas de serviço) utilizadas por ele:

a) Get (Request, Next Request, Response): Trata-se do pedido do gerente para ler os dados de gerenciamento da MIB do agente. A Get Request faz o pedido inicial pelo gerente, a Response envia os dados para o gerente e a Get Next Request pede outro trecho da tabela seqüencialmente.

b) Set (Request): Serve para alteração de dados da MIB. O gerente recebe um pedido de Set Request para alterar determinado dado.

c) Trap: É um informe dado ao gerente de que algo de anormal está acontecendo no sistema, tendo o funcionamento semelhante a um alarme. Tipicamente é enviado quando ocorre alguma mudança de estado de algum parâmetro do equipamento (estado do link, estado da fonte de alimentação, etc.)

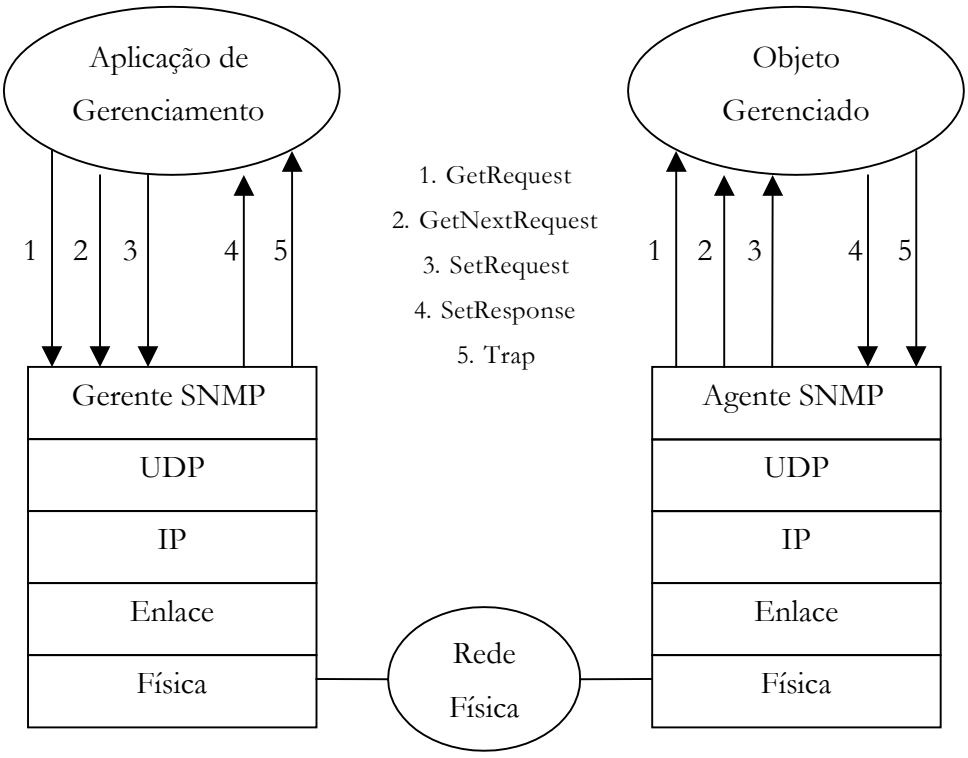

Figura 3.4- Modelo de Serviço do SNMPv.1

Apesar disto, alguns problemas aparecem derivados da simplicidade de implementação da versão 1 do protocolo SNMP (SNMPv.1). Em primeiro lugar, o Trap SNMP não é confirmado. Em virtude disto, o agente até pode enviar a mensagem de Trap ao gerente, mas não saberá se ele a recebeu, podendo esta mensagem ser perdida na rede, e a anomalia presente eventualmente nem ser corrigida.

Outro problema é a limitação da rede a ser gerenciada. Isto ocorre em virtude do "polling" (operação onde o gerente, de tempos em tempos, consulta os agentes para coletar informações). Além disto, a autenticação do protocolo é deficiente, uma vez que ela é baseada nas chamadas comunidades ("community based"). Neste tipo de

abordagem, alguns dados do protocolo circulantes na rede podem ser lidos por pessoas estranhas ao sistema em questão.

Finalizando, podemos citar também o fato de que o SNMPv.1 não suporta a busca em tabelas, que ele permite a existência de apenas um gerente por sistema e que não se pode criar ou excluir objetos dentro do sistema, com este protocolo.

3.2.2. SNMP v.2

A versão 2 do SNMP (SNMPv.2, 1993) busca corrigir algumas deficiências da versão 1. Ela basicamente surgiu da evolução do SNMPv.1 e do RMON. Utiliza a SMI2, que permite a presença de novos tipos ASN.1. Além disto, permite a criação e exclusão de objetos, juntamente com a comunicação entre gerentes através da chamada Manager to Manager MIB.

Houve também a inclusão de mais dois tipos de mensagens nesta versão:

a) GetBulkRequest: Pedido do gerente para leitura de trechos específicos da MIB.

b) InformRequest/Response: Representa a implementação do Trap confirmado. O InformRequest é o Trap propriamente dito e o InformResponse, a confirmação dada pelo gerente.

A segurança também foi melhor implementada. Nas versões denominadas SNMPv2u e SNMPv2*, existe a segurança feita por usuário (user-based), o que só permite a realização de operações por usuários específicos, e não qualquer um. Na prática, a versão utilizada para o SNMP é v.2c, sendo que as questões de segurança ficaram a encargo da versão 3.

3.2.3. SNMP v.3

A versão 3 do SNMP (SNMPv.3, 1997) trouxe como principais vantagens aspectos ligados à segurança. Esta segurança busca evitar a alteração das mensagens enviadas. Além disto, barra-se o acesso a elementos estranhos à execução de operações

de controle, que são realizadas através da primitiva SetRequest. Evita-se também a leitura das mensagens por parte de estranhos, além de se garantir ao gerente o direito de alteração da senha dos agentes.

A segurança é conseguida através da introdução de mecanismos de criptografia com o DES (Data Encryption Standard) e de algoritmos de autenticação que podem ser tanto o MD5 quanto o SHA (Secure Hash Algorithm).

3.2.4. MIB

A MIB (Management Information Base) é a forma de estrutura de dados do SNMP. São basicamente tabelas com dados de gerenciamento, cujo formato é especificado pela SMI (Structure of Management Information). Sua descrição é efetuada em linguagem ASN.1 (Abstract Syntax Notation One).

Uma vez que um equipamento tenha características específicas, é desenvolvida uma MIB para este. Diz-se então que um certo equipamento pode responder a uma MIB ou à um conjunto de MIB's. Uma MIB é uma coleção de objetos gerenciáveis. Abrindo-se uma MIB, ela lembra uma estrutura de diretórios, onde pode-se partir de um diretório raiz com alguns diretórios e chegar até o fim de um diretório específico. A grande diferença talvez esteja no modo de funcionamento. É possível dar nomes aos objetos, porém o que realmente faz sentido é o número que lhes é atribuído. Cada objeto é chamado de OID (Objeta Identifier), que nada mais é que um identificador único para cada parâmetro do equipamento. Sendo assim, cada "diretório" ou "pasta" tem um número associado, e o caminho até se chegar ao objeto final nada mais é que uma seqüência de números. E é esta seqüência que é passada pela rede ao agente SNMP.

É possível então, fazer uma organização com tabelas especificas para cada grupo de características do equipamento. O fabricante então estuda a maneira como deve ser organizada a MIB de cada equipamento seu.

Para que faça sentido se poder gerenciar equipamentos de mais de um fabricante na mesma rede, existe um órgão regulamentador que coordena a distribuição de números únicos para os fabricantes de equipamentos de telecomunicações. Normalmente existe um caminho padrão até chegarmos à informação pertinente a fabricantes de equipamentos. Isto significa que existem trechos da MIB que são padrões, a exemplo do trecho da MIB-II. São objetos que devem estar implementados no agente e que fornecem informações gerais do funcionamento da rede.

4. Atividades do Estágio

4.1. Desenvolvimento do Agente SNMP

4.1.1. Finalidade do Projeto

Hoje em dia, é praticamente regra se ter um meio de como gerenciar um equipamento de telecomunicações. A função do agente SNMP é justamente esta: possibilitar que o equipamento seja passível de ser gerenciado. A finalidade do projeto se apóia nesta idéia, mas tem um objetivo mais amplo, pois visa o desenvolvimento de um agente flexível, que seja robusto e acompanhe as novas tecnologias do mundo das telecomunicações.

4.1.2. Requisitos

Os requisitos foram estabelecidos pelo setor de Pesquisa e Desenvolvimento da empresa. Os itens relevantes em questão são:

- Desenvolvimento do software em linguagem C
- Utilização do sistema operacional Linux
- Estudo da Implementação da MIB no agente
- Geração de traps
- Portabilidade

4.1.3. Hardware utilizado

Do ponto de vista da interface entre o sistema operacional e o agente SNMP, não há uma dependência direta do hardware. Já o sistema operacional em si tem que ser compilado e completamente preparado para rodar no hardware, pois depende diretamente dele. Ele depende do tipo de processador que irá usar, como são implementadas as instruções, do tipo de memória, do barramento, etc.

Do ponto de vista do agente SNMP, a parte de hardware específica de que depende se diz respeito às funcionalidades do equipamento em si, quando olhado como um equipamento de telecomunicações. O agente SNMP tem que, de alguma forma, "conversar" com estas partes do equipamento e obter as informações necessárias. O hardware utilizado, então, não será citado por não entrar no mérito da questão do SNMP e apenas partes relevantes serão expostas quando necessário.

A titulo de testes do agente em desenvolvimento, foi utilizado um DM706, pois ele já é um equipamento de telecomunicações funcional, de onde podem ser obtidas respostas reais. O DM706 possui uma porta Ethernet 10BaseT, por onde foi feita a comunicação entre o agente SNMP e o gerente, através do protocolo SNMP encapsulado em TCP/IP.

O DM706 possui uma interface serial (padrão RS232) que foi utilizada para visualizar a saída de vídeo. Isto foi de vital importância para depurar o agente, visto que as mensagens de depuração podiam ser visualizadas através de um terminal de emulação VT-100 em um PC. Além disso, é possível interagir com o sistema operacional e com o próprio agente através do teclado.

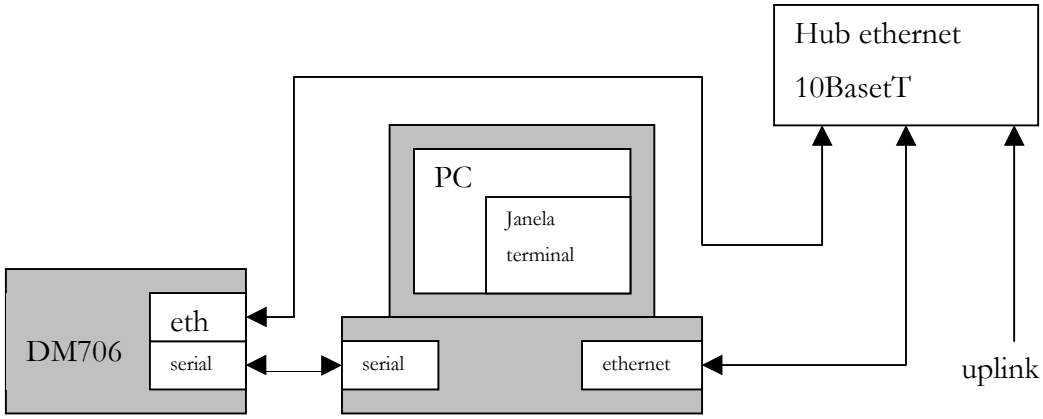

Figura 4.1: Ambiente de Validação

4.1.4. Protocolo SNMP

Para se poder efetuar a implementação do protocolo no sistema, suas características foram analisadas para um melhor entendimento do problema.

A versão escolhida foi a versão 2. Isto se deve ao fato de que ela possui um nível um pouco maior de segurança nas transações, principalmente no que diz respeito à primitiva de Trap. No SNMP v.1 não havia confirmação para o Trap enviado, sendo que este poderia nem chegar ao destino sem que o agente pudesse tomar conhecimento. Na versão 2 isto pode ser contornado, visto que o gerente deve enviar uma confirmação de recebimento ao agente, quando ele receber o Trap. Além disso, o SNMP v.2 permite o gerenciamento de uma rede descentralizada, pois suporta mais de uma estação gerente (cooperação gerente-gerente). Permite também a transferência de maiores porções de dados com mais facilidade.

4.1.5. Estrutura do Software

A idéia básica para o software a ser implementado é dada na figura 4.2:

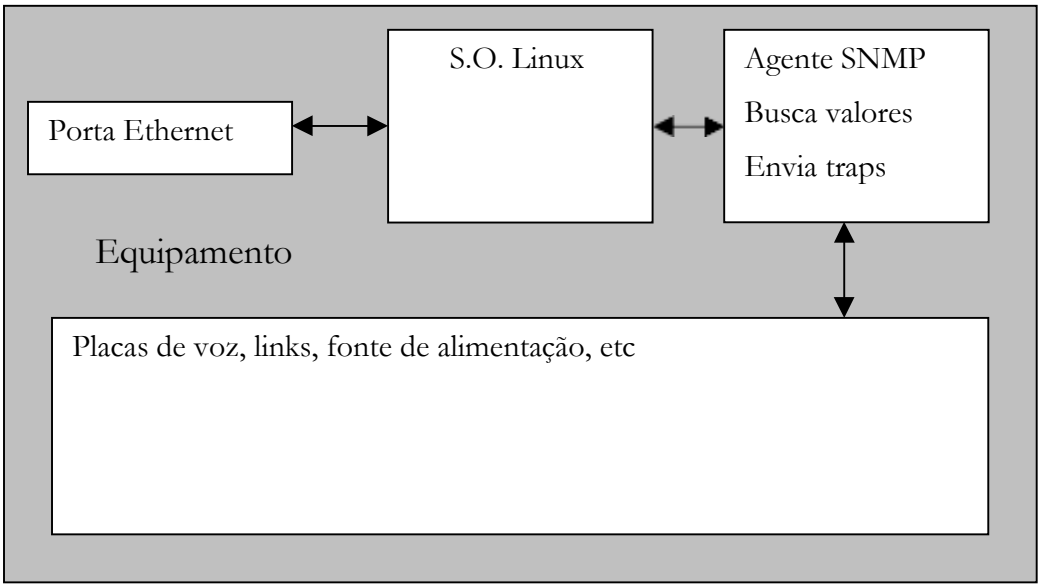

Figura 4.2: Estrutura básica de funcionamento do software/equipamento

De fato, o sistema operacional é o responsável pelo gerenciamento das portas de comunicação, a exemplo da porta de Ethernet. No caso, é o Linux quem deve gerenciar o processo de recebimento do pacote de rede e encaminhá-lo ao processo

responsável. Conforme o modelo OSI, o pacote SNMP vem "encapsulado" em um pacote IP, pois as duas camadas abaixo do pacote são a camada física e enlace (responsáveis pelo sincronismo e transporte). Assim sendo, só é necessário fazer a interface com a camada IP e obter o pacote SNMP.

PDU type	Request-id	0	0	Variable-bindings

(a) GetRequest-PDU, GetNextRequest-PDU, SetRequest-PDU, SNMPv2-Trap-PDU, InformRequest-PDU

PDU type	Request-id	Error-status	Error-index	Variable-bindings

(b) Response-PDU

PDU type	Request-id	Non-repeaters	Max-repetitions	Variable-bindings

(c) GetBulkRequest-PDU

Name1	Value1	Name2	Value2	...	Name*n*	Value*n*

(d) Variable-bindings

Figura 4.3: PDU's do pacote SNMP v.2

Dentro do pacote SNMP podemos reconhecer a estrutura PDU (protocol data unit) mostrada na figura 4.3 (SNMP v.2), que nada mais é que a informação do pacote SNMP em si. Se, por exemplo, um pacote do tipo GetRequest (a) for enviado por um gerente, este será recebido pelo agente que tem a função de entender a formatação do PDU do protocolo, e tomar a ação devida. Neste contexto existe um projeto conhecido, cujo nome é Net-SNMP, que é um pacote de software de caráter gratuito e com várias ferramentas relacionadas ao SNMP.

A estrutura modular utilizada tem como propósito possibilitar o uso do agente SNMP em diversos equipamentos. Deste modo, apenas pequenas partes do programa necessitarão ser alteradas e adaptadas a diferentes hardwares. A parte do software que é responsável pela decodificação do pacote é independente do hardware. Já o bloco que retira as informações específicas do equipamento depende diretamente dele. As funções deste bloco estão associadas à maneira de como a informação deve ser acessada, e como será o formato recebido do parâmetro consultado. Este bloco também pode, em alguns casos, mudar o valor do parâmetro solicitado, de acordo com o que foi pedido através de um pacote SetRequest.

4.1.6. Ferramentas utilizadas

4.1.6.1. O Net-SNMP

O Net-SNMP foi objeto de estudo e de grande utilidade no desenvolvimento do agente SNMP. O Net-SNMP possui várias ferramentas úteis para desenvolvimento e depuração de aplicativos relacionados à parte do SNMP.

Munido de um agente genérico, o Net-SNMP já oferece uma maneira amigável para se desmontar o pacote SNMP proveniente da rede, ou montar um para ser enviado ao sistema de gerência. Com ele é possível abrir a porta de comunicação SNMP, deixando a cargo dele a recepção ou envio do pacote SNMP, o qual será entregue ou pego de outra parte do software, personalizável pelo usuário.

As partes mais úteis do Net-SNMP foram sem dúvida o conjunto de aplicativos para depuração. São programas para envio de mensagens (SetRequest, GetRequest, etc), envio de traps, monitoração e outras, que são executados pela linha de comando. Há também um software MIB-browser que trabalha com as bibliotecas do Net-SNMP, e tem interface gráfica.

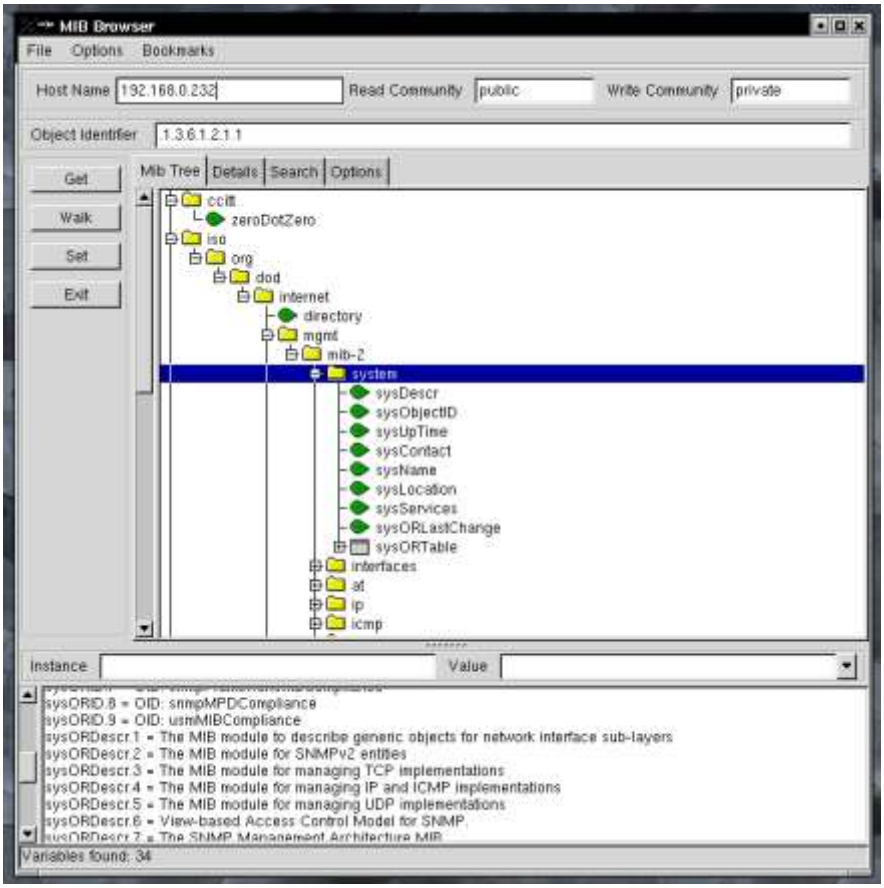

Figura 4.4: MIB-browser e visão de parte da MIB-II com as pastas.

4.1.6.2. DDD Debugger

Para se efetuar a depuração em tempo de execução do software, foi utilizado o DDD (Data Display Debugger). Ele é um aplicativo incorporado ao Linux que permite execução passo a passo do programa de maneira remota. Assim sendo, é possível rodar o programa em uma máquina e observar o seu comportamento de outra.

Foi utilizado o link Ethernet para efetuar a interligação entre o DDD e o processo remoto (no caso o agente SNMP). O DDD então roda no PC e se comunica com o processo remoto via rede, podendo parar sua execução, ler as variáveis da memória, etc. Enfim, é como se fôssemos depurar o programa localmente. A vantagem de se fazer este tipo de coisa é que se tem o funcionamento real do programa, em termos de velocidade de processamento e de rede, além da capacidade de memória do equipamento que também é restrita.

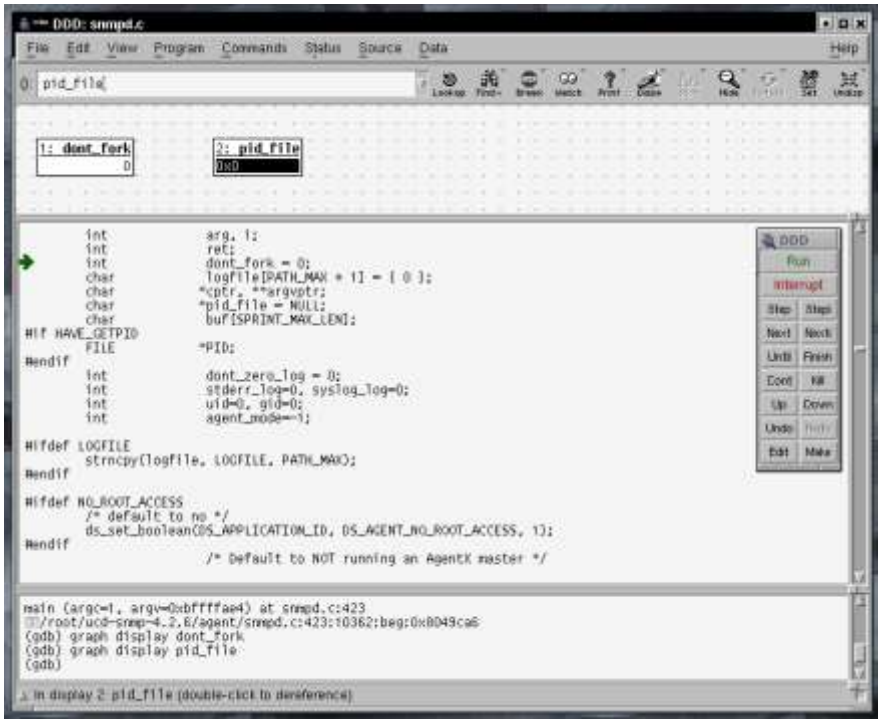

Figura 4.5: DDD executando o programa remotamente.

4.1.7. Organizando a Informação

Uma vez estabelecido o padrão de como o pacote SNMP seria montado e desmontado, faz-se necessário o estudo da MIB, pois é ela que estabelece a forma de como acessar as informações do equipamento, sob a forma de objetos.

Uma vez recebido um pacote de GetResponse, este conterá um OID. Este OID faz referência a algum tipo de informação do equipamento. Embora pareça simples, um equipamento possui uma quantidade relativamente grande de OID's, o que leva o agente a ter que verificar a validade do OID, descobrir qual informação é pertinente a ele e mandar o pacote de resposta para o gerente. Uma pergunta do tipo GetNextResponse é mais complexa ainda, pois o OID proveniente da pergunta pode não ser válido, sendo que o agente deverá então descobrir quem é o próximo OID para prosseguir com o processo. A maneira de como poderia ser guardada a informação da MIB e como fazer para procurá-la de forma eficiente também foram focos do estudo, visto que afetam sensivelmente a performance do produto.

Há um compromisso entre o tamanho utilizado pela informação guardada e a velocidade com que se consegue encontrar o valor solicitado. Diferente de um PC, não há uma infinidade de memória RAM no equipamento, e seu processador não roda a 1GHz, o que significa que o código de busca deve ser extremamente eficiente e que se deve tentar utilizar o mínimo de recursos do sistema, tanto dinamicamente (como alocação de memória) quanto estaticamente (código de programa).

4.1.8. Traps

Um outro foco de estudo foi de como seria o processo de envio de traps. De um modo geral, os traps são enviados quando ocorre alguma mudança no equipamento, com o intuito de avisar a gerência que algo aconteceu. A exemplo disto podemos citar a queda de algum link, ou um problema na fonte de alimentação.

Quando um estado de algum objeto muda, esta mudança deve ser detectada e um trap contendo a identificação de quem mudou deve ser enviado. Mais especificamente, é gerado um trap com um certo número de identificação, e este trap conterá as informações pertinentes ao objeto em questão. Se, no exemplo acima, o problema na fonte de alimentação correspondesse ao trap número 5125, um trap com

este número seria enviado, e a informação contida no trap poderia ser um número que indicaria que a fonte está com problemas ou que voltou a funcionar corretamente. Quem tem a tarefa de interpretar a informação de modo correto é o gerente.

Esta parte de traps também foi implementada no agente, sendo que, tratando-se do uso da versão 2 do protocolo, utilizou-se trap's com confirmação de recebimento. O papel do agente aqui é descobrir qual é o OID do objeto que mudou de estado, e mandar o trap ao gerente com esta informação. Estes também foram objetos de estudo, visto que o agente deve tomar conhecimento o mais rápido possível da alteração do parâmetro, a fim de enviá-lo à gerência.

4.1.0. Testes e funcionamento

O funcionamento do software pode ser acompanhado pelo terminal. Na figura 4.6 estão mostradas algumas mensagens de depuração do programa, quando pacotes de GetNextResponse são enviados pelo aplicativo de gerência para a rede. Estes pacotes são recebidos pelo DM706 e decodificados conforme o exposto até aqui.

As mensagens podem servir para se verificar se o pacote está sendo interpretado corretamente, e se a mensagem de resposta está coerente com o valor do objeto solicitado.

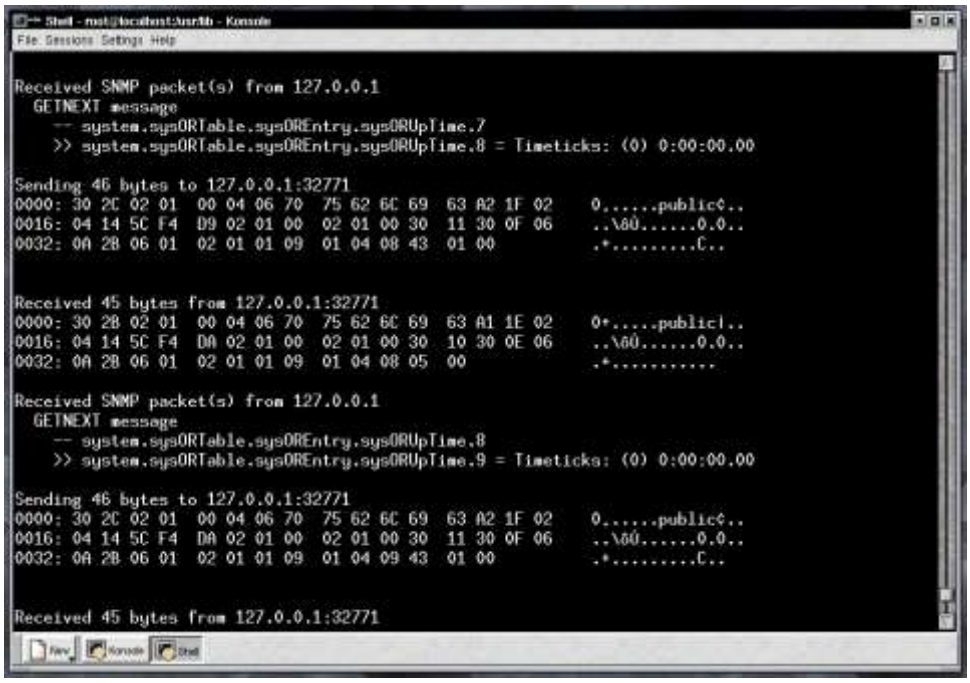

Figura 4.6: Terminal mostrando mensagens de depuração.

Na operação de GetNextResponse, o agente SNMP receberá o pacote contendo um OID. Este OID deverá ser pesquisado na MIB do agente que verificará qual é o próximo OID a partir do que foi informado. O valor do objeto correspondente a este próximo OID é o que será respondido à gerência. Este processo de procura gasta tempo e é um dos motivos da "lentidão" no protocolo.

5. Conclusão

A vivência da prática profissional é fundamental para a formação de todo o indivíduo, independente da área ou profissão em que for atuar. Portanto, servindo de "interface" entre o meio acadêmico e o mercado de trabalho, a disciplina de Estágio Supervisionado vem complementar a formação acadêmica do curso, ampliando os horizontes do aluno, preparando-o para a realidade empresarial e mercadológica. A obrigatoriedade de um estágio se faz necessária a medida em que força o contato do aluno com o "mundo real", tendo-se em vista que uma grande parte dos alunos do curso não possuem experiências profissionais extra-acadêmicas.

Tendo como área de estágio o ramo de telecomunicações, no decorrer do período percebeu-se que as cadeiras de fim de curso na Universidade Federal do Rio Grande do Sul não estão muito voltadas para este ramo, embora ele esteja crescendo cada vez mais.

Embora se saiba que o corpo docente tem se esforçado para manter a nossa Escola em um bom nível, são relevantes alguns comentários. Tendo em vista que o estágio é de extrema importância para a formação profissional do aluno, seria melhor se as disciplinas de fim de curso fossem ministradas à noite. Fica um tanto complicado conciliar as aulas diurnas com o estágio. Outro comentário fica em relação à escolha dos professores que ministrarão as disciplinas. Muitas vezes parece que o que menos se levou em conta foi a área de atuação do professor, ficando assim um profissional formado e especializado em um tema, exercendo uma aula muito diferente do que seria se outro professor da área fosse aplicar na prática.

Em relação ao conteúdo abordado no curso, uma sugestão seria a da inclusão de alguma disciplina de lógica de programação mais específica e voltada para a Engenharia, de preferência com base na linguagem C, que é cada vez mais utilizada para a programação de microprocessadores.

Finalizando, o estágio proporcionou a oportunidade da aplicação dos conhecimentos teóricos, oportunidade para obter uma série de informações novas, oportunidade de relacionamento com profissionais da área e também de outras áreas, e conseqüentemente a oportunidade para um acréscimo de experiência em nível pessoal, profissional e social.

Baseado nestes fatos considera-se que os conhecimentos e experiência agregados no período de estágio satisfizeram completamente as expectativas.

6. Referências Bibliográficas

Stallings, William. SNMP, SNMPv2, SNMPv3, RMON 1 and 2. Third Edition. Addison Wesley, 1999.

Gerenciamento de Redes: Uma Abordagem de Sistemas Abertos; BRISA – Sociedade Brasileira para Interconexão de Sistemas Abertos. Makron Books. 1993.

SNMP & MIB RFC's, www.hio.hen.nl/rfc/snmp/

Gerenciamento de Redes, www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html

Net-SNMP, www.net-snmp.org