UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
MESTRADO EM ENGENHARIA ELÉTRICA E COMPUTAÇÃO

Proposta de um Sistema de Gerência de Redes PLC Utilizando SNMPv3

Diogo Nunes de Oliveira

Orientador: Prof. Dr. Flávio Henrique Teles Vieira

Goiânia
2009

DIOGO NUNES DE OLIVEIRA

Proposta de um Sistema de Gerência de Redes PLC Utilizando SNMPv3

Dissertação apresentada ao programa de Mestrado em Engenharia Elétrica e Computação da Universidade Federal de Goiás, para obtenção do título de Mestre em Engenharia Elétrica e Computação.
Área de Concentração: Telecomunicações.
Orientador: Prof. Dr. Flávio Henrique Teles Vieira.

Goiânia
2009

Universidade Federal de Goiás
Escola de Engenharia Elétrica e Computação
Mestrado em Engenharia Elétrica e Computação

FOLHA DE APROVAÇÃO

"Proposta de um Sistema de Gerência de Redes PLC Utilizando SNMPv3"

DIOGO NUNES DE OLIVEIRA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Dr. Flávio Henrique Teles Vieira, Orientador - EEEC/UFG

Prof. Dr. Getúlio Antero de Deus Júnior - EEEC/UFG

Prof. Dr. Sérgio Granato Araújo - EEEC/UFG

Prof. Dr. Pedro José Abrão - IFG

Goiânia, 01 de julho de 2009

Dedico esta dissertação à minha esposa,
que tem me apoiado em todos os momentos
de dificuldade, e também à meu pai,
que me ajudou a traçar metas na busca
pela qualificação.

Agradecimentos

Dedico meus sinceros agradecimentos

– à minha esposa Elisa Gomes Loiola de Oliveira, pelo constante apoio e compreensão;

– à meu pai, Sinoeste Cardoso de Oliveira, pelo apoio e orientação;

– ao professor doutor Flávio Henrique Teles Vieira, pelo trabalho de orientação e esclarecimento no processo de criação desta dissertação;

– ao professor doutor Getúlio Antero de Deus Júnior, pelo espírito de liderança e incentivo constante durante o processo de co-orientação;

– ao professor doutor Sérgio Granato Araújo, por coordenar, de forma exemplar, o projeto de pesquisa e desenvolvimento envolvendo tecnologia PLC, firmado entre CELG e UFG;

– à CELG, por permitir a utilização da rede PLC e dos equipamentos dessa tecnologia, o que viabilizou essa dissertação;

– à todos os envolvidos no Projeto de Pesquisa e Desenvolvimento entre UFG e CELG envolvendo tecnologia PLC;

Resumo

TECNOLOGIAS de acesso para transmissão de dados, como xDSL, *Wi-fi* e *cable modem* são amplamente utilizadas por permitirem altas taxas de transmissão a baixo custo. Dentre essas tecnologias, a *Power Line Communications*, conhecida como PLC, é uma solução promissora.

A tecnologia PLC permite a transmissão de dados através da rede elétrica, rede essa que apresenta elevada capilaridade, pois está presente em 99% das residências. Por ser uma tecnologia que já tem grande parte de sua estrutura pronta, as concessionárias de energia elétrica começam a investir nessa solução, com o intuito de deixar de ser apenas uma concessionária de energia, passando a ser também uma operadora de telecomunicações.

Para ter controle sobre uma tecnologia é necessário utilizar técnicas de gerenciamento que permitam extrair o máximo de informações a respeito do funcionamento e estado da tecnologia e dos equipamentos envolvidos, e como resultado, proporcionar confiabilidade nessa tecnologia.

Este trabalho tem como um de seus objetivos apresentar a solução de gerenciamento desenvolvida para redes PLC. Esta solução difere de sistemas de gerência de outras tecnologias de transmissão de dados devido ao meio utilizado para a transmissão e por ser uma tecnologia ainda pouco utilizada. O *software* de gerenciamento utilizado como base do sistema de gerência que fora implementado é um *software* de código livre e gratuito. Para o desenvolvimento da ferramenta de gerência de redes PLC foi adotado o conceito do *software* livre, sendo assim, todos os *softwares* utilizados são livres e gratuitos.

O outro objetivo deste trabalho é apresentar a proposta e implementação de um sistema embarcado baseado em microcontrolador para realizar a conversão de versões do protocolo SNMP, utilizado no gerenciamento de redes TCP/IP. A final-

idade deste conversor é implementar segurança no gerenciamento de redes PLC, visto que os ativos PLC suportam apenas o protocolo SNMP em sua versão 2c, versão esta que é bastante falha se tratando de segurança dos dados. Como o SNMPv3 suporta algoritmos de autenticação e criptografia, o equipamento conversor desenvolvido é capaz de prover segurança, devido à sua capacidade de codificar um pacote SNMPv2c em um pacote SNMPv3, e vice-versa.

Abstract

ACCESS technologies for data transmission, such as xDSL, Wi-fi and cable modem are widely used because they support high data transmission rates at low cost. Among these technologies, Power Line Communications, known as PLC, is a promising solution.

PLC technology transmits data over power network, which presents high capilarity, due to the fact that it is present in 99% of residences. Since most of its structure already exists, power supply concessionaries started investing in this solution to stop being only a power supply concessionary and to be also a telecommunication company.

In order to obtain control over a technology it is necessary to use management techniques that permits the maximum extraction of information from technology and involved devices.

One of the goals of this work is to present the management solution developed to PLC networks. This solution differs from network management solutions used on other data transmission technologies due to the transmission media utilized. The management software used as base of the management system implemented is a free and no cost software. The concept of free code was adopted to the solutions implemented to the management system.

The other goal of this work is to present the proposal and implementation of an embedded system based on PIC microcontroller that performs conversion of versions of SNMP protocol, which is the default management protcol in TCP/IP based networks. This converter device brings security to PLC networks management, since PLC devices only support version 2c of SNMP protocol, which is faulty regarding security. Since SNMPv3 supports authentication and privacy algorithms, the designed converter device is capable of providing security, due to its

capacity of coding a SNMPv2c packet into a SNMPv3 packet, and vice-versa.

Sumário

Lista de Abreviaturas

ADSL - *Assymmetric Digital Subscriber Line* (Linha Digital Assimétrica do Assinante),

AES - *Advanced Encryption Standard* (Padrão de Criptografia Avançado),

ARQ - *Automatic Repeat Request* (Requisição de Repetição Automática),

BPL - *Broadband over Power Lines* (Banda Larga sobre Rede Elétrica),

CBC - *Cipher Block Chaining* (Corrente de Blocos Cifrados),

CGI - *Common Gateway Interface* (Interface de Ligação Comum),

CMIP - *Common Management Information Protocol* (Protocol de Informação de Gerenciamento Comum),

CPE - *Customer Premises Equipment* (Equipamento do Consumidor),

CRC - *Cyclical Redudance Checking* (Verificação de Redundância Cíclica),

DES - *Data Encryption Standard* (Padrão de Criptografia de Dados),

DHCP - *Dynamic Host Control Protocol* (Protocolo de Controle de Host Dinâmico),

DSL - *Digital Subscriber Line* (Linha Digital do Assinante),

ETSI - *European Telecommunication Standards Institute* (Instituto de Padrões de Telecomunicações da Europa),

FDM - *Frequency Division Multiplex* (Multiplexação por Divisão de Frequência),

FEC - *Forward Error Correction* (Correção de Erros),

GMSK - *Gaussian Minimum Shift Keying* (Deslocamento de Chave Mínima Gaussiana),

GPL - *General Public License* (Licença Pública Geral),

HTTP - *HyperText Transer Protocol* (Protocolo de Transferência de Hipertexto),

ICMP - *Internet Control Message Protocol* (Protocolo de Controle de Internet),

ICSP - *In-Circuit Serial Programming* (Programação Serial de Circuito),

IE - *Intermediate Equipment* (Equipamento Intermediário),

IP - *Internet Protocol* (Protocolo de Internet),

ISO - *International Standards Organization* (Organização Internacional de Padrões),

LCD - *Liquid Crystal Display* (Tela de Cristal Líquido),

MAC - *Media Access Control* (Controle de Acesso ao Meio),

MCM - *MultiCarrier Modulation* (Modulação de Multi Portadoras),

MIB - *Management Information Base* (Base de Informações de Gerenciamento),

NIST - *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia),

NMS - *Network Management System* (Sistema de Gerenciamento de Rede),

OFDM - *Orthogonal Frequency Division Multiplex* (Multiplexação por Divisão de Frequência Ortogonal),

OPERA - *Open PLC European Research Alliance* (Aliança Européia de Pesquisa de Tecnologi PLC Aberta),

OPLAT - Ondas Portadoras em Linhas de Alta Tensão,

OSI - *Open Systems Interconnection* (Interconexão de Sistemas Abertos),

PC - *Personal Computer* (Computador Pessoal),

PDU - *Protocol Data Unit* (Unidade de Dados de Protocolo),

PLC - *Power Line Communications* (Comunicação pela Rede de Energia),

PLTF - *PowerLine Telecommunications Forum* (Fórum de Telecomunicações sobre Rede Elétrica),

PNC - *Power Network Communications* (Comunicações sobre Rede de Energia),

QAM - *Quadrature Amplitude Modulation* (Modulação por Amplitude em Quadratura),

QPSK - *Quadrature Phase Shift Keying* (Deslocamento de Chave em Quadratura),

RADIUS - *Remote Authentication Dial In User Service* (Serviço de Autenticação Remota por Demanda de Usuário),

RAM - *Random Access Memory* (Memória de Acesso Aleatório),

RISC - *Reduce Instruction Set Computer* (Computador de Conjunto Reduzido de Instruções),

SMI - *Structure of Management Information* (Estrutura da Informação de Gerenciamento),

SNMP - *Simple Network Management Protocol* (Protocolo de Gerenciamento Simples),

SPI - *Serial Peripheral Interface* (Interface Periférica em Série),

SS - *Spread Spectrum* (Espalhamento Espectral),

SSP - *Synchronous Serial Port* (Porta Serial Síncrona),

TCP - *Transmission Control Protocol* (Protocolo de Controle de Transmissão),

TCP/IP - *Transmission Control Protocol/Internet Protocol* (Protocolo de Controle de Transmissão/Protocolo de Internet),

TE - *Transformer Equipment* (Equipamento Transformador),

TFTP - *Trivial File Transfer Protocol* (Protocolo Trivial de Transferência de Arquivos),

UDP - *User Datagram Protocol* (Protocolo de Datagrama de Usuário),

USB - *Universal Serial Bus* (Barramento de Série Universal),

USM - *User Security Model* (Modelo de Segurança de Usuário),

Lista de Figuras

Lista de Tabelas

1 Introdução

ANTES do advento das redes de computadores o compartilhamento e transmissão de informações ocorria através do manuseio de mídias portáteis de armazenamento, como os disquetes. A criação de métodos de transmissão de dados através de cabos (meios guiados) trouxe grande facilidade ao compartilhamento de informações e recursos, sendo esse um dos fatores principais ao grande crescimento da computação e das telecomunicações.

Na década de 90, o uso das redes de computadores com acesso à Internet expandiu consideravelmente. Com o crescimento da Internet, aumentou também a quantidade de fabricantes e equipamentos diferentes, o que causou aumento da complexidade das redes. Hoje, as redes de computadores são utilizadas em muitos estabelecimentos devido à importância do compartilhamento de informações.

Computadores são utilizados para armazenar todo tipo de informação. Portanto é necessário garantir a disponibilidade e perfeito funcionamento dos ativos de rede para garantir a disponibilidade das informações. Até o final da década de 90, técnicas reativas de análise de redes eram comumente utilizadas. Técnicas reativas são ações executadas quando um problema é encontrado. Isso significa que informações só são obtidas quando um problema se faz presente, o que gera indisponibilidade e perda técnica e financeira.

Para reduzir a necessidade de intervenção do administrador de redes, quanto ao monitoramento de tráfego e ativos de rede, foram criados os sistemas de gerenciamento de redes (do inglês: *Network Management Systems* - NMS). Um NMS é

um *software* ou conjunto de *softwares* utilizados para monitorar ativos de redes de comunicações. O NMS é responsável por verificar informações de ativos e, quando necessário, avisar ao administrador de redes quanto aos resultados obtidos.

Existem no mercado várias soluções de gerenciamento de redes, algumas proprietárias e comerciais, outras, livres e gratuitas. Entretando, grande parte delas, tem como proposta somente apresentar os resultados de coletas, e não possibilitam modificações de dados dos equipamentos.

Os NMS abertos também apresentam barreiras ao administrador por limitarem as possibilidades de gerenciamento. Visto que o gerenciamento de redes pode ser dividido em cinco áreas funcionais (STALLINGS, 1999b), as soluções abertas não cobrem todas as áreas.

Este trabalho se propõe a apresentar uma solução de gerenciamento baseada no *software* aberto Nagios, que possibilite a modificação de valores dos ativos de redes e também implemente todas as áreas do gerenciamento.

O sistema de gerenciamento proposto foi desenvolvido para gerenciar redes PLC (do inglês: *Power Line Communications*) e substituir soluções proprietárias de gerenciamento atualmente utilizadas. O uso de *software* aberto gera maior controle sobre a tecnologia, pois possibilita maior conhecimento da mesma e possibilidade de inserção de melhorias.

O gerenciamento de redes PLC é realizado através do protocolo de gerenciamento SNMP. Entretanto, esse gerenciamento é feito de forma falha. Este trabalho apresenta também uma proposta e implementação de um equipamento capaz de fornecer segurança ao gerenciamento dos ativos PLC.

1.1 Organização da Dissertação

No capítulo 2 é apresentada uma revisão de conceitos utilizados na dissertação.

No capítulo 3, *Introdução ao PLC*, é apresentada a tecnologia de transmissão

de dados através da rede elétrica. Conhecida por *Power Line Communications* - PLC ou *Broadband over Power Line* - BPL. Essa tecnologia se encontra em estado comercial na Europa e nos Estados Unidos. No Brasil, inicia-se a comercialização desta tecnologia.

A importante tarefa de gerenciamento de redes tem seus conceitos abordados no capítulo 4. Nesse capítulo também é abordado o protocolo SNMP. São definidas suas versões, as diferenças entre essas versões e características quanto a segurança.

O capítulo 5 aborda o *software* de gerenciamento Nagios. Este *software* possui código aberto, é gratuito e é amplamente utilizado devido a sua vasta documentação e possibilidade de expansão.

A proposta desse trabalho é apresentada no capítulo 6. Esse capítulo apresenta a proposta de um sistema de gerência voltado para tecnologia PLC.

No capítulo 6 também é apresentado o equipamento baseado em microcontrolador capaz de realizar a conversão de pacotes SNMP em diferentes versões e traz a capacidade de gerenciar redes PLC de forma segura.

1.2 Contribuições

Inicialmente este trabalho apresenta estudos e informações úteis ao contexto de gerenciamento de redes PLC. É apresentado também o *software* Nagios, o qual foi adaptado para o gerenciamento de redes PLC.

Para permitir o gerenciamento de redes PLC através do uso do Nagios, foram desenvolvidos *plugins* para monitorar informações específicas de ativos PLC.

Com foco na segurança do gerenciamento de redes PLC, foi proposto o desenvolvimento de um sistema embarcado capaz de implementar criptografia de dados no gerenciamento da rede PLC. Para possibilitar o desenvolvimento desse equipamento conversor foram realizados estudos sobre o protocolo SNMP e algoritmos de criptografia.

O sistema embarcado foi simulado em um *software* de simulação de componentes elétricos e eletrônicos.

Este trabalho também apresenta resultados de testes de comparação entre as versões 2c e 3 do protocolo SNMP. Esses testes são realizados para verificar a viabilidade técnica do uso do protocolo SNMPv3 no lugar do SNMPv2c.

2 *Fundamentos das Comunicações em Redes de Computadores*

Este capítulo apresenta os conceitos iniciais necessários para compreensão do trabalho proposto.

Inicialmente, serão apresentados conceitos referentes às redes de computadores, protocolos e tecnologia da informação. A preocupação com a segurança da informação é essencial e este tema também será abordado. Por fim, serão abordadas tecnologias de acesso ao meio e conceitos e métodos de modulação, importantes para o entendimento da tecnologia *Power Line Communications* - PLC.

2.1 Redes de Computadores

O século XX foi marcado pelo grande avanço tecnológico, como por exemplo a criação do rádio, a difusão da telefonia, bem como evolução dos sistemas computacionais. Entretanto, a computação só atingiu um maior desenvolvimento com a popularização dos computadores pessoais (do inglês: *Personal Computer* - PC) na década de 80 (TANENBAUM, 2003).

Até o início da década de 80 era comum a utilização de disquetes para levar arquivos à outro computador. Essa dificuldade gerada pela separação física entre computadores foi fator primordial para a grande difusão e evolução das redes de

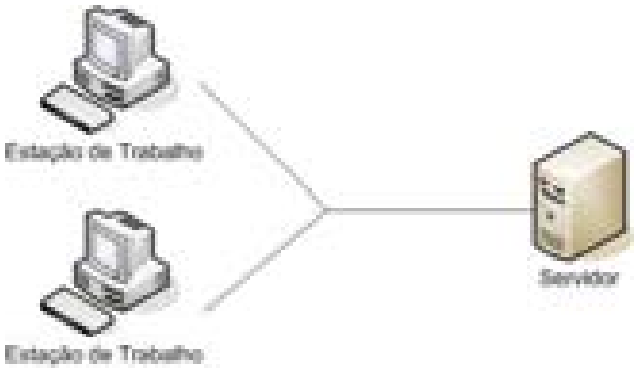

Figura 1: Modelo cliente/servidor.

computadores.

As redes de computadores surgiram no início da década de 60. Uma rede de computadores é um conjunto de computadores autônomos interconectados. Dois ou mais computadores estão interconectados quando podem trocar informações e não importa se a conexão entre eles seja por meio guiado (cabo) ou não-guiado (transmissão sem fio). Um computador autônomo não pode depender de outro computador para funcionar, ou seja, os computadores trocam informações, mas não existe uma relação de dependência entre eles (TANENBAUM, 2003).

Grande parte das redes de computadores são baseadas no modelo cliente-servidor. Nesse modelo, um computador de maior capacidade computacional, chamado servidor, disponibiliza recursos enquanto outros computadores, chamados clientes, acessam os recursos disponibilizados (TANENBAUM, 2003). O modelo cliente-servidor é apresentado na Fig. 1. A troca de informações ocorre a partir do momento que a máquina cliente abre uma conexão de rede (do inglês: *socket*), também chamada porta, e tenta estabelecer comunicação através dessa porta com a máquina servidora, que também possui uma porta aberta para receber conexões. À essas portas são designados números específicos.

As redes de computadores passaram a ser utilizadas por grandes empresas, o que defasou a utilização de terminais remotos, dependentes de um supercomputa-

dor chamado *mainframe*, que por sua vez possuí custo bastante elevado. No início da década de 90, junto com a popularização dos computadores pessoais as redes de computadores também se disseminaram, pois facilitam o compartilhamento de recursos entre os computadores. Através da percepção dessa nova tendência, empresas foram motivadas a desenvolverem soluções para permitir e facilitar a troca de comunicações de dados através das redes.

2.1.1 Pilhas de Protocolos

A comunicação entre elementos de rede (modems, PCs, roteadores, entre outros) ocorre através de regras pré-estabelecidas por de protocolos de comunicação. Assim, as partes envolvidas na transmissão saibam como tratar a informação a ser enviada ou recebida.

Para tornar a tarefa do desenvolvedor do *software* ou do *hardware* mais simples, um modelo de hierarquia de protocolos, chamado pilha de protocolos, foi criado. A finalidade desse modelo é simplificar o projeto de desenvolvimento de comunicação de rede através da divisão de tarefas entre camadas. Em cada camada deve ser realizadas tarefas específicas àquela camada. A camada de mais alto nível do equipamento transmissor, responsável por realizar a interface com o usuário, dá início à comunicação através da criação da informação. Esta informação é transmitida para sua camada inferior. Esta segunda camada superior irá encapsular a informação recebida sem ter conhecimento dos dados encapsulados, incluir suas próprias informações e repassar esse bloco de dados à sua camada inferior. Esse encapsulamento de dados, inserção de informações específicas à sua camada e repasse à camada inferior ocorre até a camada de mais baixo nível. Esta então tem como tarefa inserir todo o bloco de informações recebido no meio de comunicação.

A informação adicionada em cada camada só é interpretada pela camada equivalente, ou seja, a transmissão ocorre de forma hierárquica internamente ao elemento de rede, mas a leitura de cada informação é realizada pela camada de mesmo nível

hierárquico do destinatário (TANENBAUM, 2003).

A comunicação entre camadas de mesmo nível entre diferentes ativos de rede é possível porque a informação trocada entre elas seguem regras determinadas pelos protocolos. O protocolo também deve executar as tarefas exigidas pela camada na qual ele trabalha.

2.1.2 Modelo de Referência ISO-OSI

Na busca pela padronização internacional dos protocolos empregados em diversas camadas, a ISO (do inglês: *International Standards Organization*) criou um modelo de referência chamado OSI (do inglês: *Open Systems Interconnection*), que busca possibilitar a interconexão de sistemas abertos. Esse modelo de referência ISO-OSI foi dividido em sete camadas, como apresentado na Fig. 2, e aplica os princípios listados a seguir (TANENBAUM, 2003):

- Uma camada deve ser criada onde houver necessidade de um grau de abstração adicional;
- Cada camada deve executar uma função bem definida;
- A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
- Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;
- O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

O modelo de referência ISO-OSI não obriga a criação de pilhas de protocolos divididas em sete camadas. A finalidade, como o próprio nome diz, é expor um

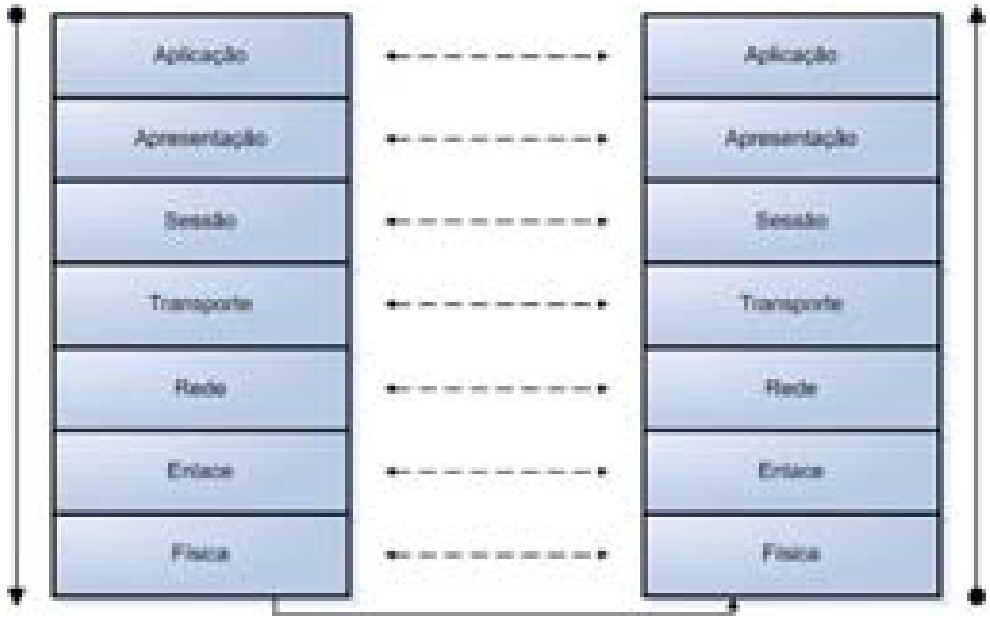

Figura 2: Modelo de referência ISO-OSI

modelo de pilha de protocolos e as tarefas que cada protocolo de cada camada deve desempenhar. Cada uma das sete camada recebe um nome associado à sua finalidade. São apresentadas cada uma das camadas a seguir (STALLINGS, 2000).

Camada de Aplicação ou Camada 7: Proporciona acesso ao ambiente de rede para usuários e também provê serviços de informações distribuídas.

Camada de Apresentação ou Camada 6: Camada responsável pela conversão de dados. As informações oriundas da camada de Aplicação são convertidas caso necessário. É o que ocorre em situações de compactação, compressão e criptografia de dados.

Camada de Sessão ou Camada 5: Camada responsável pelo controle de conexões entre aplicações como estabelecimento, gerenciamento e término de sessões entre as partes envolvidas.

Camada de Transporte ou Camada 4: Realiza controle dos dados transmiti-

dos e proporciona confiabilidade, controle de fluxo, recuperação de dados perdidos e transmissão simultânea de envio e recebimento (do inglês: *full duplex*).

Camada de Rede ou Camada 3: Provê às camadas superiores independência quanto à tecnologia de transmissão utilizada. Responsável também por endereçamento lógico e roteamento de pacotes.

Camada de Enlace ou Camada 2: Faz a interface entre o bloco de dados e o meio físico. Sua principal finalidade é dividir a informação recebida da camada superior (Rede) em quadros (do inglês: *frames*) com tamanho permitido pelo meio físico, o que reduz a a perda dessas informações através de controle de fluxo, controle de erros e sincronização.

Camada Física ou Camada 1: Lida com as características de acesso ao meio físico, ou seja, é a camada responsável pela transmissão dos *bits* em um meio de comunicação.

2.1.3 Pilha de Protocolos TCP/IP

O modelo de referência ISO-OSI é apenas um modelo que especifica as requisições existentes para que uma comunicação de rede aconteça. Entretanto, não há necessidade de que sejam envolvidos sete protocolos em uma transmissão. Assim, é possível que um protocolo execute tarefas de mais de uma camada referenciada no modelo OSI.

Muitas pilhas de protocolos foram criadas baseadas nas especificações do modelo da ISO. Entretanto, a quantidade de camadas foi reduzida, ou seja, uma camada realiza a tarefa de uma ou mais camadas do modelo OSI, como é o caso da pilha TCP/IP (do inglês: *Transmission Control Protocol/Internet Protocol*), que possui apenas quatro camadas hierárquicas. A pilha de protocolos TCP/IP obteve maior destaque entre tantas por ter sido a pilha utilizada na ARPANET, a mais antiga

rede de computadores geograficamente distribuída e que deu origem à Internet (TANENBAUM, 2003).

O modelo hierárquico TCP/IP recebeu esse nome em função de seus dois principais protocolos, o TCP e o IP, protocolos que trabalham nas camadas de Transporte e Rede (pelo modelo OSI) respectivamente. No modelo TCP/IP as quatro camadas existentes são (do nível superior para inferior) Aplicação, Transporte, Inter-redes e Host/Rede (TANENBAUM, 2003). Existem algumas diferenças de nomes dadas à primeira (Host/Rede) e segunda (Inter-redes) camadas entre alguns autores, sendo possível encontrar nomes como Interface de Rede e Internet, respectivamente (SCRIMGER et al., 2002).

A Fig. 3 apresenta a pilha TCP/IP e suas camadas. Pode-se observar que o modelo TCP/IP possui apenas quatro camadas, mas todas as especificações requeridas para uma completa transmissão são realizadas por essas camadas. A camada de Aplicação realiza as tarefas referentes às camadas de Aplicação, Apresentação e Sessão do Modelo OSI, enquanto a camada Host/Rede realiza as tarefas das camadas de Enlace e Física do modelo de referência.

Alguns protocolos pertencentes à pilha TCP/IP merecem destaque e são apresentados a seguir.

Protocolo de Transferência de Hiper Texto: do inglês: *Hypertext Transfer Protocol* - HTTP). Protocolo da camada de aplicação responsável pela transmissão de conteúdo hipertexto. O conteúdo hipertexto possui textos, imagens, sons e vídeos disponibilizados em páginas de Internet e acessados através de programas navegadores (do inglês: *browsers*). Este protocolo trafega dados através do uso do TCP como protocolo de transporte. Um servidor HTTP, também chamado servidor Web recebe conexões na porta 80.

Protocolo de Gerenciamento de Rede Simples: (do inglês: *Simple Network Management Protocol* - SNMP). Protocolo da camada de Aplicação utilizado

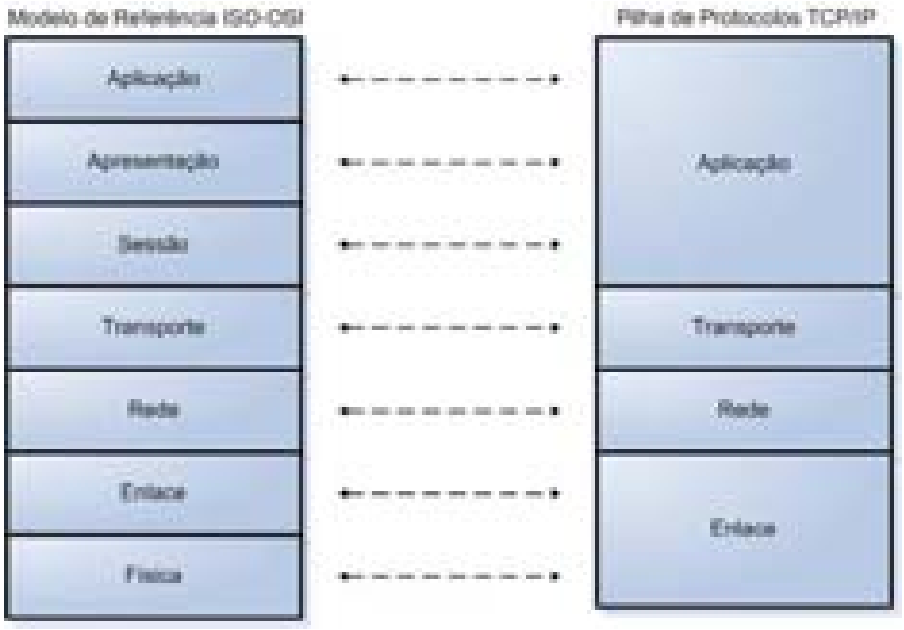

Figura 3: Pilha TCP/IP e Suas Camadas.

para gerenciar redes de comunicações através de consultas aos dispositivos da rede. Utiliza o UDP como protocolo de transporte e utiliza as portas 161 e 162.

Protocolo de Controle de Transmissão: (do inglês: *Transmission Control Protocol* - TCP). Protocolo da camada de transporte utilizado pela grande maioria dos protocolos de aplicação da pilha TCP/IP por ser confiável (o receptor não envia confirmação de recebimento do pacote ao emissor), orientado a conexão e realizar controle de fluxo. Sua desvantagem é gerar um cabeçalho (do inglês: *overhead*) muito grande. A confiabilidade é uma importante característica desse protocolo pois permite a detecção de perda de segmentos (fragmentos da informação gerada pelo protocolo de Aplicação).

Protocolo de Datagrama de Usuário: (do inglês: *User Datagram Protocol* - UDP). Protocolo da camada de Transporte utilizado por poucos protocolos de Aplicação da pilha TCP/IP por não ser confiável (emissor não recebe confirmação

de recebimento por parte do receptor), não estabelecer conexão e não realizar controle de fluxo. Sua vantagem é gerar um cabeçalho (*overhead*) pequeno, o que deixa a transmissão mais rápida.

Protocolo de Internet: (do inglês *Internet Protocol* - IP). Protocolo da camada de Inter-rede responsável por integrar redes através do endereçamento lógico dos ativos de rede através do número IP. Esse endereçamento lógico permite a integração de redes de diferentes enlaces. O protocolo IP também realiza roteamento de pacotes (ou datagramas), ou seja, escolhe a melhor rota para transmitir o pacote. O protocolo IP não é confiável (emissor não recebe confirmação de recebimento por parte do receptor).

Protocolo de Mensagens e Controle de Internet: (do inglês: *Internet Control Messaging Protocol* - ICMP). Protocolo da camada de Inter-rede que tem como finalidade realizar ou pelo menos aumentar a confiabilidade não proporcionada pelo IP, ou seja, é utilizado como complemento ao IP. Quando necessário, envia mensagens de erro e controle aos elementos de rede envolvidos em uma transmissão.

Ethernet: protocolo de enlace responsável pela etapa final para transmissão da informação ou etapa inicial de recebimento da informação. Quando a informação é enviada, o protocolo Ethernet verifica se o datagrama recebido da camada superior (Rede) precisa ser segmentado. Se necessário a informação é divida em quadros (do inglês: *frames*) e então o cabeçalho Ethernet é adicionado ao quadro e transmitido. Quando a informação é recebida pela rede, o Ethernet captura a informação e verifica se o destinatário é ele mesmo. Se verdadeiro, então ele realiza a tarefa de desencapsular o datagrama IP e entregá-lo à camada de Rede (superior).

Dentre as informações encontradas no cabeçalho do protocolo Ethernet duas merecem maior destaque, que são endereço MAC (do inglês: *Media Access Control*) de origem e endereço MAC de destino. O campo endereço MAC de origem

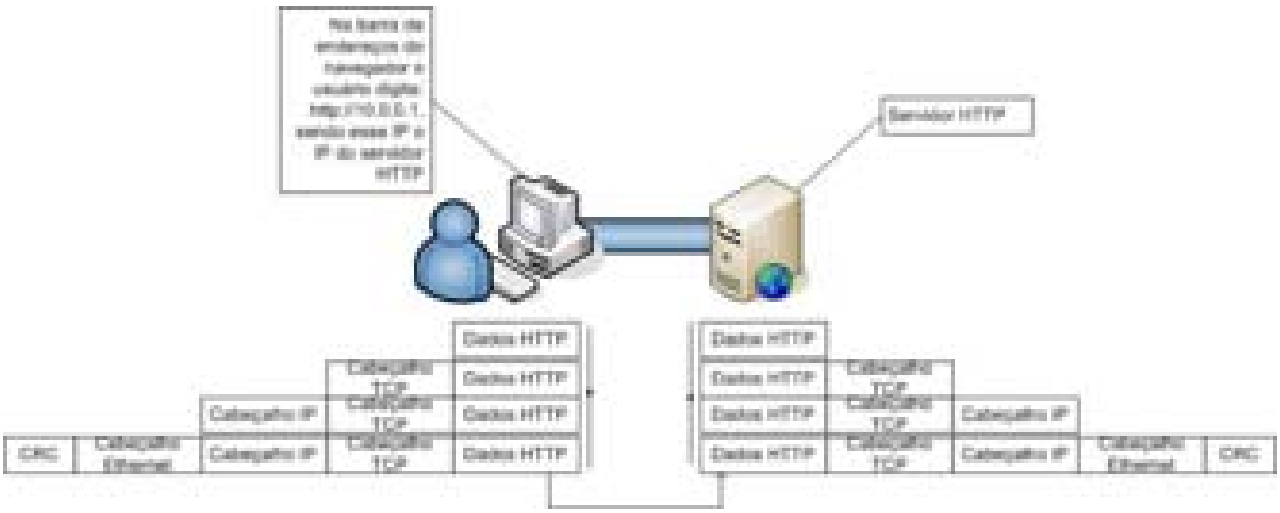

Figura 4: Transmissão HTTP.

contém uma sequência de 48 *bits* que representa um número único de uma interface de rede Ethernet. Quando um ativo de rede Ethernet recebe um quadro Ethernet, o endereço de origem é verificado para saber quem enviou esta informação, e portanto, para quem deve responder. O endereço MAC de destino identifica qual ativo de rede ethernet deve receber e tratar a informação (HELD, 2003).

A Fig. 4 apresenta uma transmissão por meio da pilha TCP/IP. Neste caso, uma transmissão HTTP é exemplificada.

2.2 Segurança da Informação

As redes de computadores, e principalmente, a rede mundial de computadores, a Internet, trouxeram diversas facilidades, como compartilhamento de informações entre lugares e pessoas fisicamente distantes. A Internet possibilita, por exemplo, que uma filial de uma empresa consulte informações disponíveis na matriz de forma simples e rápida, o que gera economia, rapidez e comodidade para essa empresa.

Porém, as informações armazenadas ou transmitidas em equipamentos de rede

devem ser tratadas com cuidado, pois o valor agregado da informação é muito alto.

Portanto, a segurança da informação se tornou imprescindível com a disseminação da Internet. A segurança da informação visa garantir que a informação se mantenha segura.

A segurança de informação envolve basicamente cinco conceitos: autenticação, autorização, confidencialidade, integridade e disponibilidade (STALLINGS, 1999a). A autenticação garante que a origem de uma mensagem ou documento eletrônico está corretamente identificada, com confirmação de que a identidade não é falsa. A autorização requer que o acesso a recursos de informação deva ser controlado pelo ou para o sistema alvo. A confidencialidade garante que a informação em um sistema computacional e a informação transmitida são acessíveis somente para leitura por terceiros autorizados. Esse tipo de acesso inclui impressão, exibição, e outras formas de fechamento, e inclui a simples revelação da existência de um objeto. A integridade garante que somente terceiros autorizados são capazes de modificar informações computacionais e informações transmitidas. Modificação inclui escrita, modificação de estado, remoção, criação, atraso ou replicação de mensagens transmitidas. A disponibilidade requer que serviços computacionais estejam disponíveis para terceiros autorizados, quando necessário (STALLINGS, 1999a).

2.2.1 Criptografia e Algoritmos Criptográficos

De acordo com Menezes, Oorschot e Vanstone (1996), criptografia é o estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação, como confidencialidade, integridade dos dados, autenticação de entidade e verificação de origem de dados. Os egípcios foram os pioneiros na criação dessa técnica, a 4.000 anos atrás através do simples deslocamento de letras três posições à direita.

Cifrar um dado significa utilizar algum método para alterar alguma informação original, de forma que somente uma entidade específica e desejada possa obter a informação original. Para que a informação original possa ser obtida, tendo-se

em mãos a informação cifrada, é necessário decifrar essa informação. A técnica de criptografia estuda exatamente como criar formas para garantir que somente a entidade desejada seja capaz de decifrar uma informação que tenha sido cifrada.

A mensagem ou texto original, sem criptografia, utiliza uma chave, definida como chave criptográfica, para gerar o texto criptografado. Somente através de uma chave específica, que pode ser ou não a mesma utilizada para cifrar o texto original, é possível decifrar a informação.

A chave criptográfica é uma cadeia de *bits*. Essa cadeia tem um tamanho pré-definido de acordo com o algoritmo. O tamanho da chave está diretamente relacionado com a quantidade de possibilidades diferentes para uma chave. Para um algoritmo que utiliza chave de 56 *bits*, existem 2^{56} possibilidades diferentes de chaves para esse algoritmo, ou seja, 7,2 x 10^{16} possibilidades (STALLINGS, 1999a).

A criptografia pode ocorrer de duas formas, simétrica e assimétrica. Na criptografia simétrica são utilizados algoritmos criptográficos simétricos que compartilham a mesma chave para executar a operação de criptografia e também de decifragem, ou seja, a mesma chave utilizada para criptografar é utilizada para decifrar. Na criptografia assimétrica são utilizados algoritmos criptográficos assimétricos, que utilizam par de chaves. Duas chaves são utilizadas, definidas como chave pública e chave privada. A chave pública é utilizada para criptografar a informação. Uma vez criptografada com a chave pública, nem mesmo através dela é possível decifrar. Para se obter a informação original é necessário ter a chave privada. Somente através da chave privada que originou a chave pública, é possível decifrar a mensagem.

A criptografia simétrica faz uso de uma chave, chamada chave simétrica, que é utilizada tanto para criptografar quanto para decifrar uma mensagem. Já a criptografia assimétrica faz uso de um par de chaves, chamadas chave pública e chave privada.

A chave pública é utilizada para criptografar o arquivo ou informação, e a

chave privada é utilizada para decifrar. Esses recursos devem ser utilizados para garantir a segurança de acesso aos aplicativos e arquivos de rede.

A segurança das redes de transmissão não deve ser aplicada somente à parte lógica, mas também à parte física. É necessário garantir o acesso físico aos equipamentos da rede somente as pessoas autorizadas. Sistemas operacionais e equipamentos de rede possuem recursos de segurança, como autenticação, autorização e criptografia, porém o gerenciamento da segurança não deve estar restrito à utilização única dessas soluções por *software*.

É necessário estabelecer políticas de segurança, como senhas seguras, alteração periódica de senhas, efetivo controle de acesso, armazenamento seguro das chaves criptográficas e uso de *softwares* de verificação de segurança que procuram por vulnerabilidades.

É importante ressaltar que a segurança deve ser garantida a todos os elementos da rede, não apenas servidores. Estações de trabalho devem possuir recursos de segurança, como *firewall* e anti-vírus. Ativos de rede embarcados, como modems, *switches* e roteadores, devem realizar outros métodos de segurança, como autenticação e autorização.

Outro recurso que deve receber atenção quanto ao gerenciamento de segurança são os registros de eventos (do inglês: *logs*). Os registros armazenam os principais eventos referentes à autenticação e autorização. Através dos *logs* é possível observar quais usuários realizaram autenticação e acesso a qual tipo de recurso, inclusive a tentativas mal-sucedidas.

É importante também ressaltar que a própria tarefa de gerenciamento deve ser realizada com segurança. O gerenciamento é feito em geral através de um protocolo de gerenciamento, onde SNMP é o mais utilizado. Para a utilização desse protocolo de gerenciamento é aconselhável utilizar a versão 3 do mesmo, que possibilita o uso de autenticação em *hash* (texto cifrado de forma unilateral, ou seja, a partir do texto cifrado não é possível obter o texto original) e criptografia

dos dados transmitidos (STALLINGS, 1999b).

2.2.1.1 *Data Encryption Standard*

De acordo com Schneier (1996), no início dos anos 70, pouco se conhecia a respeito da criptografia. Quase não se publicava artigos a respeito desse assunto. Porém, o órgão americano NBS (do inglês: *National Bureau of Standards*), responsável por criar padrões, hoje conhecido como NIST (do inglês: *National Institute of Standards and Technology*), iniciou um projeto para aumentar a segurança de computadores e dados, através da criação de um algoritmo de criptografia que se tornaria um padrão criptográfico.

Então, ao final de 1976, o algoritmo de criptografia denominado DES (do inglês: *Data Encryption Standard*) foi adotado como um padrão federal de criptografia. O DES é baseado em um algoritmo denominado Lucifer, que fora desenvolvido pela IBM. Entretanto, algumas modificações foram feitas, como a mudança do tamanho da chave de 128 *bits* para 56 *bits*.

Como define o nome do algoritmo DES, este foi inicialmente tratado como um padrão, não como algoritmo, porque quando foi realizado o concurso para a escolha de um algoritmo internacional de criptografia, não se sabia qual seria o algoritmo selecionado. Sabia-se apenas que este algoritmo se tornaria um padrão para criptografia, justificando seu nome.

O DES é um algoritmo de chave simétrica de 56 *bits* e pode receber um padrão (texto) de entrada a ser criptografado de até 64 *bits*. Como resultado, é gerado um texto cifrado de também 64 *bits*.

Caso o texto claro, não cifrado, de entrada seja maior que 64 *bits*, esta cadeia de *bits* é segmentada em blocos de 8 *bytes*, e então cada bloco é criptografado.

De acordo com Schneier (1996), tabelas definidas como tabelas de permutação são utilizadas para substituir a cadeia de *bits* do texto claro por bits da chave criptográfica. Essa permutação é realizada 16 vezes, e ao término de cada permutação,

também é realizada uma operação de ou-exclusivo. Ao final das 16 rodadas, uma última permutação é executada e obtem-se o texto cifrado.

O algoritmo utiliza operações lógicas e aritméticas, o que demonstra a simplicidade de processamento, e portanto, demonstra a possibilidade de uso deste algoritmo até mesmo em dispositivos de baixo poder de processamento e com recursos limitados, como um microcontrolador.

Algoritmos de criptografia podem utilizar métodos complementares ao seu funcionamento, o que aumenta sua capacidade de segurança. O método utilizado é aplicado antes da criptografia do texto. A criptografia DES implementada no SNMPv3 utiliza o o modo de operação CBC (do inglês: *Cipher Block Chaining*). Este método utiliza um vetor de inicialização, definido como IV (do inglês: *Initialization Vector*). Uma operação de ou-exclusivo é realizada entre o vetor de inicialização e o primeiro texto claro de entrada, ainda não cifrado pelo algoritmo DES. Em seguida, o texto resultante da operação ou-exclusivo é cifrado. Para que os próximos textos de entrada sejam criptografados, o texto criptográfico gerado anteriormente é utilizado na operação de ou-exclusivo com o próximo texto a ser criptografado.

2.3 Modulações de Tecnologias de Acesso

Tecnologias de acesso utilizam meios para transmitir os dados, que podem ser meios guiados (por cabo) ou não-guiados (sem fio).

Para possibilitar a transmissão de dados pelos meios específicos, são utilizados métodos de adaptação da informação àquele meio específico. Esses métodos são chamados de modulação. A tecnologia ADSL (do inglês: *Assymmetric Digital Suscriber Line*, por exemplo, utiliza uma modulação chamada Multiplexação por Divisão de Frequência (do inglês: *Frequency Divison Multiplex* - FDM). Já a tecnologia *cable modem* utiliza as modulações Deslocamento de Chave por Fase Quadratura (do inglês: *Quadrature Phase Shift Keying* - QPSK) e Modulação de

Amplitude Quadratura (do inglês: *Quadrature Amplitude Modulation* - QAM).

Para a tecnologia PLC, a qual é analisada nessa dissertação, existem duas modulações utilizadas, que são Espalhamento Espectral e OFDM, apresentadas a seguir.

2.3.1 Modulações da Tecnologia PLC

Diferentes técnicas ou opções de modulação são utilizadas na tecnologia PLC para acoplar o sinal elétrico ao sinal de comunicação. As duas técnicas mais difundidas são: Espalhamento Espectral (do inglês: *Spread Spectrum*) e Multiplexação por Divisão de Frequência Ortogonal (do inglês: *Orthogonal Frequency Division Multiplexing* - OFDM). O canal PLC tem a característica de ser seletivo em frequência, devido à característica multipercurso das redes de transmissão de energia. Por esta razão, é necessário que se aplique uma técnica de modulação mais eficiente em redes PLC.

O número de portadoras adotadas varia conforme o tipo de padrão de PLC usado. A tecnologia PLC utiliza a faixa de frequência de 1,7 MHz a 30 MHz, com espalhamento de harmônicos em frequências mais altas. Por permitir a transmissão de dados através de várias sub-portadoras independentes, a técnica de modulação OFDM tem sido uma boa alternativa para a transmissão de dados sobre o canal PLC (BORBA; SILVA; ELIAS, 2007).

2.3.1.1 Espalhamento Espectral

Uma grande preocupação no estudo das comunicações digitais é com o uso eficiente da largura de banda e energia do sinal transmitido. Entretanto, existem situações em que a eficiência deve ser deixada em segundo plano, e deve-se focar na segurança, quando se existe um ambiente hostil para a transmissão dos dados. Para suprir essa necessidade é possível utilizar técnicas conhecidas como modulação por Espalhamento Espectral (do inglês: *Spread Spectrum Modulation*) (HAYKIN,

1988).

A principal vantagem de se utilizar um sistema de espalhamento espectral é sua habilidade de rejeitar interferência, seja ela causada de forma inconsciente por outro usuário que tenta transmitir simultaneamente, ou seja ela causada por um hostil que deseja atrapalhar ou congestionar a transmissão.

Ainda de acordo com Haykin (1988), a definição de espalhamento espectral pode ser dividida em duas partes. A primeira define que espalhamento espectral é uma forma de transmissão na qual a sequência de dados ocupa uma largura de banda excedente à minima requerida para transmissão. A segunda define que o espalhamento espectral é realizado antes da transmissão, através do uso de um código que independe da sequência de dados. O mesmo código é utilizado pelo receptor da informação para reorganizar a sequência anteriormente espalhada, e então obter a mensagem original. A modulação por espalhamento espectral foi desenvolvida para atuar em ambientes onde a susceptibilidade a interferências é uma grande preocupação.

2.3.1.2 Multiplexação por Divisão de Frequência Ortogonal

A Modulação OFDM gera um grande número de portadoras de faixa estreita, distribuídas bem próximas, sendo possível suprimir os sinais interferentes ou variar o número de *bits* de acordo com a relação sinal/ruído.

O OFDM consiste em um grande número de portadoras estreitas, distribuídas lado a lado. Este tipo de modulação se adapta facilmente à variação das características do canal, com eliminação de portadoras interferidas e correspondente diminuição na taxa de transmissão.

De acordo com Hrasnica, Haidine e Lehnert (2004), Modulação de Múltiplas Portadoras (do inglês: *MultiCarrier Modulation* - MCM) é o princípio de transmistir dados pela divisão da sequência de dados em várias cadeias de bits em paralelo, onde cada cadeia tem uma taxa de bits muito menor, e utiliza-se várias portadoras,

chamadas sub-portadoras, para modular essas sub-cadeias. Os primeiros sistemas que utilizaram MCM foram *links* de rádio HF na década 1960.

Multiplexação por Divisão de Frequência Ortogonal (do inglês: *Orthogonal Frequency Divison Multiplex* - OFDM) é uma forma especial de de MCM que utiliza sub-portadoras com espaços densos e espectro sobreposto. Para permitir uma recepção sem erros de sinais OFDM, as formas de ondas das sub-portadoras são ortogonais entre elas.

A modulação OFDM transmite símbolos que tem relativa longa duração, mas pouca largura de banda. No caso de um símbolo que tem duração menor ou igual ao máximo espalhamento de atraso, o sinal recebido consiste de versões sobrepostas dos símbolos transmitidos ou interferência entre os símbolos. Geralmente, OFDM são criados de forma que cada sub-portadora seja estreita o bastante para provocar o efeito *flat fading* (o sinal em cada sub-portadora sofre os efeitos degradantes de propagação simultaneamente). Isso permite que as sub-portadoras permaneça ortogonal quando o sinal é transmitido sobre um canal seletivo de frequência, mas invariável no tempo. Se um sinal modulado por OFDM é transmitido nesse tipo de canal, cada sub-portadora sofre uma atenuação diferente. Durante a codificação das cadeias de dados, erros que geralmente ocorrem em sub-portadoras severamente atenuadas são detectados e geralmente são corrigidos no receptor pelo por métodos de correção de erros.

3 *Power Line Communications*

Neste capítulo serão abordados os conceitos e informações técnicas relacionados à tecnologia *Power Line Communications*, tais como funcionamento, topologia, arquitetura, equipamentos envolvidos e segurança.

Uma das grandes barreiras existentes para uma ampla disseminação do acesso à Internet para o público em geral é a ausência de um meio de transmissão de dados de baixo custo. Nos últimos anos, um grande esforço tem sido realizado para permitir a utilização da rede de energia elétrica para a transmissão de dados em banda larga.

Este esforço inclui o desenvolvimento de equipamentos para a rede de acesso, tanto em baixa quanto em média tensão, e de dispositivos a serem utilizados pelo usuário final, baseado no conceito de aproveitamento da rede elétrica. As adversidades do meio elétrico, como harmônicos, ruído e distância, são as principais barreiras para a transmissão de dados num canal sobreposto à rede de Energia Elétrica (CAVALIERE; BANDIM, 2007). Um fator relevante para a adoção dessa tecnologia, denominada PLC (do inglês: *Power Line Communications*) é a capilaridade que o sistema pode atingir (HRASNICA; HAIDINE; LEHNERT, 2004).

Segundo dados da ANEEL (ANEEL, 2009), o mercado de distribuição de energia elétrica no Brasil é atendido por 64 Concessionárias, estatais ou privadas, que abrangem todo o País, atendendo cerca de 47 milhões de unidades consumidoras. 85% dos desses consumidores são residenciais.

Exemplificando a potencialidade, O Estado de Goiás possui 2.048.251 unidades consumidoras de Energia Elétrica (GOIáS, 2009). A Concessionária de Energia Elétrica que atende a esses consumidores, denominada Companhia Energética de Goiás (CELG), possui aproximadamente dois milhões de clientes distribuídos em 237 municípios, beneficiando quatro milhões de habitantes, o que representa 90% da população total do Estado (CELG, 2009).

A tecnologia PLC pode ser utilizada como suporte a Operação e Manutenção (O&M) do fornecimento de Energia Elétrica. Dentro deste contexto, várias funções da rede e inúmeros serviços de interesse da concessionária de energia elétrica podem ser providos, dentre os quais se destacam: (a) supervisão do fornecimento de energia elétrica em Média Tensão (MT) (RODRIGUES; SILVA, 2003) e Baixa Tensão (BT) (ALMEIDA; SILVA; MACHADO, 2006), que proporciona suporte à redução das perdas comerciais e a melhora dos índices de continuidade e qualidade dos serviços prestados pela concessionária; e (b) serviços de Rede Inteligente (RI), como o sensoriamento remoto, a telemedição e os serviços de segurança e de alarme e manutenção da rede.

A tecnologia PLC mais atual, também conhecida como Banda Larga sobre Rede Elétrica (do inglês: *Broadband Powerline Communications* - BPL) utiliza a rede elétrica para a transmissão de dados em banda larga (HRASNICA; HAIDINE; LEHNERT, 2004). Esta tecnologia tem se mostrado bastante competitiva no mercado de acesso em banda larga, e conta com a vantagem de ter uma infra-estrutura bastante abrangente. É plenamente possível que a tecnologia PLC venha a se tornar uma boa solução de acesso e permita o surgimento de uma série de serviços que poderão ser oferecidos por concessionárias de energia elétrica, como:

- Transmissão de voz, dados e vídeo;
- Internet banda larga (e aplicação Voz sobre IP - VoIP);
- Serviços de Rede Inteligente (sensoriamento remoto, telecomando/telemedida, supervisão e automação);

- Serviços de segurança (câmeras de monitoramento, sistemas de alarme e manutenção remota);
- Supervisão do fornecimento de energia elétrica.

Algumas restrições são comuns à tecnologia PLC aplicada tanto em redes de baixa quanto nas de média tensão, como por exemplo relação sinal-ruído, interferência, segmentação de alimentadores e segurança no trabalho.

A solução de comunicação em média tensão, combinada com a tecnologia *Power Line Communications* de baixa tensão resulta em um sistema otimizado que provê economia do meio de transmissão e disponibiliza serviços de dados em banda larga.

Na rede de energia de baixa tensão, para suportar a transmissão de dados sobre o sistema de transmissão de energia, um controlador de portadoras PLC (do inglês: *PLC Controller*) é instalado, normalmente, no transformador de baixa tensão. O controlador PLC acopla o sinal de dados proveniente dos equipamentos de última milha à rede de telecomunicações (BORBA; SILVA; ELIAS, 2007).

A tecnologia PLC não pode ser considerada uma nova tecnologia, pois desde o início do século passado as redes elétricas têm sido utilizadas para suportar serviços de telecomunicações em ambientes internos.

Desde a década de 1920, o Sistema de Ondas Portadoras em Linhas de Alta Tensão (do inglês: *PowerLine Carrier* - OPLAT), de acoplamento capacitivo, vem sendo utilizado pelas empresas de energia elétrica para telemetria, controle remoto e comunicação de voz. Todas essas aplicações de faixa estreita, que operam em baixa frequência (de 3 kHz a 148,5 kHz) com modulação analógica e velocidade de transmissão de dados que não ultrapassa a 9,6 kbps.

Diversas empresas resolveram abandonar o *Power Line* devido ao avanço das fibras óticas e ao barateamento de outros sistemas de telecomunicações. Devido a falta de demanda, os fabricantes deixaram de produzir estes equipamentos por um

bom tempo.

O meio físico PLC é bastante hostil para a transmissão de dados, visto que não foi concebido para este fim. Há, portanto, uma série de propriedades das redes de energia que influenciam negativamente as comunicações em alta velocidade, como perdas no cabo, propagação em múltiplos caminhos e ruído (HRASNICA; HAIDINE; LEHNERT, 2004).

Uma forma de reduzir o impacto do meio de transmissão na comunicação é a aplicação de métodos eficientes de modulação, como por exemplo, o OFDM, além de mecanismos de correção de erro, dentre os quais podem-se destacar o FEC (do inglês: *Forward Error Correction*) e o ARQ (do inglês: *Automatic Repeat reQuest*). Entretanto, independente das técnicas adotadas, um fator a ser observado e bem compreendido é o ruído presente na comunicação.

Na Europa, em 1997, foram criados o PLC Forum (PLCFORUM, 2009) e o projeto OPERA (do inglês: *Open PLC European Research Alliance*). Em 1998 foi lançado nos Estados Unidos o PLTF (do inglês: *PowerLine Telecommunications Forum*).

Nesta época, o setor de telecomunicações brasileiro apresentava um crescimento explosivo, principalmente na área de telecomunicação móvel e acesso à Internet, e várias empresas de telecomunicações foram privatizadas. Muitas empresas de energia elétrica começaram a avaliar a possibilidade de se tornarem provedores de serviços de telecomunicações. Na época, o acompanhamento do desenvolvimento dessa tecnologia no Brasil era realizado pelo Sub-Comitê das Comunicações do GCOI e pela APTEL, criada em abril de 1999.

3.1 Funcionamento da Tecnologia PLC

A tecnologia PLC, ou BPL, utiliza um princípio similar à tecnologia do DSL (GOLDEN; DEDIEU; JACOBSEN, 2008) (do inglês: *Digital Subscribe Line*) para a

transmissão de dados.

Os dados são transmitidos pelo cabo de energia elétrica devido ao uso de frequências de sinalização mais altas do que as utilizadas para transmissão de energia elétrica. O PLC se relaciona principalmente com a camada 2 do modelo ISO/OSI (Enlace) e pode ser agregado a uma rede TCP/IP (camada 3, rede) já existente ou trabalhar em conjunto com outras tecnologias de camada 2 (HRASNICA; HAIDINE; LEHNERT, 2004).

O PLC utiliza faixa de frequência alocada para radiodifusão (ondas curtas) e parte da faixa de frequência de radiocomunicações em VHF utilizada por serviços públicos (polícia, bombeiros, defesa civil).

A faixa típica de frequências utilizada pela rede PLC está entre 1,7 MHz e 30 MHz, com espalhamento de harmônicos em frequências mais altas (HRASNICA; HAIDINE; LEHNERT, 2004). De modo geral, o PLC é composto de unidades concentradoras (do inglês: *Head End*), repetidoras e Unidades de Terminação de Cliente (do inglês: *Customer Premise Equipment* - CPE). O sinal PLC é transmitido sobre os fios de cobre das redes de distribuição de baixa e média tensão.

A transmissão de sinais de comunicação sobre as linhas de corrente alternada se torna complexa devido às características topológicas das linhas de distribuição de energia elétrica, existência de ruídos e interferências não previsíveis, problemas de segurança de dados devido ao compartilhamento de circuitos entre diversos consumidores, e irradiação das frequências transmitidas em linhas abertas sem nenhum tipo de blindagem (BORBA; SILVA; ELIAS, 2007).

O sinal PLC é gerado na central e encaminhado ao injetor, que se encarrega de enviá-lo a rede de energia elétrica.

Para a transmissão do sinal PLC em média tensão, os repetidores também tem a finalidade de evitar que transformadores filtrem as altas frequências, que são utilizadas para transmissão do sinal PLC.

Ao chegar à rede domiciliar, o extrator, o qual separa o sinal elétrico do sinal

de dados, deixa o sinal pronto para ser utilizado na residência, e é encaminhado por meio da própria fiação elétrica até o modem PLC, que entrega o sinal através de uma porta Ethernet ou USB (do inglês: *Universal Serial Bus*).

Para se conectar equipamentos PLC à rede de energia elétrica, devem ser utilizados equipamentos padronizados que oferecem isolamento adequado entre os sinais de telecomunicações e de energia elétrica, e mantém a integridade do sistema e do usuário.

De acordo com Hrasnica, Haidine e Lehnert (2004), alguns equipamentos residenciais, em especial eletrodomésticos, podem causar interferências na rede PLC, como motores e *dimmers* de luz, além de secadores de cabelos, aspiradores de pó, furadeiras elétricas, e, com menor atuação, os chuveiros elétricos.

3.1.1 Características das Linhas de Transmissão

Os cabos utilizados para distribuição de energia elétrica empregam dielétricos (SCHMIDT, 1979) que apresentam elevadas perdas em altas frequências, o que limita a distância de propagação do sinal ao longo dos cabos. Os cabos de distribuição aéreos, utilizados em grande parte da rede de energia elétrica brasileira, não são eletricamente simétricos (balanceados), o que facilita a irradiação de sinais de alta frequência e causa interferência nas radiocomunicações, ao mesmo tempo em que também recebem interferências.

Segundo Dostert (2001), o sistema de fornecimento de energia elétrica possui três níveis de tensão distintos, de acordo com a distância alcançada: nível de alta tensão (acima de 60 kV), de média tensão (entre 1 kV e 60 kV) e de baixa tensão (abaixo de 1 kV). Entretanto, essa padronização varia de acordo com o país e literatura.

O nível de alta tensão interliga centros de geração aos centros de consumo, e geralmente percorrem grandes distâncias. Com frequência de 50 ou 60 Hz, o comprimento de onda correspondente às linhas aéreas é de 6.000 ou 5.000 km,

respectivamente. O nível de tensão é marcado principalmente pelas perdas por efeito Joule, descargas oriundas do efeito corona, que introduz componentes de alta frequência na rede, por capacitâncias e indutâncias parasitas.

O nível de média tensão interliga subestações a centros de distribuição de consumo. São redes construídas através de linhas aéreas com valores nominais de tensão típicos entre 10 e 20 kV, ou cabos, geralmente subterrâneos. As linhas aéreas normalmente fornecem energia elétrica para áreas rurais, pequenas cidades ou companhias industriais, e tem comprimento típico entre 5 e 25 km.

O nível de baixa tensão é o nível que efetivamente chega à maioria das unidades consumidoras. Possui o ambiente mais hostil para a transmissão de sinais, devido à natureza dinâmica de cargas inseridas e removidas da rede, às emissões provenientes dos equipamentos e às perturbações. Neste nível de tensão, os raios de fornecimento típico a partir de um transformador de baixa tensão são de 100 a 500 m (DOSTERT, 2001).

A propagação do sinal através da linha de transmissão de energia elétrica provoca uma atenuação e um atraso no sinal que aumentam com a distância e a frequência. A atenuação depende da impedância característica (Z_L) e da constante de propagação (γ) das linhas de transmissão, que são funções da resistência R, condutância G, indutância L e capacitância C por unidade de comprimento, e dependem da frequência f. A impedância característica Z_L e a constante de propagação $\gamma(f)$ são dadas pelas seguintes equações (HRASNICA; HAIDINE; LEHNERT, 2004):

$$Z_L(f) = \sqrt{\frac{R(f) + j2\pi.L(f)}{G(f) + j2\pi.C(f)}} \tag{3.1}$$

e

$$\gamma(f) = \sqrt{(R(f) + 2j\pi.L(f)).(G(f) + 2j\pi.f.C(f))}. \tag{3.2}$$

A equação da função de transferência de uma linha de comprimento l em função da frequência e da distância é dada por

$$H(f,l) = exp(-\gamma(f).l). \tag{3.3}$$

Em diferentes investigações e medições, concluiu-se que para altas frequências, como a banda de frequência PLC (1 MHz a 30 MHz), a impedância característica e a constante de propagação são, respectivamente

$$Z_L(f) = \sqrt{\frac{L}{C}} \tag{3.4}$$

e

$$\gamma(f) = \frac{1}{2}.\frac{R(f)}{Z_L} + \frac{1}{2}G(f)Z_L + 2j\pi.f\sqrt{L.C}. \tag{3.5}$$

A função de transferência é dada por

$$H(f) = A(f,l)exp(-j2\pi.f\tau), \tag{3.6}$$

onde $A(f,l)$ representa a atenuação do sinal e $exp(-j2\pi.f\tau)$ representa o atraso de propagação do sinal. A topologia das redes de distribuição de energia elétrica difere consideravelmente das redes de comunicações tradicionais. Numerosas reflexões do sinal são recebidas e ocorrem principalmente devido à junção de cabos de diferentes impedâncias. Desta forma, a função de transferência da linha de transmissão é dada por

$$H(f) = \sum_{i=1}^{N} g_i.A(f,l_i)exp(-j2\pi.f\tau_i). \tag{3.7}$$

No domínio do tempo tem-se o canal PLC representado pela seguinte equação:

$$h(t) = \sum_{i=1}^{N} C_i \delta(t - \tau_i), \tag{3.8}$$

onde C_i e τ_i são, respectivamente, um fator de atenuação e o atraso dos múltiplos sinais recebidos, e N é o número de multipercursos consideráveis no canal. O δ é o delta de Dirac ou impulso unitário.

As junções dos cabos, os transformadores, os medidores de energia, a entrada e saída de cargas e as topologias das redes provocam grandes variações de carregamento nas redes e formam múltiplos pontos de reflexão, o que torna o ambiente dinâmico e repleto de ecos. Os transformadores e medidores de energia são elementos de bloqueio para sinais de alta frequência, que necessitam de elementos *by-pass* para a propagação de sinais (HRASNICA; HAIDINE; LEHNERT, 2004).

3.1.2 Redes Domiciliares Através da Fiação Elétrica

A configuração básica de uma rede PLC é constituída por um equipamento denominado *Master* ou *Head End Router* instalado próximo ao transformador de baixa tensão onde é realizado o acoplamento em paralelo com as três fases e o neutro da rede de energia elétrica. O *Master* tem a função de gerenciar e distribuir/concentrar a transmissão das informações aos *modems* PLC, instalados nos assinantes.

Para se introduzir e adaptar os sinais de dados dos equipamentos PLC para as redes de baixa e média tensão são necessários acopladores, que podem ser capacitivos (injetam os sinais de dados através de contato direto com as linhas de energia elétrica) ou indutivos (injetam os sinais por indução). Os acopladores do tipo indutivo são mais utilizados em média tensão, enquanto que os acopladores capacitivos têm maior aplicação na injeção do sinal PLC em baixa tensão.

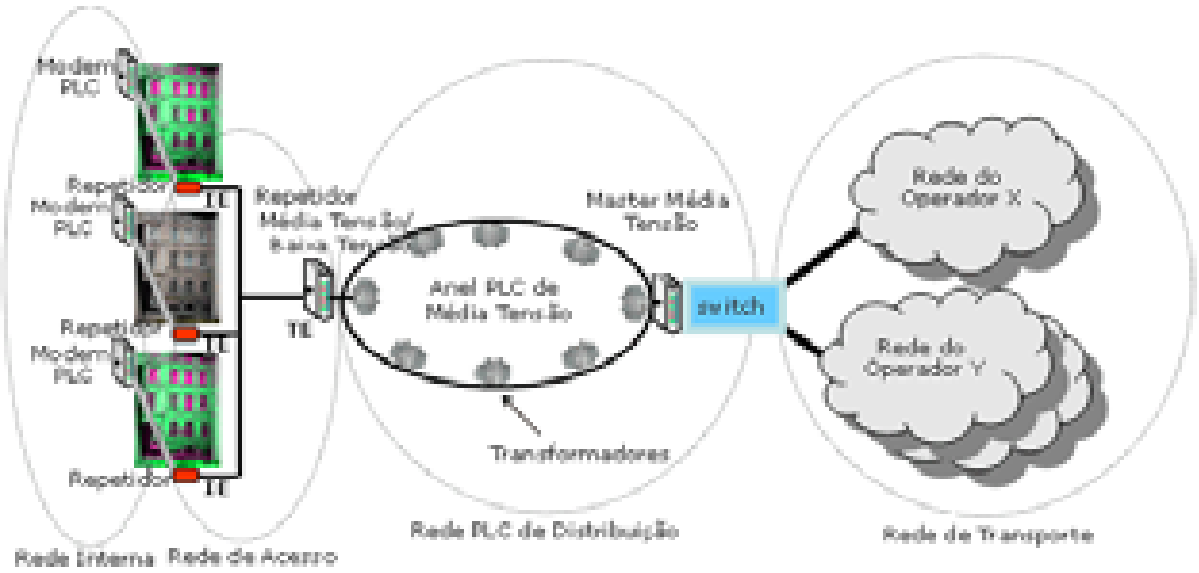

Figura 5: Topologia Básica de uma Rede PLC (RODRIGUES, 2005).

O *modem* PLC ou CPE é conectado à tomada de energia da rede de distribuição, por onde, além de ser alimentado, recebe o sinal PLC através de uma tomada simples. No *modem* existe um filtro passa alta para os sinais de dados e um filtro passa-baixa para os sinais elétricos, e normalmente possuem interfaces de comunicação RJ45 para a rede Ethernet, USB e interface RJ11 para permitir ao usuário a conexão com o equipamento de interesse.

A Fig. 5 apresenta uma topologia típica da rede PLC, com quatro níveis de rede: a rede interna do usuário final, a rede de acesso, a rede de distribuição e a rede de transporte, com a interconexão com a Internet, enquanto a Fig. 6 apresenta a topologia de uma rede de acesso PLC.

A rede interna do usuário final é constituída pela rede de distribuição elétrica nas instalações do usuário e pelos *modems* para conexão dos equipamentos que serão interligados ao serviço de banda larga.

A rede de acesso PLC se inicia junto ao medidor de energia elétrica do usuário com introdução do equipamento repetidor ou equipamento intermediário (do in-

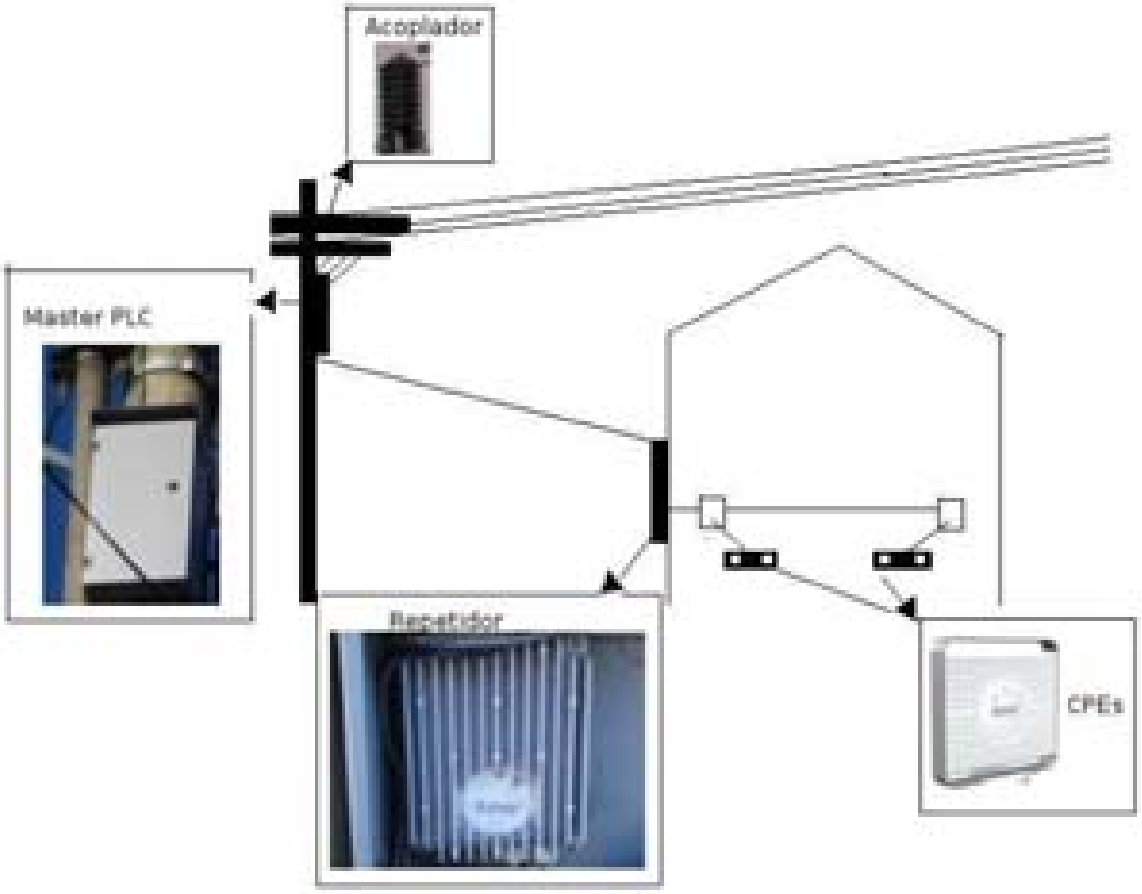

Figura 6: Topologia de Rede de Acesso PLC.

glês: *Intermediate Equipment* - IE), que recebe os sinais PLC gerados nos diversos *modems* existentes na rede, e repassa esses sinais através do medidor, o qual os reinjeta na rede de baixa tensão. A rede de acesso termina no equipamento transformador (do inglês: *Transformer Equipment* - TE), um equipamento repetidor baixa tensão / média tensão (ANDRADE; SOUZA, 2004).

A rede de distribuição PLC promove a interconexão do sinal PLC com a rede de transporte do operador de telecomunicações, através de equipamentos *master*, e segue até alcançar um ponto de acesso à rede Internet.

De acordo com Moura (2005), as redes PLC podem ser sub-divididas em dois ambientes de comunicação: *power line indoor communication* e *power line outdoor communication*. *Powerline indoor communication* é uma rede PLC existente em ambiente fechado, como por exemplo, residências, salas comerciais, laboratórios, etc. Nestes ambientes a maioria das fontes de interferência é causada, na maioria das vezes, por equipamentos de iluminação, pequenos motores e outros equipamentos elétricos de pequeno porte. A relação sinal ruído média para esse tipo de ambiente é de 35,8 dB (o sinal é aproximadamente 3.800 vezes maior que o ruído), com desvio padrão médio de 4,0 dB.

Power line outdoor communication é uma rede PLC existente em ambiente aberto. É neste tipo de ambiente que o sinal PLC trafega sobre o sistema de transmissão e distribuição de energia elétrica. O desempenho neste caso é mais afetado por descargas atmosféricas, chaveamentos, influência de banco de capacitores, transformadores e grandes motores.

A *HomePlug Powerline Alliance* desenvolveu o padrão *HomePlug*, o qual está em sua primeira versão. Este padrão define o método de acesso ao meio e especificações da camada física. Sua principal preocupação é a robustez da transmissão de dados para compensar as adversidades do canal (ALLIANCE, 2009a).

Segundo Pavlidou et al. (2003), o meio elétrico tende a ser pior que o meio sem fio em termos de atenuação e ruído. Portanto, diferentes trabalhos foram feitos

para aprimorar técnicas de modulação, de codificação e de processamento de sinais para obter altas taxas de transferência.

As características do meio elétrico como o canal de transmissão de dados foram modeladas em diferentes artigos. Em Canete et al. (2003), os autores descrevem o meio e propõem a adoção de um modelo para o canal que é função das características físicas da rede. Assim, o modelo é aplicável a qualquer cenário, desde que se conheçam o tamanho do ambiente, a quantidade de circuitos e o tipo de cabos.

Atualmente, o principal concorrente do *HomePlug* é o padrão IEEE 802.11 de redes sem fio devido ao seu sucesso comercial (CANETE et al., 2003).

3.1.3 Redes de Média Tensão

Para que seja utilizável em localidades residenciais ou comerciais, a energia elétrica proveniente da rede de transmissão é reduzida e então entregue aos consumidores através da rede de distribuição. O local onde ocorre a redução da "transmissão" para a "distribuição" é a subestação de distribuição. Podem ser citados alguns objetivos para uma subestação de distribuição:

- Reduzir a tensão de transmissão (de uma faixa de dezenas ou centenas de milhares de volts) para a tensão de distribuição (geralmente menos de 10 mil volts, que depende da norma em questão);
- Direcionar a energia elétrica para as várias cargas pelo barramento;
- Desconectar a subestação da rede de transmissão ou desligar linhas que saem da subestação de distribuição quando necessário, através de disjuntores e chaves.

Portanto, a rede de média tensão está convencionada ao que se chama de distribuição, ao contrário, por exemplo, de uma rede de alta tensão, que é enquadrada

como transmissão. Estas linhas de médio valor de tensão ligam as subestações aos postos de transformação ou ligam diferentes postos de seccionamento e transformação entre si. Podem ser aéreas ou subterrâneas. As aéreas são normalmente em cabo nu, apoiadas em postes de betão ou metálicos, e os condutores são suspensos ou apoiados por isoladores. Ambas com sentido horizontal na disposição dos cabos.

A quantidade de normas técnicas faz com que os valores atribuídos para a tensão correspondente a um valor médio difiram muito. A Norma Técnica de Distribuição 10 (NTD10) da CELG em seu glossário não define o que é média tensão, somente o que é alta e baixa tensão (RODRIGUES; SILVA, 2004). Assim sendo, por um senso comum bibliográfico os valores nominais de uma rede de média tensão seriam 13,8 kV, 23,1 kV e 34,5 kV na frequência de 60 Hz.

3.1.4 Redes de Baixa Tensão

Em um nível hierárquico abaixo da rede de média tensão encontra-se a rede de baixa tensão, como apresentado na Fig. 7, que transporta a energia elétrica dos postos de transformação, ao longo de logradouros, até os locais onde é consumida. Essas redes podem ser de dois tipos: aéreas ou subterrâneas.

As linhas aéreas podem ser em condutores nus ou isolados em feixe. As linhas em condutor nu estão fixas sobre isoladores apoiados em postes de betão, ou sobre postaletes metálicos fixos na fachada. Os cabos de distribuição de baixa tensão são normalmente constituídos por cinco condutores um dos quais se destina à iluminação pública.

Em termos de valores atribuídos à quantidade de tensão presente neste tipo de rede, a NTD 10 da CELG descreve em seu glossário que a baixa tensão é superior a 50 volts em corrente alternada ou 120 volts em corrente contínua e igual ou inferior a 1000 volts em corrente alternada ou 1500 volts em corrente contínua, entre fases ou entre fase e terra.

Porém, os valores mais utilizados são 110 V e 220 V. Em Goiás, na CELG,

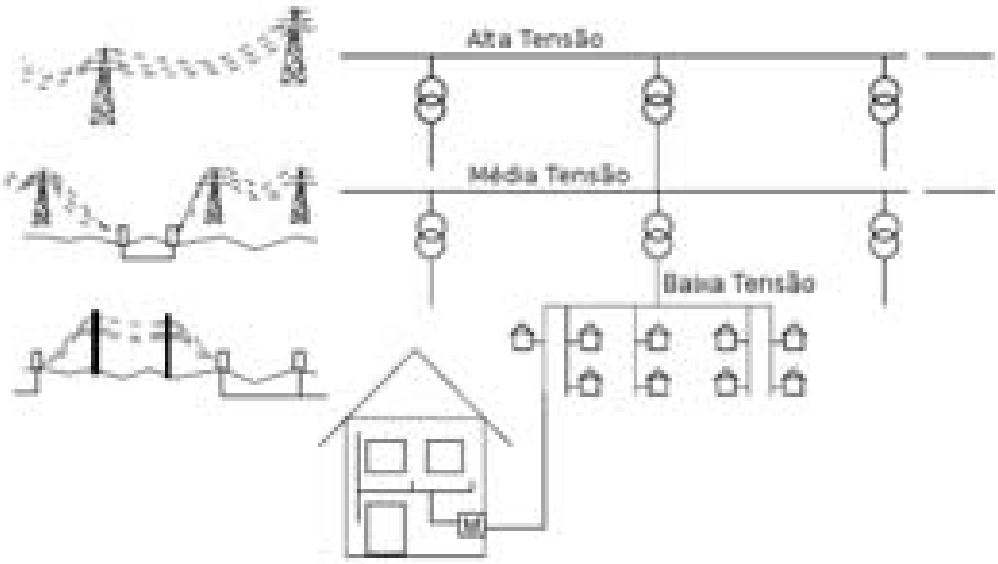

Figura 7: Redes de alta, média e baixa tensão (HRASNICA; HAIDINE; LEHNERT, 2004).

as tensões utilizadas são de 220 V e 380 V, com o sentido vertical na posição dos cabos em uma rede convencional. Em uma rede compacta os cabos são trançados uns nos outros.

Do mesmo modo que numa rede de média tensão, as decisões gerenciais tomadas em relação à instalação, manutenção e suporte de equipamentos elétricos e ativos de rede PLC devem levar em consideração os aspectos característicos desse cenário de distribuição, o que certamente impactará no perfil da equipe técnica destinada para operar esse perfil de serviço e no departamento da companhia de energia elétrica a se responsabilizar pela obra.

3.1.5 Tipos de *Chipsets*

Quando se trata do desenvolvimento e evolução na tecnologia BPL, não se pode deixar de discorrer sobre os conjuntos de *chips* (do inglês: *chipsets*) responsáveis por implementar todas as funcionalidades de nível físico até a camada de aplicação

nos equipamentos.

O *chipset* é o processador do equipamento PLC que permite altas taxas de transmissão de dados, realocação e padronização da faixa de frequência, estabilidade e todas as funcionalidades gerenciais por meio de protocolos específicos, como o protocolo SNMP (do inglês: *Simple Network Management Protocol*).

Há diversos fabricantes de *chipset* que estão na vanguarda de pesquisas voltadas para evolução da tecnologia, especificamente nas áreas de menor susceptibilidade a ruído e elevadas taxas de transmissão de dados.

Nos primórdios da tecnologia BPL a primeira geração chegou a uma taxa de transmissão de até 14 Mbps. Na segunda e atual geração pesquisas científicas em torno dos *chipsets* elevaram essa taxa para até 200 Mbps. A terceira geração já promete para o final deste ano de 2009 taxas na ordem de 400 Mbps.

Alguns dos principais fabricantes de *chipset* para tecnologia PLC são:

Lugh Networks: Empresa de Utah, Estados Unidos, responsável pela fabricação de ativos de rede BPL bem como *chipsets* para implementação nos seus próprios equipamentos;

Cogency: fabricante de *chip power line* localizada em Ottowa no Canadá;

Intellon: *Intellon Corporation's PowerPacket Chipset* é o padrão da Aliança *homePlug powerline* 1.0. Fabrica produtos PLC específicos para ambientes residenciais, BPL integrado com *bluetooth*, *streaming* de áudio e vídeo digitais e dispositivos de rede, e faz uso da tecnologia *PowerPacket*;

Enikia: desenvolve e fornece circuitos integrados para fabricantes da aliança *Home Plug* e para tecnologia PLC de acesso ou *outdoor*;

Adaptive Networks: empresa que desenvolve *chipsets* para telemetria, automação industrial e equipamentos PLC com perfil residencial;

ACTIMA: além de fabricar *chipsets*, apóia companhias de transmissão e distribuição de energia elétrica nos ramos de gestão estratégica, viabilidade e gestão de projetos;

Teamcom: empresa com mais de 50 anos de mercado na área de PNC (do inglês: *Power Network Communications*), fornece desde chips e equipamentos, consultorias em engenharia, instalação, manutenção e até mesmo financiamento de sistemas no mundo;

DS2: principal fornecedora de *chipsets* e *softwares* de tecnologia PLC tanto para baixa quanto para média tensão;

Cyan: empresa que fabrica microcontroladores de 16 e 32 *bits* para sistemas PLC e propõe soluções de integração com produtos automatizados;

Renesas: desenvolve microcontroladores PLC para AMRs, redes residenciais para utilização de eletro-eletrônicos em PLC, automação industrial, segurança e iluminação externa.

3.1.6 Padrões e Alianças PLC

O conhecimento de padrões, alianças e fóruns relacionados à tecnologia PLC/BPL é de vital relevância, pois é por meio da comunidade tecnológica que contribuições são oferecidas, problemas são solucionados e necessidades são averiguadas.

Para que o gerenciamento, em cenários hierárquicos, ocorra de modo ideal é necessário estar atualizado com as proposições dessas entidades, para não apenas contribuir, mas utilizar a tecnologia com maior e melhor aproveitamento que ela pode oferecer. As principais alianças e padrões PLC estabelecidos em diversas localidades são alistadas a seguir.

Home Plug (ALLIANCE, 2009a): *Home Plug* é o padrão norte-americano adotado para pequenas redes domésticas, que serve como adaptador entre os

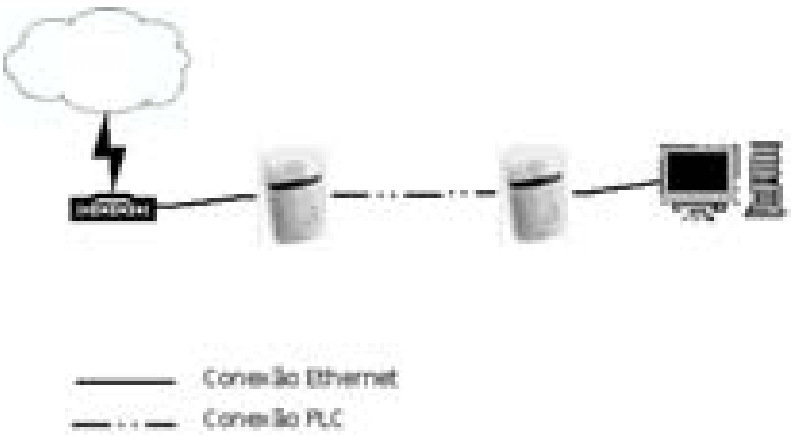

Figura 8: Rede Padrão *HomePlug*.

computadores e até mesmo entre impressoras de rede e a rede elétrica da edificação. Esses adaptadores geralmente disponibilizam taxas de transmissão de 200 Mbps com alcance de 300 m, segundo a normatização do padrão *HomePlug* 1.0. Essa aliança é formada por fabricantes tradicionais como Motorola, Sharp, LG, entre outros. A Fig. 8 apresenta uma rede *HomePlug*.

OPERA (OPERA, 2007): Aliança Européia Aberta de Pesquisa PLC (do inglês: *Open PLC European Research Alliance*). O Projeto Opera é um consórcio com 27 parceiros integrados, entre universidades, fabricantes, companhias de energia elétrica e telecomunicações, e desenvolvedores de 11 países, que provê e comparta conhecimento no desenvolvimento de soluções e testes associados à tecnologia BPL, com o objetivo de se contribuir para mais uma tecnologia de acesso e com isso cobrir regiões menos desenvolvidas, periféricas e rurais, proporcionando a inclusão digital.

ETSI (ETSI, 2009): Instituto Europeu de Padronização em Telecomunicações (do inglês: *European Telecommunication Standards Institute*). Instituto que tem contribuído para a padronização da tecnologia PLC na Europa, determina espectros de frequências específicos e regula faixas de acesso, assim como nomenclaturas para se definir o processo de amadurecimento tec-

nológico do PLC.

PLC Fórum (PLCFORUM, 2009): é uma associação internacional de líderes que representa os interesses dos fabricantes, companhias de energia elétrica e de outras organizações que desenvolvem atividades relacionadas à tecnologia PLC. Além da criação de uma rede de contatos e intercâmbio de informações entre os membros, o PLC Fórum, tem como principais objetivos questões regulamentares, processo de desenvolvimento tecnológico, estudos de caso e divulgação e propagação da tecnologia.

3.1.7 Projetos Piloto de PLC no Brasil

A tecnologia PLC começou a ser implantada pelo mundo através de projetos piloto. As concessionárias brasileiras seguiram esse caminho. A criação de projetos piloto é importante para testar a tecnologia antes de fazer o lançamento comercial desta, no intuito de evitar problemas posteriores.

De acordo com Ávila e Pereira (2007), dois dos principais projetos piloto realizados no Brasil foram os projetos pilotos PLC Barreirinhas e Restinga. O município Barreirinhas localiza-se a 240 km da capital do Maranhão, São Luiz, e foi escolhido pela Secretaria de Tecnologia da Informação do Ministério do Planejamento para sediar um projeto de inclusão digital com a participação das empresas CELG, CEMAR, EBA PLC, FITec, Samurai, FourComm e Positivo Informática. Obteve também apoio da ANATEL, da ANNEL e do SEBRAE-RJ.

Barreirinhas apresenta índice de Desenvolvimento Humano (IDH) que o coloca em 5.287^o lugar entre os municípios brasileiros. O Município, com 40 mil habitantes e 7,7 mil domicílios, possui 178 escolas com cerca de 20 mil alunos, dos quais 8 mil estão no nível médio.

Através de uma topologia de comunicação híbrida, realizou-se a integração da rede local com um canal de comunicação via satélite. No ano de 2005, a tecnologia de acesso PLC, uma dentre outras utilizadas neste projeto, teve sua aplicação

consagrada a partir da inauguração dos serviços de teleinformática nas escolas do município.

A segunda fase do projeto, intitulada "Cidades Digitais: Projeto Barreirinhas Fase 2" amplia a oferta de serviços de telecomunicações. Em colaboração com o projeto OPERA (do inglês: *Open PLC European Research Alliance*), o projeto Barreirinhas tem como objetivos a conectividade com PLC em rede multiserviço, o atendimento às necessidades prioritárias de conexão da comunidade, a avaliação dos impactos nas populações envolvidas e o subsídio ao plano diretor municipal - modelo sustentável.

O projeto piloto Restinga, desenvolvido em parceria com o Centro de Excelência em Tecnologias Avançadas (CETA-SENAI), a Companhia Estadual de Energia Elétrica do Rio Grande do Sul (CEEE), a Companhia de Processamento de Dados do Município de Porto Alegre (PROCEMPA) e a Universidade Federal do Rio Grande do Sul (UFRGS), trata da implementação de uma rede PLC em média tensão de aproximadamente 3,5 km de extensão em bairro da periferia da capital do estado do Rio Grande do Sul, distante aproximadamente 30 km do centro da cidade de Porto Alegre.

A finalidade do Projeto Piloto Restinga é ampliar a inclusão digital e levar acesso à Internet para regiões mais afastadas e menos favorecidas. Neste projeto, foram utilizados equipamentos desenvolvidos pela Mitsubishi com tecnologia DS2-Geração I, que podem atingir taxas de transmissão de dados de até 45 Mbps.

As Concessionárias Eletropaulo (São Paulo, SP) (ELETROPAULO, 2007), CELG (Goiânia, GO), CEMIG (Belo Horizonte, MG), COPEL (Curitiba, PR) e LIGHT (Rio de Janeiro, RJ) implementam as chamadas experiências piloto, todas elas com relativo sucesso.

4 Gerenciamento de Redes e o Protocolo SNMP

De acordo com Kurose e Ross (2005), o gerenciamento de redes inclui a disposição, a integração e a coordenação de elementos de *hardware*, *software* e recursos humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede a fim de satisfazer as exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.

Sendo assim, a finalidade do gerenciamento de redes é disponibilizar informações e ferramentas de verificação que possibilitem reduzir o tempo de queda ou indisponibilidade de equipamentos ou serviços de redes de comunicações.

O gerenciamento de redes é dividido em cinco funcionais.

4.1 Áreas Funcionais do Gerenciamento

O modelo funcional da arquitetura OSI (do inglês: *Open Systems Interconnection*) trabalha com requisitos de gerenciamento orientado ao usuário, e suas diversas atividades de gerenciamento de redes podem ser divididas, de acordo com a ISO, em cinco áreas funcionais específicas, conhecidas como FCAPS (*Fault Management, Configuration Mangement, Accouting Management, Performance Management e Security Management*), e que descrevem requisitos exigidos por qualquer sistema de gerenciamento de redes (MARSHALL, 1996)(STALLINGS, 1999b).

4.1.1 Gerenciamento de Desempenho

O objetivo do gerenciamento de desempenho (do inglês: *Performance Management*) é permitir o monitoramento das atividades da rede e controle dos recursos através de quantificação e medições, e possibilita a análise de taxas de erro, a análise da capacidade da rede e a obtenção de desempenho ótimo dos diferentes componentes da rede, tanto *hardware* quanto *software*. Entre esses componentes, estão dispositivos individuais, como por exemplo, enlaces e roteadores, bem como abstrações fim-a-fim, como por exemplo, um trajeto pela rede e conecta dispositivos (KUROSE; ROSS, 2005).

A gerência de desempenho compreende duas categorias principais: monitoramento (análise de atividade na rede) e controle (permite ações ou ajustes para aumentar o desempenho da rede). As três principais fontes geradoras de baixo desempenho podem ser falhas de componentes, elevadas cargas de utilização e/ou erros de configuração (STALLINGS, 1999b).

Uma regra básica adotada na avaliação de desempenho de uma rede se respalda na utilização de recursos compartilhados. Para um bom desempenho da rede, a utilização deste recurso deve ficar abaixo de um limiar. Por outro lado, um mau desempenho indica, comumente, algum gargalo num lugar específico e não, em geral, um problema generalizado de desempenho.

Uma das maiores dificuldades na medição do desempenho é eleger o indicador apropriado. Esses indicadores podem ser divididos em duas categorias: medidas orientadas a "serviços" (disponibilidade, tempo de resposta e exatidão), e medidas orientadas à "eficiência" (*throughput* e utilização), e permitem a garantia de níveis aceitáveis de desempenho na rede e uma utilização eficiente dos recursos (KUROSE; ROSS, 2005)(STALLINGS, 1999b)(ABREU; PIRES, 2005).

4.1.2 Gerenciamento de Falhas

O gerenciamento de falhas tem como objetivos registrar, detectar e reagir as condições de falha da rede. Via de regra, deve ser a primeira área a obter tratamento (KUROSE; ROSS, 2005).

Uma falha é uma condição anormal normalmente causada por operações incorretas ou um número excessivo de erros, cuja recuperação exige alguma ação de gerenciamento. O impacto e a duração do estado de falha pode ser minimizado pelo uso de componentes redundantes e rotas de comunicação alternativas (KUROSE; ROSS, 2005)(MARSHALL, 1996)(PUPAK; GOMES, 2006).

O monitoramento de cada componente é essencial para garantir o perfeito funcionamento da rede. Em caso de detecção de falhas, é importante (STALLINGS, 1999b):

- Determinar exatamente onde a falha ocorreu;
- Isolar as falhas com o uso de técnicas para diagnosticar a localização e a razão da falha, para que a rede continue a funcionar sem interferências;
- Re-configurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou;
- Reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

A supervisão de alarmes, ou procedimento de notificação ou *tracking*, consiste em uma interface do usuário que indica quais elementos estão em funcionamento, quais estão em funcionamento parcial e quais estão fora de operação. Tal interface pode ser configurada para:

- Indicar falhas visualmente, através de e-mail ou *pager*;

- Incluir níveis de severidade (com a utilização de filtros baseados em *thresholds* para gerar eventos a partir de medições);
- Indicar possíveis causas;
- Registrar ocorrências para emissão de relatórios para análise de ocorrências e avaliação sobre correlação de alarmes.

A situação ideal é que as falhas que possam vir a ocorrer em um sistema, sejam detectadas antes que os efeitos significativos decorrentes desta falha sejam percebidos. Isso pode ser conseguido através do monitoramento das taxas de erro do sistema e da evolução do nível de severidade gerado pelos alarmes (função de relatório de alarme), que permite a emissão de notificações de alarme ao gerente, que pode definir as ações necessárias para corrigir o problema e evitar que determinadas situações se tornem mais críticas (STALLINGS, 1999b).

O procedimento exposto evidencia a gerência pró-ativa, onde ações são tomadas antes da degradação da rede, procedimento este que pode ser automatizado através de técnicas de Inteligência Artificial (IA), como, por exemplo, a implementação de Agentes Autônomos (AA). Por outro lado, na gerência convencional ou reativa, sintomas são fornecidos como entrada em um sistema que oferece como saída um diagnóstico e ações são tomadas apenas após a degradação da rede.

4.1.3 Gerenciamento de Configuração

O gerenciamento de configuração tem como objetivos, o controle das configurações físicas e lógicas, a identificação de elementos e a manipulação do estado da rede, que pode ser realizada remotamente através de um console gerente (STALLINGS, 1999b).

O gerenciamento de configuração possibilita também a inicialização da rede e uma eventual desativação da mesma ou de parte dela, e promove sua manutenção, adição, atualização, a identificação dos componentes da rede, bem como a definição

da conectividade entre eles e a modificação da configuração em resposta a avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou a fim de atender as necessidades dos usuários da rede (ABREU; PIRES, 2005).

A gerência de configuração tem como principais requisitos:

- Definição, obtenção e alteração dos parâmetros de configuração dos dispositivos gerenciados;
- Definição e alteração dos relacionamentos entre os diversos dispositivos da rede;
- Distribuição e atualização de *software*;
- Configuração local ou remota.

Especificamente em relação aos dispositivos de rede, a gerência de configuração pode disponibilizar facilidades de configuração dos mesmos, usualmente através do protocolo TFTP, o que possibilita instalar novas versões de *software* de controle, como novos agentes, fazer atualização em *bulk* (vários dispositivos), fazer atualização escalonada (por exemplo, a noite) e fazer atualização automática (sem atendimento humano).

4.1.4 Gerenciamento de Contabilização

A gerência de contabilização, ou contabilidade, é a area da gerência responsável por fazer o levantamento do uso da rede o do custo de utilização da mesma. Dessa forma, é possível estabelecer custos individuais. Através da gerência de contabilidade é possível estabelecer limites de utilização da rede, como por exemplo, limite de tráfego ou de tempo de acesso (HELD, 2003).

Através dessa área funcional da gerência é possível um provedor de acesso a Internet cobrar de seu cliente um valor de acordo com a utilização da rede, e não uma mensalidade pré-definida.

É também possível estabelecer um limite de tráfego, que caso venha a ser atingido, o acesso do cliente é bloqueado. O valor cobrado pode ainda variar de acordo com o tipo de utilização da rede, ou seja, alguns recursos que geram custo maior a rede, como utilização de equipamentos mais caros, podem também ter preço diferenciado. Essa definição é possível devido a contabilização individual do usuário.

Concessionárias de energia elétrica podem também fazer uso da contabilização. O valor a ser cobrado de seus clientes depende da taxa de utilização da rede elétrica.

De acordo com Pras (1995), a gerência de contabilidade pode informar usuários do custo até o momento e custos esperados no futuro. Pode também definir limites de custo (por exemplo: desabilitar seis conexões telefônicas) e combinar custos para evitar que o usuário receba contas separadas por cada conexão individual ou, em caso de conexões internacionais, por cada país.

De acordo com (STALLINGS, 2000), alguns exemplos de recursos que podem ser gerenciados quanto a aspectos de contabilidade são:

- Ambientes de comunicação: LANs, WANs, linhas dedicadas, linhas discadas e sistemas PABX;
- *Hardware* de computador: estações de trabalho e servidores;
- *Softwares* e sistemas: aplicativos e *softwares* de servidores, *data center* e sítios para usuários;
- Serviços: inclui todas as comunicações comerciais e os serviços de informação disponíveis para usuários de rede.

A gerência de contabilidade também tem papel fundamental na escalabilidade da rede.

A contabilização permite a geração de relatórios estatísticos de utilização da mesma. Essa estatística pode ser utilizada para planejar uma possível necessidade de ampliação dos equipamentos de rede. É possível estatisticamente verificar quando a situação atual dos equipamentos não mais estará compatível com a necessidade dessa rede.

A análise dos valores coletados tem importante papel sobre a escalabilidade da rede porque caso a rede não seja ampliada com antecedência, fruto dessa análise, gargalos serão gerados, o que pode até mesmo tornar serviços e dados indisponíveis na rede.

Para um gerenciamento mais específico é necessário juntar várias informações para cada entidade. Por exemplo, para um usuário específico é possível coletar a identificação do usuário, o destinatário da transmissão, a quantidade de pacotes trafegados, o nível de segurança, intervalos de tempo das transações, o estado da rede indicando a natureza de erros ou mau funcionamento, e recursos utilizados (*hardware e software*).

4.1.5 Gerenciamento de Segurança

Gerência de segurança é o conjunto de recursos que permite ao gerente iniciar ou alterar funções que proteja a rede contra usuários com comportamentos errôneos ou acessos não-autorizados (PRAS, 1995).

Partes importantes da gerência de segurança são o gerenciamento de chaves para autorização, criptografia e autenticação, a manutenção de *firewalls* e a criação de registros de segurança.

A segurança de redes envolve basicamente cinco conceitos descritos a seguir.

Autenticação: utilizada pra verificar se o usuário que deseja realizar acesso as

informações da rede ou a algum equipamento é um usuário válido;

Autorização: realizada após a autenticação e verifica se o usuário válido também é um usuário permitido. Ser um usuário valido (existente) não significa que pode ter acesso a todas as informações e recursos disponíveis, ou seja, um controle de acesso é estabelecido através da definição de quem pode acessar o que;

Disponibilidade: a informação deve estar disponível em tempo integral;

Integridade: a informação deve chegar ao destinatário de forma íntegra, sem alteração durante a transmissão;

Confidencialidade: utilizada para garantir que a informação transmitida seja compreendida somente pelo destinatário. A confidencialidade é garantida através do uso de criptografia.

Os algoritmos criptográficos podem ser simétricos ou assimétricos, como abordado no capítulo 2.

A segurança das redes de transmissão não deve ser aplicada somente na parte lógica, mas também na parte física. É necessário garantir o acesso físico aos equipamentos da rede somente as pessoas autorizadas.

Sistemas operacionais e equipamentos de rede possuem recursos de segurança, como autenticação, autorização e criptografia. Entretanto, o gerenciamento da segurança não deve estar restrito a utilização única dessas soluções por *software*. É necessário estabelecer políticas de segurança, como senhas seguras, alteração periódica de senhas, efetivo controle de acesso, armazenamento seguro das chaves criptográficas e uso de *softwares* de verificação de segurança que procuram por vulnerabilidades.

É importante ressaltar que a segurança deve ser garantida a todos os elementos da rede, não apenas servidores. Estações de trabalho devem possuir recursos de

segurança, como *firewall* e anti-vírus. *Modems*, *switches* e roteadores também devem realizar autenticação e autorização, visto que a segurança de rede deve também garantir a disponibilidade da rede. Portanto, esses equipamentos devem estar disponíveis a todo momento.

Outro recurso que deve receber atenção quanto ao gerenciamento de segurança são os registros de eventos (*logs*). Os registros armazenam os principais eventos referentes a autenticação e autorização. Através dos *logs* é possível observar quais usuários realizaram autenticação e quais os recursos foram acessados, o que inclui tentativas mal-sucedidas.

É importante também ressaltar que a própria tarefa de gerenciamento deve ser realizada com segurança. O gerenciamento é feito em geral através de um protocolo de gerenciamento, onde SNMP (do inglês: *Simple Network Management Protocol*) é o mais utilizado. Para a utilização desse protocolo de gerenciamento é aconselhável utilizar a versão 3 que possibilita o uso de autenticação em *hash* e criptografia dos dados transmitidos.

4.2 Arquitetura de Gerenciamento

Arquiteturas cliente/servidor são caracterizadas por possuírem servidores como pontos de concentração. Portanto, os dados transmitidos ou acessados através dessa arquitetura estão concentrados nesses servidores, o que torna esses equipamentos essenciais para o bom funcionamento dessa arquitetura.

Os sistemas de gerenciamento de rede utilizam arquitetura cliente/servidor. Assim, todo o sistema de gerenciamento dependa do equipamento gerente (do inglês: *network manager*).

Um sistema de gerenciamento de redes é composto pelo gerente de rede, agentes de rede e protocolo de gerenciamento de rede. O gerente de rede é um ativo de rede que possui *software* capaz de coletar ou receber informações dos dispositivos

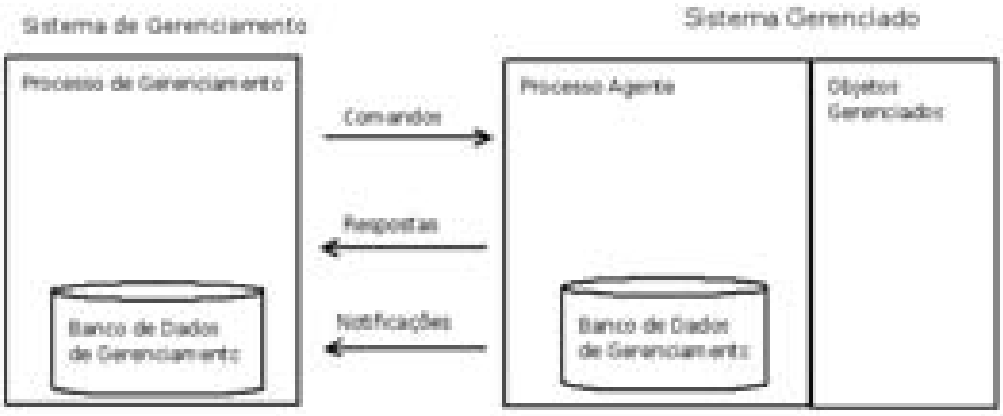

Figura 9: Modelo de Gerenciamento.

gerenciados. O agente de rede é o *software* instalado em ativo de rede que se deseja obter informações e o protocolo de gerenciamento de rede é protocolo utilizado para trocar informações de gerenciamento entre gerente e agente (STALLINGS, 2000). O modelo gerente/agente utilizado pelo gerenciamento de rede é apresentado na Fig. 9.

O sistema de gerenciamento, implementado no equipamento gerente, possui um banco de dados de informações. O banco de dados armazena as informações dos objetos gerenciados dos agentes. Os agentes possuem também o banco de dados de gerenciamento, onde armazenam os valores dos objetos gerenciados.

O gerenciamento pode ocorrer através de uma requisição feita pelo gerente ao agente. O agente, por sua vez envia ao gerente uma resposta à consulta realizada pelo gerente ou notificações ao gerente que contém valores de objetos encontrados, sem que este tenha requisitado tal informação. A notificação ocorre quando valores inesperados de objetos são encontrados pelo próprio agente.

Para garantir que o sistema de gerenciamento esteja sempre disponível, algumas arquiteturas de gerenciamento podem ser utilizadas A definição de uma arquitetura de gerenciamento deve levar em consideração a relação custo/benefício,

pois é financeiramente inviável adquirir muitos equipamentos para implementar arquiteturas dispendiosas sem necessidade. As principais arquiteturas de gerenciamento são descritas a seguir.

Centralizada: nesta arquitetura, apenas um servidor realiza todo o trabalho de gerenciamento da rede. A tarefa de gerenciamento se torna mais simples, pois há apenas um gerente a ser administrado. Como o gerenciamento da rede está concentrado em um único ponto, o servidor se torna indispensável para o sistema de gerência;

Hierárquica: nesta arquitetura, a rede é dividida em blocos, e para cada bloco existe um gerente denominado "escravo". Os gerentes escravos repassam as informações de gerenciamento para o gerente principal. Caso o gerente principal fique inoperante, o gerenciamento ainda será realizado pelos gerentes escravos, porém as informações poderão ser acessadas apenas localmente. Caso algum gerente escravo fique inoperante, somente o bloco por ele monitorado deixará de ser gerenciado;

Distribuída: assim como a gerência hierárquica, na arquitetura distribuída a rede é dividida em blocos e existe um gerente para cada bloco. Entretanto, não há dependência entre eles e não existe a figura do gerente principal. Cada gerente é responsável por monitorar bloco(s) da rede. É possível também enviar informações para um gerente superior e essa configuração não caracteriza o gerenciamento hierárquico porque o acesso as informações dos blocos não depende do gerente superior, visto que cada gerente de bloco pode disponibilizar interface própria.

Dentre as arquiteturas de gerenciamento possíveis, a combinação entre as arquiteturas hierárquica e distribuída garante maior disponibilidade de informações por possuir mais pontos de concentração (gerenciamento). Quando se tem uma topologia mais simples e com poucos equipamentos sendo gerenciados não há a necessidade de uma arquitetura tão complexa e onerosa.

4.3 O Protocolo SNMP

Os dois protocolos de gerenciamento mais conhecidos são o CMIP (do inglês: *Common Management Information Protocol*) (WARRIER et al., 1990), que surgiu a partir do modelo de referência ISO/OSI, e o SNMP (do inglês: *Simple Network Management Protocol*), que é um protocolo de aplicação da pilha TCP/IP, definido em (CASE et al., 1990).

De acordo com Stallings (1999b), o SNMP é um protocolo usado para gerenciar dispositivos de rede IP, e utiliza um banco de dados de gerenciamento, chamado MIB (do inglês: *Management Information Base*), através de nove operações SNMP, como apresentadas a seguir.

***Get*:** é a operação na qual o gerente consulta (do inglês: *pool*) o agente por alguma informação específica, como por exemplo, a quanto tempo ocorreu a última inicialização do equipamento ou quantos pacotes com erro foram recebidos através de alguma interface de comunicação de dados;

***Get-Next*:** mesmo que *get*, mas utilizado para buscar vários objetos. Realiza uma consulta a um objeto e ao receber a resposta deste, executar outra consulta pelo próximo objeto da MIB;

***Get-Bulk*:** o gerente executa uma única consulta, mas requisita valores de vários objetos nesta única consulta. Somente as versões 2 e 3 do SNMP tem suporte a esta operação;

***Set*:** é executado quando o gerente SNMP deseja modificar alguma informação específica na MIB do agente SNMP. Não são todas as informações da MIB que podem ser alteradas através da operação *set*;

***Trap ou Event*:** é uma operação assíncrona executada pelos agentes. Pode ser configurada para enviar informação ao gerente em um intervalo de tempo específico ou quando alguma situação inesperada ocorre. O formato da

Unidade de Dados do Protocolo (do inglês: *Protocol Data Unit* - PDU) é diferente, pois não há relação com um PDU anterior;

***Notification*:** mesmo que a operação *trap*, porém o formato da PDU da operação *notification* é igual ao formato de PDU de uma operação *get* ou *set*. Esta operação é suportada apenas pelas versões 2 e 3 do SNMP;

***Response*:** é o pacote que contém a resposta SNMP pela consulta feita após o recebimento de uma operação *get*;

***Report*:** parte apenas do SNMPv3, permite que máquinas SNMP possam comunicar entre si. Informações sobre problemas no processamento de mensagens são enviadas;

***Inform*:** habilita a comunicação gerente-a-gerente quando o gerenciamento distribuído é utilizado. O gerenciamento distribuído veio a ser implementado a partir da versão 2 do SNMP. Portanto, SNMP versão 1 não suporta esta operação.

O protocolo SNMP utiliza o UDP como protocolo de transporte para transmitir dados entre agentes e gerentes. A Fig. 10 apresenta como ocorre a tarefa de gerenciamento SNMP. O UDP foi escolhido, ao invés do TCP, por não ser orientado a conexão. Isso faz com que a comunicação fique mais rápida, porém menos confiável. O UDP é aconselhável em comunicações que transmitam pequenos pacotes de dados, como é o caso de uma comunicação SNMP. A porta de comunicação UDP para consultas é 161 e para o envio de *traps*, a porta utilizada é 162.

4.3.1 A Estrutura do Gerenciamento de Informações e as MIBs

De acordo com Mauro e Schmidt (2001), a Estrutura do Gerenciamento de Informações (do inglês: *Structure of Management Information* - SMI), determina como definir objetos gerenciáveis e seus comportamentos. Um agente tem uma

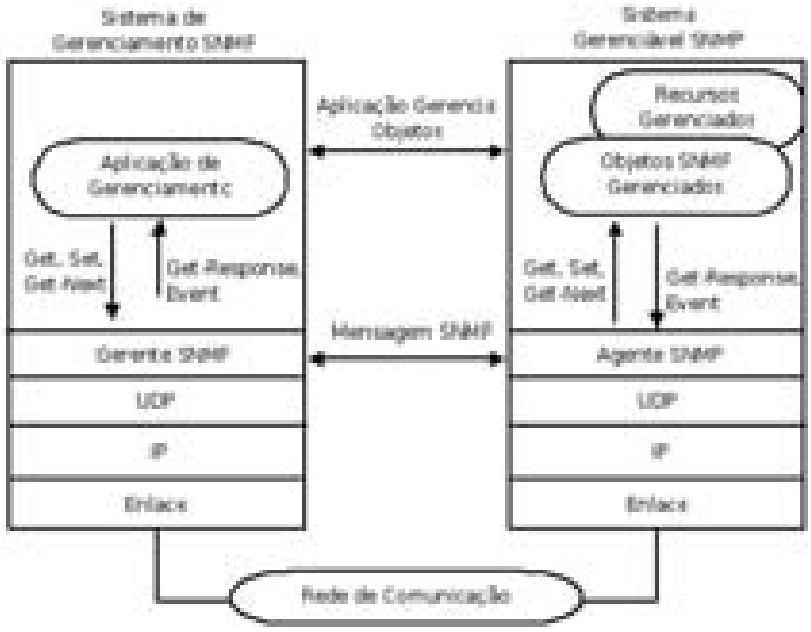

Figura 10: Comunicação SNMP.

lista de objetos que ele monitora, e este armazena em sua base de informações de gerenciamento um valor para cada objeto. Esta lista define a informação que um Sistema de Gerenciamento de Redes (do inglês: *Network Management System* - NMS) pode usar para determinar o estado da rede.

A Base de Informações de Gerenciamento (MIB), é portanto, um banco de dados que armazena os valores dos objetos da lista daquele equipamento específico. A SMI provê uma forma de definir cada objeto, enquanto a MIB é a definição do objeto. A MIB define cada objeto baseada na sintaxe SMI.

Um agente SNMP pode implementar várias MIBs, mas todos agentes implementam uma MIB chamada MIB-II, definida na RFC 1213 (MCCLOGHRIE; ROSE, 1991). O objetivo da MIB-II é definir informações de gerenciamento TCP/IP.

Cada dispositivo pode possuir objetos (ou atributos) únicos, porque algumas informações são específicas, de acordo com o fabricante e modelo. Por exemplo, dispositivos BPL possuem em uma de suas MIBs um objeto que indica a relação

sinal-ruído presente no equipamento, objeto este que não se encontra em MIBs de estações de trabalho.

4.3.2 SNMP Versão 1

O protocolo de gerenciamento SNMP teve sua versão inicial especificada em 1990 pela RFC 1157. Apesar de ser bastante antiga, ainda é a versão mais utilizada (MAURO; SCHMIDT, 2001).

A cada nova implementação desenvolvida para o protocolo SNMP, uma nova versão é padronizada, o que demonstra sua evolução. A segurança do SNMPv1 é baseada em comunidade. Cada agente SNMP possui uma comunidade definida. Para que um gerente possa consultar alguma informação do agente, é necessário que esse gerente especifique uma comunidade que tenha sido definida no agente. Caso a comunidade seja informada corretamente, o acesso ao objeto é permitido.

As versões baseadas em comunidade, como o SNMPv1, também implementa controle de acesso baseado em comunidade. É possível configurar permissões de acesso do tipo somente leitura ou leitura e escrita para uma comunidade específica. De acordo com a comunidade informada no processo de autenticação, o gerente poderá somente obter informações. Caso a comunidade informada seja com permissão de somente leitura, o gerente poderá apenas obter a resposta do valor do objeto, mas não poderá alterá-lo, caso essa operação seja permitida pela MIB. Se a comunidade informada pelo gerente for com permissão de leitura e escrita, o valor do objeto pode ser alterado, se permitido pela MIB.

A comunicação trocada entre gerente e agente SNMP é realizada através de uma mensagem SNMP. Cada mensagem inclui o número de versão, o qual indica a versão do SNMP, a comunidade utilizada na troca de informações e um dos cinco tipos de operação SNMP (*get,get-next,set,trap,response*). A Fig. 11 apresenta o formato de uma mensagem SNMP.

Os campos da mensagem SNMP (com exceção do *trap*, que tem um formato

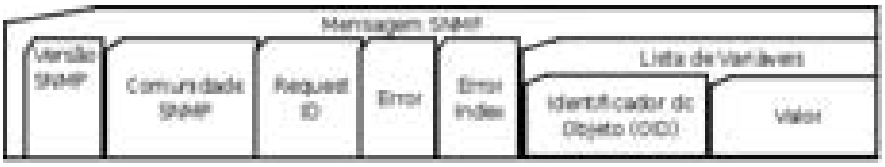

Figura 11: Mensagem SNMP.

diferente) são apresentados a seguir.

versão: versão SNMP. Para versão 1, o valor é 0;

comunidade: comunidade SNMP;

***request-id*:** número de identificação único para cada requisição;

***error-status*:** usado para indicar que uma exceção ocorreu enquanto a requisição era processada. Os valores possíveis são 0, que indica que não houve erro, 1, indica que a mensagem é muito grande, 2, indica que o valor é ilegal, 3, indica que o objeto é somente leitura e 5, para indicar um erro genérico;

***error-index*:** quando o valor de *error-status* não for zero, este campo é utilizado para indicar qual variável causou a exceção, sendo a variável uma instância de um objeto gerenciado;

lista de variáveis: sequência de variáveis;

identificador do objeto: identificador de objeto que indica um objeto específico da MIB;

valor: caso a PDU seja *set*, este campo possui o valor a ser enviado para o objeto. Se a operação for *get*, este campo é nulo. Caso seja operação *response*, este campo carrega o valor do objeto requisitado pela operação *get*.

4.3.3 SNMP Versão 2

A segurança no SNMPv2 é baseada em autenticação por comunidade. Para que as operações SNMP possam ser executadas, a autenticação por comunidade é requerida. Essa autenticação é baseada em um texto pré-definido que é transmitido em texto puro. Se um gerente SNMP deseja fazer, por exemplo, uma consulta SNMP através da operação *get*, e buscar alguma informação em um roteador, o gerente deve informar o texto da comunidade como um texto de autenticação. Se a comunidade estiver correta, então o agente responde a consulta pelo envio de uma operação SNMP *response*. Esse método de segurança é bastante falho, visto que qualquer equipamento presente na rede que que execute um *software* de captura de dados, denominado *sniffer*, é capaz de obter essa comunidade e então executar operações SNMP.

O acesso às informações de gerenciamento proporciona um amplo conhecimento da rede, como tabelas de roteamento, tráfego de rede e aplicativos em execução. O conhecimento da rede proporciona o domínio da tecnologia e permite que um invasor obtenha informações que tornam a rede vulnerável.

Além do conhecimento das informações, se uma pessoa indevida obtiver a comunidade SNMP, essa pessoa pode enviar operações *set* aos ativos de rede e alterar o comportamento destes, bem como o comportamento de todo o sistema computacional.

A versão 2 do SNMP é definida nas RFCs 1905 (CASE et al., 1996b), 1906 (CASE et al., 1996c) e 1907 (CASE et al., 1996a). O SNMPv2 possui várias sub-versões, sendo que SNMPv2c se tornou a sub-versão padrão do SNMPv2. A versão inicial do SNMPv2 nunca foi aceita, pois introduziu um novo conceito de segurança, baseado em identificadores lógicos. Então, vários grupos paralelos iniciaram o desenvolvimento das versões variantes. A versão inicial ficou conhecida como SNMPv2p. As versões variantes propostas são apresentadas a seguir. (KOZIEROK, 2005):

SNMPv1.5: trouxe de volta a segurança baseada em comunidade, mas não foi bem aceita;

SNMPv2c: bastante semelhante ao SNMPv1.5, pois utiliza autenticação baseada em comunidade. Se difere do SNMPv1.5 por padronizar em sua RFC a nova versão da estrutura de gerenciamento de informações, definida como SMIv2;

SNMPv2u: definida pelas RFCs 1909 e 1910, substitui a autenticação baseada em comunidade por autenticação baseada em usuário, mas em essência, tem o mesmo funcionamento do SNMPv2c, e por isso não foi bem aceita;

SNMPv2*: como as outras variantes, não foi bem aceita. Esta variante utiliza uma combinação das versões SNMPv2p com SNMPv2u para realizar autenticação, ou seja, união de uso de identificadores lógicos com autenticação por usuário.

A mensagem SNMPv2c é bastante semelhante a mensagem SNMPv1. O SNMPv2c foi definido desta forma para permitir compatibilidade entre as versões. Uma diferença entre as mensagens é que a PDU *trap* do SNMPv2c tem o mesmo formato da PDU *get* ou *set*. O *trap* PDU do SNMPv2c é chamado *notification* ou *SNMPv2-trap*. A outra diferença é que na PDU *getbulk* (ausente no SNMPv1), os campos *error-status* e *error-index* são substituídos por *non-repeaters* e *max-repetitions*, respectivamente.

4.3.4 SNMP Versão 3

A diferença principal entre SNMP versão 1 e 2c para o SNMP versão 3 é o fator segurança. O SNMP versão 3 traz uma implementação de segurança real. De acordo com Stallings (1999b), o SNMPv3 foi proposto em 1998 para corrigir os problemas de segurança do SNMP versões 1 e 2c. SNMPv3 implementa três serviços importantes, sendo eles autenticação, criptografia e controle de acesso.

Para realizar essas tarefas, SNMPv3 traz o conceito de "principal", que é uma entidade pela qual os serviços são providos ou onde o processamento ocorre.

O SNMPv3 é modular. Cada entidade SNMP possui uma única máquina SNMP, sendo que uma máquina SNMP implementa funções para enviar e receber mensagens, autenticar e criptografar dados, e realizar o controle de acesso.

Os módulos, ou processadores, do SNMPv3 são apresentados a seguir.

Dispatcher provê suporte a versões diferentes do SNMP. Esse processador é responsável por aceitar PDUs de de aplicações para transmití-los através da rede e entregar PDUs que chegam para as aplicações. Também é responsável por mensagens de saída para o subsistema de processamento de mensagens para preparar as mensagens, bem como o inverso, e receber as mensagens e repassá-as ao subsistema de processamento de mensagens, para que este possa extrair a PDU entrante;

Subsistema de Segurança conhecida como Modelo de Segurança do Usuário (do inglês: *User Security Model* - USM), provê os serviços de segurança, como autenticação e criptografia de mensagens (BLUMENTHAL; WIJNEN, 1999);

Subsistema de Controle de Acesso provê um conjunto de serviços de autorização que uma aplicação pode utilizar verificar permissões de acesso;

Gerador de Comando cria as PDUs de requisição *get, get-next, getbulk* e *set*, e processa as PDUs de resposta;

Receptor de Comandos recebe PDUs de requisição destinados ao sistema local, realiza o controle de acesso, e executa a devida operação de protocolo. Por fim, gera o PDU de resposta;

Gerador de Notificação monitora condições e eventos específicos do sistema, e gera *traps* ou *informs* de acordo com os valores encontrados. Deve ser configurado no sistema para onde enviar as mensagens;

Receptor de Notificação recebe notificações e gera mensagem de resposta quando uma mensagem com PDU de *inform* é recebida;

Proxy Forwarder repassa mensagens SNMP e é opcional.

O SNMPv3 é dividido em duas sub-camadas de aplicação: sub-camada de processamento do PDU e sub-camada de processamento da mensagem. A sub-camada superior é a sub-camada de processamento de PDU. Nela, a PDU é formada e indica o comando de gerenciamento, como *get, set, trap* e *inform*, e quais são as variáveis associadas. Uma vez formado ou processado o PDU, a informação é enviada para a sub-camada de processamento de mensagem. Esta camada cria o cabeçalho SNMPv3, que contém os campos de segurança relacionados a autenticação e criptografia de dados. A Fig. 12 apresenta a mensagem SNMPv3.

A autenticação é realizada através da verificação de usuário e senha. A senha é transmitida em *hash*. Existem dois algoritmos de *hash* suportados pelo SNMPv3: HMAC-MD5-96 e HMAC-SHA-96 (SCHNEIER, 1996).

O Modelo de Segurança do Usuário também executa tarefa de proteção contra atraso ou repetição de mensagens.

A etapa de privacidade do USM realiza a criptografia dos dados, para que estes não trafeguem pela rede em texto claro e aberto. DES e AES, apresentados no capítulo 2, são os dois algoritmos de criptografia suportados pelo SNMPv3.

O campo de mensagem *msgSecurityParameters* também é definido pelo USM, e suporta as funções de autenticação, proteção de tempo e privacidade.

Outra importante tarefa do USM é o gerenciamento de chaves, que define os procedimentos para geração, atualização e uso de chaves criptográficas.

No capítulo 6 serão tratados a proposta e a implementação de um equipamento conversor de versões SNMP. Para realizar essa conversão, o equipamento irá implentar parte do USM, sendo essa parte responsável por realizar apenas a criptografia dos dados. Esse tratamento será feito para que o monitoramento das

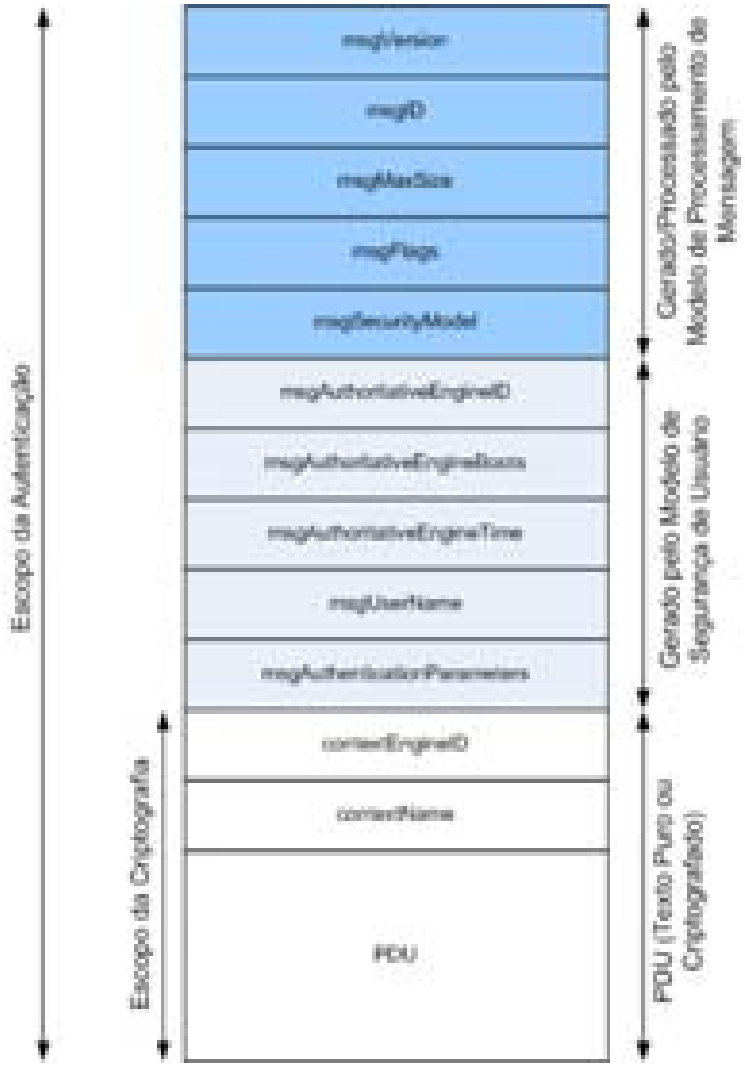

Figura 12: Mensagem SNMPv3.

redes PLC possa ocorrer de forma cifrada. O gerenciamento das redes PLC tratado ainda no capítulo 6 será realizado através do *software* Nagios, que é um *software* de código aberto e gratuito com bastante documentação e ampla utilização.

O SNMPv3 com suporte a algoritmo de criptografia AES foi padronizado na RFC 3826 em 2004 (BLUMENTHAL; MAINO; MCCLOGHRIE, 2004). Portanto, o uso do SNMPv3 com criptografia AES é um padrão de Internet relativamente novo, assim, os dispositivos de rede que suportam SNMPv3, em sua maioria, suportam apenas DES como algoritmo criptográfico.

Os agentes SNMPv3 possuem três métodos de autenticação e controle. O método *noAuthNoPriv* permite o recebimento de operações SNMP sem autenticação e não criptografa os dados. O método*authNoPriv* realiza a autenticação, mas não criptografa os dados transmitidos, enquanto o método *authPriv* realiza a autenticação e criptografa os dados. Este último é o método mais seguro.

Para demonstrar a diferença entre o gerenciamento com SNMPv2c e SNMPv3, foi executada uma consulta SNMPv2c e o tráfego foi capturado através do *software* Wireshark (WIRESHARK, 2009), como apresenta Fig. 13.

É possível notar que quando uma transmissão SNMPv2c é realizada, o pacote capturado pode ser completamente interpretado, tornando o monitoramento bastante vulnerável. Como pode ser visto, uma consulta SNMP versão 2c foi realizada na busca ao valor do objeto 1.3.6.1.2.1.1.3.0, que se refere ao objeto *sysUpTime*. Esse objeto informa a quantos milisegundos o sistema está ativo. O equipamento monitorado responde a requisição e informa o valor 29256, ou seja, informa que o sistema está ativo a 29256 milisegundos.

A captura de tráfego apresenta a falha do SNMPv2c, pois todo o tráfego pode ser capturado e visualizado por qualquer equipamento que esteja no mesmo barramento da transmissão.

A mesma consulta é realizada. Entretanto a versão 3 do SNMP é utilizada. A Fig. 14 demonstra que os dados de monitoramento são cifrados (*encryptedPDU*),

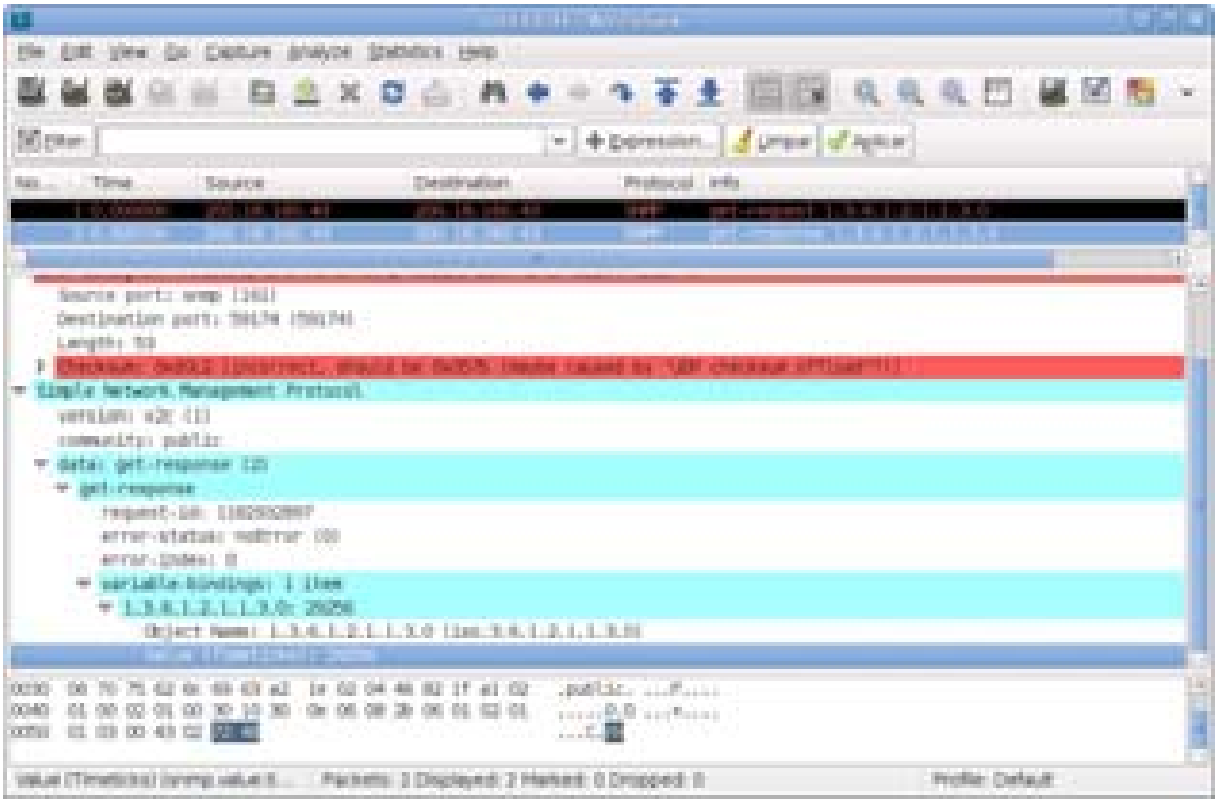

Figura 13: Captura de tráfego SNMPv2c.

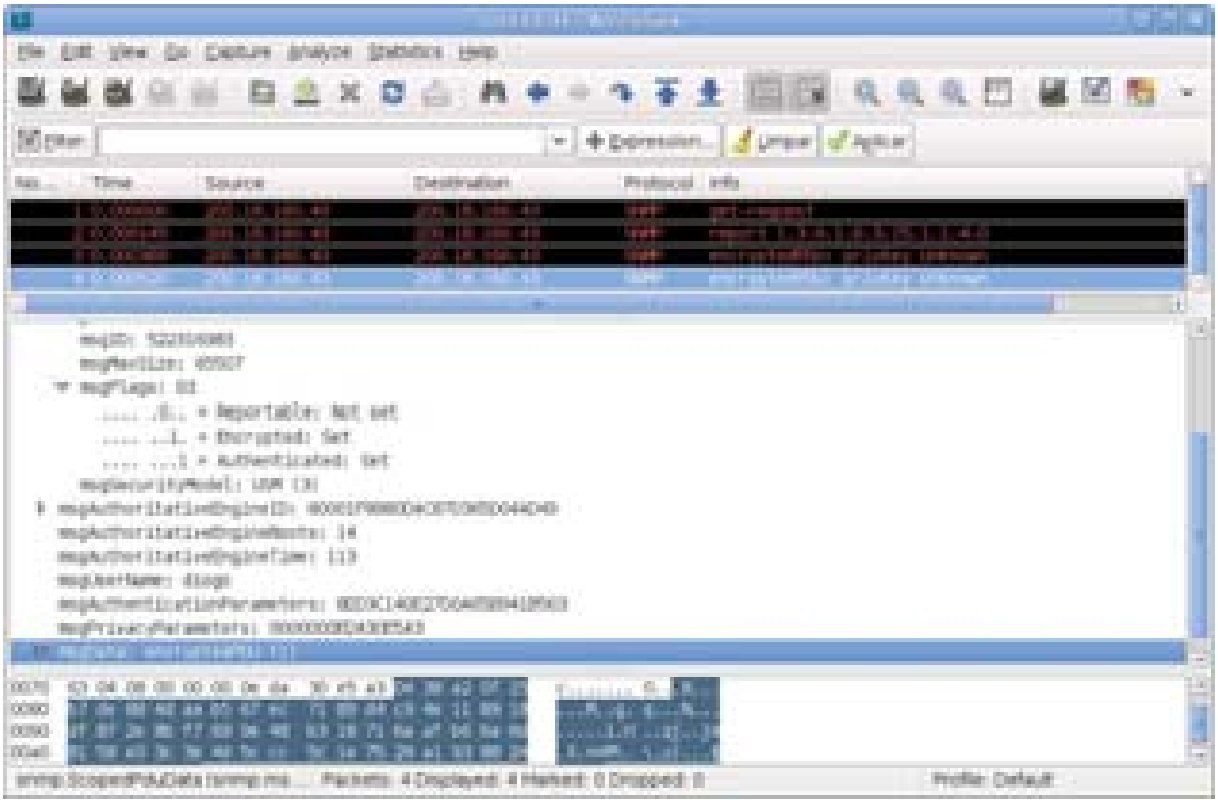

Figura 14: Captura de tráfego SNMPv3c.

e só podem ser visualizados pelo receptor e transmissor.

5 Gerenciamento com o Nagios

O Nagios é um programa de computador gratuito sob a licença GPL versão 2 (FSF, 2009) (do inglês: *General Public License*), e foi desenvolvido para os sistemas operacionais Linux ou Unix (NAGIOS, 2009).

O Nagios é uma aplicação de monitoramento de rede e sistema que verifica equipamentos e serviços desejados, e gera alarmes quando necessário. Algumas das principais características do Nagios são:

- Monitoramento de informações de rede;
- Monitoramento de equipamentos de rede;
- Criação simples de *plugins*, o que permite ao administrador desenvolver suas próprias verificações;
- Execução de *plugins* de verificação em paralelo;
- Possibilidade de criação de hierarquia através de definição de equipamentos "pais", e permite detecção e distinção entre equipamentos que estão inoperantes e equipamentos inalcançáveis;
- Envio de notificações ao responsável em caso de problemas encontrados;
- Possibilidade de definir tratadores de eventos durante o gerenciamento, o que possibilita um gerenciamento pró-ativo;

- Rotação automática dos arquivos de registro;
- Suporte a *hosts* de monitoramento redundantes;
- Interface Web para visualização de informações de rede, *status* de equipamentos, histórico de notificações, arquivos de registro, entre outros;

Existem diversas ferramentas livres com o código fonte aberto, que se enquadram, ou não, na licença GPL, e que possuem uma ou mesmo várias características do Nagios. O Nagios, além de possuir todas as funcionalidades descritas, consegue utilizá-las em grande parte das áreas funcionais do gerenciamento de redes aplicadas a redes PLC/BPL. Portanto, isso confere a este *software* uma ampla esfera de utilização quanto ao monitoramento e gerência de rede.

Algumas dessas ferramentas livres de gerenciamento, como o Cacti (CACTI, 2009), são excelentes para visualizações estatísticas, e permite, entre outras informações, uma visão do desempenho da rede no último mês e em que horário ocorreu o maior pico. O Cacti é uma ferramenta de fácil configuração e possui vários *templates* gráficos. Entretanto, este *software* deixa a desejar no gerenciamento pró-ativo de falhas. A capacidade do Cacti executar alguma tarefa quando encontrado um valor inesperado é bastante limitada. O Cacti também não possibilita a visualização de valores absolutos por ser uma ferramenta voltada para a visualização de gráficos estatísticos.

Outro *software* interessante para o gerenciamento de redes é o OpenNMS (OPENNMS, 2008). Ele é considerado um sistema de gerência completamente baseado em SNMP, bastante semelhante ao *HP OpenView Node Manager* (HEWLETT-PACKARD, 2009). Entretanto, o OpenNMS não proporciona a flexibilidade de configuração do Nagios.

O Nagios é baseado no modelo de duas camadas, conhecido como cliente/servidor, porém um pouco diferenciado de outras implementações baseadas no mesmo modelo. Por se hospedar de modo centralizado apenas no servidor e utiliza os conceitos

de gerenciamento de redes, o *software* desempenha o papel de cliente enquanto todos os outros dispositivos da rede a serem gerenciados são os servidores. Isso ocorre porque os equipamentos de rede tanto contêm como servem informações, enquanto o *host*, o cliente Nagios, as consulta.

5.1 API de Gerenciamento do Nagios

Todo o gerenciamento realizado pelo Nagios é realizado através de *plugins*. Os *plugins* são programas externos desenvolvidos em qualquer linguagem interpretada ou compilada que segue o padrão Posix (padrão de desenvolvimento utilizado para Linux/Unix) (LEWINE, 1991). Algumas linguagens muito utilizadas para a criação de *plugins* são PERL, C, Bash, Java e Python, sendo as duas primeiras as mais utilizadas.

O *plugin* deve ser desenvolvido como um programa que possa ser executado pelo sistema operacional que o armazena (Linux ou Unix), ou seja, deve funcionar como um comando que possa ser executado manualmente através de um interpretador de comandos. Este último tem a finalidade de receber um comando digitado, verificar se o comando é válido e então passar as instruções necessárias ao núcleo do sistema operacional para que essas instruções sejam executadas.

O Nagios deve então ser configurado para executar o *plugin* como se este estivesse fosse executado pela linha de comandos (interpretador de comandos). Quando algum *plugin* é executado pelo Nagios, ele aguarda as seguintes respostas:

Mensagem de Saída: mensagem que o desenvolvedor deseja exibir na interface Web apresentada pelo Nagios. É uma forma de facilitar a interpretação do monitoramento realizado. Como exemplo, pode-se imaginar o monitoramento da relação sinal-ruído em um *Master* PLC. Quando essa informação é monitorada, o *plugin* passa ao Nagios uma mensagem de saída que informa esse valor no momento da consulta.

Tabela I: Valores de Retorno do Nagios.

Código Retornado	Estado do Serviço	Estado do Equipamento
0	Normal	Rodando
1	Alerta	Rodando
2	Crítico	Inoperante/Inalcançável
3	Desconhecido	Inoperante/Inalcançável

Valor de Retorno: valor que representa o estado do serviço ou ativo monitorado. Cada valor tem significado específico para o Nagios. A Tabela I apresenta os valores de retorno do Nagios e seus respectivos significados.

Através do valor recebido, decisões podem ser tomadas pelo Nagios, como enviar *e-mail* para o responsável caso tenha sido detectado algum serviço em estado crítico, ou enviar uma mensagem de texto para o celular do responsável e informa a respeito de um dispositivo de rede inoperante.

5.2 Funcionalidades Básicas

O Nagios não depende de um servidor de páginas para que possa ser instalado e utilizado. Isto porque ele é executado como um aplicativo de segundo plano e realiza todo gerenciamento como um serviço. Os resultados obtidos através do gerenciamento podem ser visualizados em modo texto, que apesar de não apresentar uma fácil visualização, pode ser utilizado.

Entretanto uma das grandes funcionalidades do Nagios é a capacidade de disponibilizar as informações gerenciadas em interface web que podem ser visualizadas através de um programa navegador, o que facilita a tarefa de gerenciamento e visualização das informações gerenciadas.

O gerenciamento através de um navegador só é possível caso o servidor que executa o Nagios também possua um servidor de páginas, como o Apache (APACHE, 2009), capaz de executar arquivos CGI (do inglês: *Common Gateway Interface*).

Figura 15: Interface web do Nagios (NAGIOS, 2009)

.

Arquivos CGI são arquivos que possibilitam a execução de programas ou *scripts*

A Fig. 15 apresenta a interface de gerenciamento *web* do Nagios, versão 3.0rc1. Do lado esquerdo estão os *links* para monitoramento. O monitoramento pode ser feito por *hosts* (*Host Details*), por serviços (*Service Details*), dentre vários outros modos.

A interface de gerenciamento é dividida em vários CGIs, descritos a seguir.

***Status*:** utilizado para visualização do estado atual de todos os serviços e equipamentos de rede;

Mapa de *Status*: utilizado para visualização de mapas dos equipamentos da rede e identificar o *status* de cada equipamento;

Interface WAP: utilizado para apresentação do CGI *Status*, porém suportado para aparelhos celulares com serviço de acesso WAP;

Mapa de *Status* 3D: semelhante ao mapa de *status*, porém com apresentação em 3D;

Visualização Genérica Tática: permite uma visualização genérica do estado dos equipamentos e serviços de rede;

Falhas de Rede: utilizado para listar equipamentos com problemas;

Configuração: permite a visualização dos arquivos de configuração do Nagios;

Comandos: permite o envio de comandos ao programa Nagios;

Informações Estendidas: disponibiliza informações adicionais, como informações do programa Nagios e estatísticas de estados de serviços e equipamentos;

Registro de Eventos: permite a visualização dos arquivos de registro do Nagios. Arquivos de registro contém informações sobre eventos, como por exemplo, detecção de falha e horário das verificações realizadas;

Histórico de Alertas: utilizado para gerar histórico de falhas ou alertas detectados;

Notificações: contém informações das notificações enviadas. Notificações são enviadas quando alertas ou problemas críticos são encontrados;

Gráfico: utilizado para criar gráfico e representar os estados de serviços ou equipamentos em um período de tempo específico;

Relatório de Disponibilidade: utilizado para verificar a disponibilidade de um serviço ou equipamento em um intervalo de tempo desejado;

Histograma de Alerta: utilizado para criar um histograma que representa os estados de serviços ou equipamentos em um período de tempo específico;

Resumo de Alertas: apresenta um relatório genérico de alertas emitidos.

O fato do Nagios ser um *software* livre faz com que seu código fonte seja aberto, e possibilita alterações em seu código, assim como ampliações de funcionalidades.

Isso significa que há a possibilidade de inserir novas tarefas ao *software*, como por exemplo, a criação de novos CGIs complementares aos já existentes. Também é possível integrar o Nagios a um Sistema de Gerenciamento de Bancos de Dados (SGBD), a escolher entre PostgreSQL (POSTGRESQL, 2009) e MySQL (SUN, 2009).

O registro de eventos (*log* de eventos) é uma funcionalidade indispensável a qualquer sistema de gerenciamento de redes, a qual é muito bem realizada pelo Nagios. Através do registro de eventos é possível que o responsável pela rede, analise a qualquer momento dados detectados pelo *software* de gerenciamento. A análise detalhada de dados proporciona maior conhecimento da rede e possibilita um melhor planejamento quanto à escalabilidade, gerência pró-ativa e configuração da rede.

As tarefas de gerenciamento somente podem ser realizadas remotamente através da interface Web após o procedimento de autenticação. É possível configurar os tipos de monitoramento que cada usuário pode realizar, como por exemplo, usuários que somente podem visualizar as informações de monitoramento e usuários que podem alterar horários de verificações.

Quanto à segurança do tráfego da informação de monitoramento, é finalidade dos comandos externos (os *plugins*) realizarem a criptografia das informações. A segurança de acesso ao equipamento gerenciado é implementada no equipamento. Portanto, essa segurança depende do fabricante do equipamento utilizado.

6 *Proposta de Gerenciamento de Redes PLC e Implementação de Conversor de Versões SNMP*

6.1 Gerenciamento de Redes PLC

As redes PLC ainda são pouco utilizadas, pois esta tecnologia passou a transmitir dados em altas taxas apenas a partir do século XXI.

A pouca utilização da tecnologia faz com que a prática do gerenciamento das redes PLC também seja pouco utilizada, o que resulta na escassez de *softwares* voltados para o gerenciamento dessa tecnologia. Por esse motivo, esse trabalho visa apresentar uma solução de gerenciamento que foi desenvolvida voltada para redes PLC. Esse sistema de gerência de redes PLC foi desenvolvido para ser utilizado pela CELG, que firmou parceria com a Universidade Federal de Goiás (UFG) para realizar um projeto de pesquisa e desenvolvimento envolvendo o gerenciamento de redes PLC.

Este trabalho também apresenta os resultados obtidos no gerenciamento de uma rede PLC através deste sistema de gerenciamento.

O sistema de gerência desenvolvido é baseado no *software* Nagios. Entretanto,

o Nagios não é capaz de cobrir todas as áreas funcionais do gerenciamento e também não possui *plugins* específicos para o gerenciamento da tecnologia PLC.

Para realizar o gerenciamento da rede PLC foi definida a utilização do protocolo SNMP. Sendo assim, para que a gerência pudesse ser feita, foi necessário realizar um estudo das MIBs dos ativos PLC utilizados. Entretanto um dos principais objetivos desse sistema de gerência é a capacidade monitorar ativos PLC de diferentes fabricantes.

Fabricantes diferentes geralmente desenvolvem MIBs específicas. Entretanto, os principais fabricantes PLC utilizam o *chipset* DS2. Uma vez que as informações de gerenciamento são definidas no *chipset*, tem-se como resultado a mesma MIBs para equipamentos com o mesmo *chipset*, mesmo que o fabricante seja diferente.

Sendo assim, foi possível desenvolver um sistema de gerência capaz de gerenciar uma rede PLC constituída de ativos de diferentes fabricantes.

Uma vez que os ativos PLC compartilham os mesmos objetos em sua MIB, foi necessário realizar um estudo dos objetos da MIB dos ativos PLC com *chipset* DS2, para então planejar o desenvolvimento de *plugins* de gerenciamento de ativos PLC. O apêndice A apresenta a MIB DS2 (CELG, 2008a).

Algumas informações importantes específicas da MIB DS2 que podem ser analisadas são temperatura dos equipamentos (*plSysTemp.0*), relação sinal-ruído (*plPhyByMACRXSNR*), quantidade de equipamentos conectados ao *master* PLC (*plMACNumConnectedNodes*), tipo (*plSysNodeType*) e modo de funcionamento do equipamento (*plSysNodeMode*), configuração de informações de rede como Endereçamento IP (*plSysStaticIPAddress*), frequência (*plBasicCentralFrequency*), largura de banda (*plBasicBandwidth*) e qualidade de serviço (*plWiscQoS*).

Através do estudo dos objetos da MIB foi possível também relacionar quais objetos foram definidos, de acordo com a SMI, com permissão de leitura e escrita, ou seja, os objetos que permitem ter seus valores alterados através da operação *set*. Essa característica é importante para a realização do gerenciamento pró-ativo,

pois permite que quando for encontrado algum dado que represente uma situação adversa, o próprio sistema de gerência tome uma atitude, e altere o valor de algum objeto que possa normalizar o funcionamento da rede.

6.1.1 Substituição de Sistemas de Gerenciamento Proprietário

O Nagios é um sistema de gerenciamento capaz de realizar gerenciamento de contabilização, desempenho e falha, mas não é capaz de cobrir duas áreas funcionais do gerenciamento: segurança e configuração. Essas duas áreas funcionais são tão importantes quanto as outras três. Portanto, para substituir os sistemas de gerenciamento proprietários, os quais são capazes de realizar todas as áreas funcionais, foi necessário integrar soluções ao servidor Nagios que implementem essas áreas.

Para implementar essas funcionalidades foi necessário estudar o funcionamento dos ativos PLC. Através do uso de ferramentas de captura de tráfego de rede e depuração do IMS (*software* de gerenciamento proprietário da fabricante Ilevo), foi possível descobrir em detalhes como funcionam as etapas de configuração e segurança.

Os equipamentos PLC com *chipset* DS2 obtém sua configuração através de inicialização remota. Os ativos PLC, ao serem ligados, procuram por um servidor de Protocolo de Controle Dinâmico de Equipamento (do inglês: *Dynamic Host Control Protocol* - DHCP). Quando esse servidor é encontrado, as configurações de rede são obtidas através deste. Dentre as configurações, como endereçamento IP, máscara de rede, roteador, é obtido também o IP do servidor de Protocolo de Transferência de Arquivo Trivial (do inglês: *Trivial File Transfer Protocol* - TFTP), bem como o nome do arquivo de configuração a ser utilizado pelo equipamento. Desta forma, o ativo PLC obtém o arquivo de configuração do servidor TFTP. Esse arquivo possui diretivas que indicam como o ativo PLC irá trabalhar. O apêndice B apresenta o exemplo de um arquivo de configuração de um *HeadEnd*

PLC que trabalha em média tensão e implementa controle de tráfego.

Já o gerenciamento de segurança em *chipsets* DS2 é implementado através do controle de acesso. O *HeadEnd* é responsável por realizar o controle de acesso dos *modems* PLC. Pode-se permitir acesso a todos *modems* PLC, realizar controle de acesso baseado em lista de endereçamento MAC ou implementar autenticação através do Serviço de Autenticação Remota por Demanda de Usuário (do inglês: *Remote Authentication Dial In User Service* - RADIUS).

Portanto, para criar um sistema de gerenciamento de redes PLC capaz de substituir por completo as soluções proprietárias, que cubra as cinco áreas funcionais da gerência, foi necessário implementar todas as funcionalidades existentes nessas soluções proprietárias. Desta forma, fez-se necessário implementar no mesmo servidor serviços que implementem o gerenciamento de configuração e segurança. Devido a tal necessidade, foram integrados ao Nagios também os *softwares DHCP-Server (VUKSAN, 2002), TFTP-server (ANVIN, 2004)* e *FreeRadius (FREERADIUS, 2009)*, todos eles *softwares* livres e gratuitos para seguir a proposta de desenvolvimento de um sistema de gerência de redes PLC aberto.

Para possibilitar a gerência da rede PLC com segurança utilizando o SNMPv3, foi proposto um sistema embarcado baseado em microcontrolador, capaz de codificar um pacote SNMPv3 em um pacote SNMPv2c, e vice-versa. Essa proposta é apresentada na sessão "O Conversor de Versões SNMP", ainda neste capítulo.

6.1.2 Arquitetura da Rede PLC

São utilizados na rede PLC implementada tipos diferentes de equipamentos, de diferentes fabricantes, e que funcionam em modos diferentes. A tabela II apresenta os equipamentos utilizados.

A Fig. 16 apresenta o CGI *Status Map* do Nagios, o qual apresenta um mapa com o estado dos ativos PLC monitorados, bem como a relação de dependência entre eles. Este mapa proporciona uma visão geral do estado da rede como um

Tabela II: Equipamentos PLC Utilizados.

Tipo	Fabricante	Modelo	Operação	Modo	Quantidade
Master	Ilevo	ILV2010	HeadEnd	BT	2
FD	Ilevo	ILV2020	Repetidor	MT	3
FD	Ilevo	ILV2020	HeadEnd	MT	3
CPE	Ilevo	ILV201	CPE	BT	3
TD	Ilevo	ILV2010	Repetidor	BT	2
CPE	Ilevo	ILV211	CPE	BT	2
CPE	Ilevo	ILV211	CPE	BT	4
CPE	Defidev	AV200	CPE	BT	1
CPE	HomePlug	PlugLink 9650 ETH	CPE	BT	2

todo, pois através dele é possível perceber como um problema em um equipamento pode afetar toda a rede.

6.1.3 *Plugins* de Gerenciamento

Uma vez realizado o estudo dos objetos da MIB foi possível desenvolver os *plugins* a serem utilizados pelo Nagios. O *plugin* apresentado no apêndice C é um *plugin* que pode ser utilizado para qualquer objeto da MIB DS2. Ele recebe o nome do objeto a ser monitorado e dois valores que definem o estado desse objeto.

O primeiro valor é o valor limite para que o Nagios interprete o objeto monitorado como em estado normal. Caso o valor recebido esteja entre o primeiro valor e o segundo valor passado ao *plugin* este objeto é indicado como em estado de aviso. Caso o valor obtido seja maior que o segundo valor indicado, então o objeto é representado como em estado crítico.

Para automatizar a tarefa de gerenciamento da rede PLC, este *plugin* também foi desenvolvido com a capacidade de tomar decisões e melhorar o desempenho dos ativos PLC.

A MIB de *chipsets* DS2 possui um objeto definido pelo nome *plSysConfDownloadConf*, que pode ser utilizado para forçar o ativo PLC a buscar uma configuração

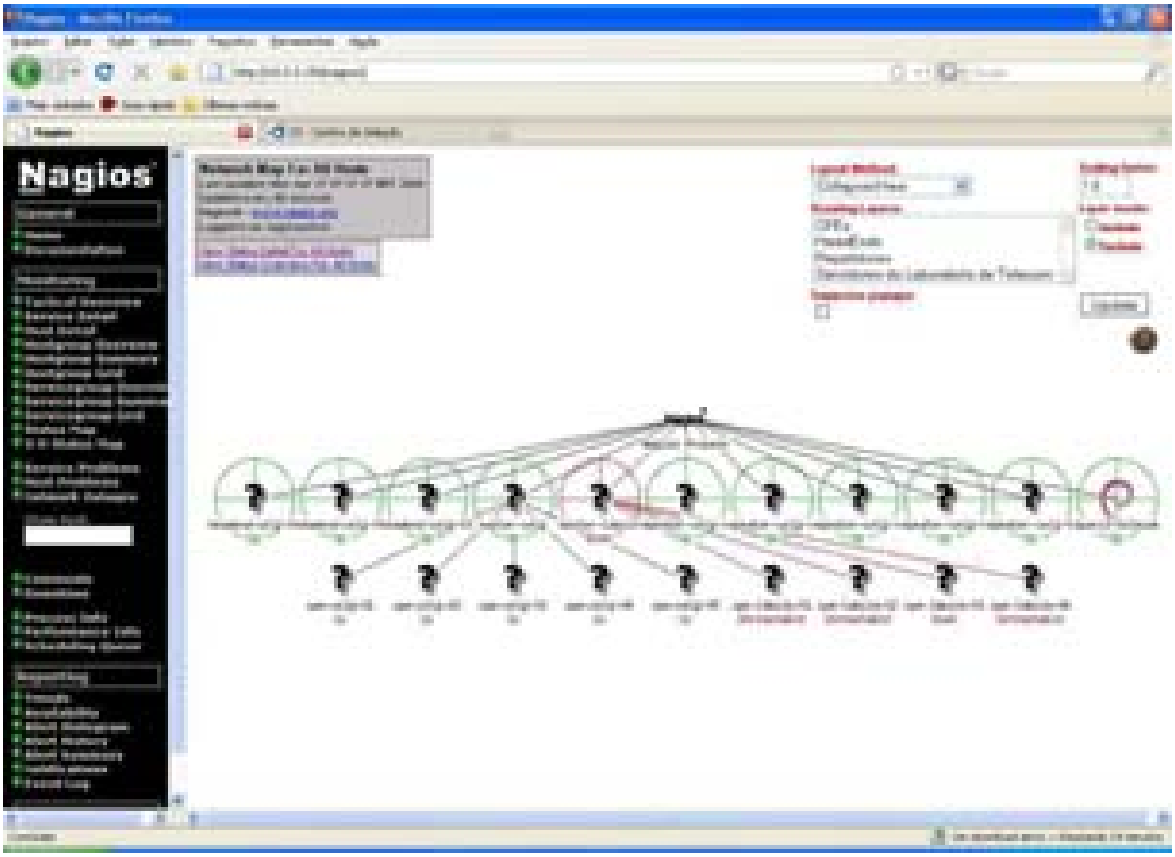

Figura 16: CGI *Status Map*.

do servidor TFTP, mesmo que esse ativo já tenha suas configurações definidas durante a inicialização (do inglês: *boot*). Através de uma operação SNMP do tipo *set*, é possível enviar a esse objeto o IP do servidor TFTP bem como o nome do arquivo contendo a configuração a ser implementada no ativo PLC. Isso fará com que o ativo PLC busque o arquivo no servidor TFTP e implemente as configurações definidas nesse arquivo.

Portanto, devido à existência do objeto *plSysConfDownloadConf*, o *plugin* apresentado no apêndice C foi desenvolvido para executar uma operação *set* e enviar ao devido ativo PLC o IP do servidor TFTP (o próprio servidor Nagios) e o nome do arquivo de configuração que altera o comportamento desse ativo e melhore seu

desempenho.

Como exemplo, é possível utilizar o *plugin* apresentado no apêndice C para analisar a relação sinal-ruído através do objeto *plPhyByMACRXSNR*. Caso o valor obtido esteja fora de um valor definido como aceitável, o *plugin* envia uma operação *set* para que o ativo busque um novo arquivo de configuração, e este arquivo deve conter a diretiva *GENERAL_SIGNAL_MODE* com um valor diferente do valor anterior do ativo. Desta forma, um novo valor de sinal será implementado ao ativo PLC, na busca de uma melhor relação sinal-ruído.

O outro *plugin* desenvolvido, apresentado no apêndice D, é utilizado para gerenciar o fluxo da rede PLC. Este *plugin* calcula como está o tráfego de rede, e caso seja detectado um fluxo acima do ideal, então é enviada uma operação *set* que informa ao concentrador PLC (como *HeadEnd*) que este deve buscar um arquivo de configuração. Este arquivo de configuração por sua vez deve conter as diretivas de controle de tráfego.

Como exemplo, considere um usuário que acessa a Internet através da rede PLC. O PC utilizado pelo usuário está conectado a um CPE. Este usuário então inicia o *download* de um arquivo muito grande, o que gera alto tráfego de dados na rede. O Nagios executa o *plugin* de controle de tráfego. Este *plugin* executa a operação *get* em busca dos objetos *plStatisticsPLCOutputPkts* e *sysUpTime*. O objeto *plStatisticsPLCOutputPkts* armazena a quantidade de pacotes que saíram da interface PLC do ativo PLC, e o objeto *sysUpTime* armazena a quantos milissegundos o ativo PLC está ligado. Entretanto, obter esses valores não proporciona dados reais do tráfego gerado pelo ativo PLC naquele exato momento. Sendo assim, os valores desses objetos obtidos na consulta anterior são utilizados. O *plugin* subtrai o valor obtido naquele momento pelo valor da última consulta, e obtém como resultado a quantidade de pacotes enviados desde a consulta anterior para a atual, e também a quantidade de milissegundos passados entre a consulta anterior e a atual. Em seguida, o *plugin* encontra a razão entre a quantidade de pacotes transmitidos e o tempo. Se essa razão entre pacotes transmitidos e tempo for

maior que 1.000 (equivalente a aproximadamente 1 Mbps), o *plugin* envia uma operação *set* ao objeto *plSysConfDownloadConf* do *HeadEnd* com o endereçamento IP do servidor TFTP e o nome de arquivo que configura o *HeadEnd* e implementa controle de tráfego através das diretivas *PROFILE_MAX_TXPUT_TX.2 = 128* e *PROFILE_MAX_TXPUT_RX.2 = 512*. Essas diretivas fazem com que o *HeadEnd* só permita a transmissão de dados a uma taxa de 128 kbps e a recepção de dados a uma taxa de 512 kbps. Deste momento em diante, o tráfego de dados é fica limitado aos valores definidos, o que evita o congestionamento da rede.

A Fig. 17 apresenta como ocorre o gerenciamento pró-ativo de ativos PLC, realizado pelo *software* Nagios. No mesmo servidor tem-se os *softwares* Nagios, DHCP-Server, TFTPd e Net-SNMP. Caso o Nagios detecte algum problema na rede ou em algum ativo, uma operação SNMP do tipo *set* é enviada para o objeto *plSysConfDownloadConf* para o ativo com problema ou para o concentrador da rede PLC, como *HeadEnd* ou repetidor. O equipamento por sua vez, busca o novo arquivo de configuração, que deve ter sido previamente armazenado no servidor TFTP. O *plugin* de monitoramento do Nagios responsável por fazer cada tipo de verificação deve ser capaz de indicar qual novo arquivo de configuração deve ser informado ao ativo PLC de acordo com o problema detectado.

6.1.4 Resultados

O Nagios monitora os equipamentos apresentados na tabela II. Através da gerência desses equipamentos alguns problemas foram detectados.

Várias caracaterísticas dos ativos da rede PLC são monitorados pelo sistema de gerência desenvolvido. A Fig. 18 apresenta alguns dos recursos monitorados em diversos CPEs, como tráfego de cada ativo (*Consulta Tráfego PLC*), quantidade de pacotes SNMP recebidos e enviados com erro (*Consulta Erros In SNMP* e *Consulta Erros Out SNMP*, respectivamente), latência de resposta (*PING*) e tentativas de consultas SNMP sem permissão (*Consulta BadCommunities*).

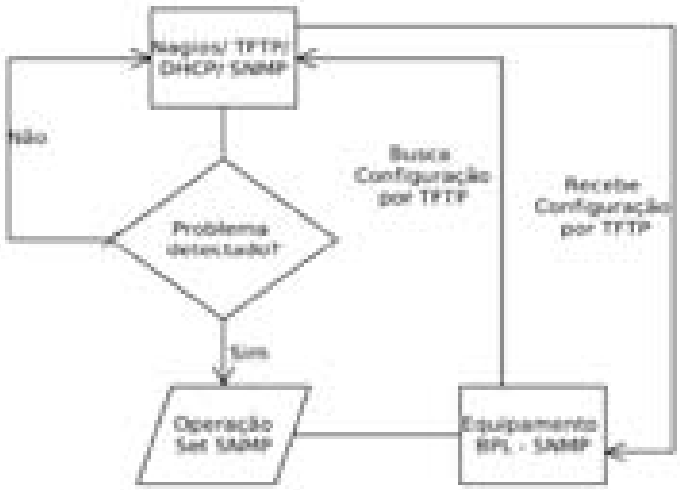

Figura 17: Fluxograma de automação do sistema de gerência.

Os mesmos recursos são monitorados em repetidores e *HeadEnds*, como apresenta a Fig. 19, acrescentando ainda o gerenciamento da informação de temperatura.

Repetidores e *HeadEnds* disponibilizam a temperatura atual em sua MIB, por se tratar de uma informação de grande importância para esses equipamentos, visto que o travamento de um desses ativos pode prejudicar parte ou até mesmo o funcionamento de toda a rede PLC.

A Fig. 19 ainda apresenta o sistema de gerência avisando que o um *HeadEnd* possui uma informação fora do estado normal. O estado apresentado é de aviso do inglês: *warning*), pois um dos gerenciamentos realizados verifica se o ativo está respondendo a consultas e ainda quanto tempo esse ativo demora para enviar a resposta. O sistema de gerência avisa que apesar do ativo estar respondendo a todas as requisições, pois nenhum pacote foi perdido ($Packet\ Loss = 0\%$), o tempo para receber a resposta desse ativo gerenciado é acima do valor esperado, que é 100 milisegundos (o tempo de resposta é de 104,86 milisegundos).

O *plugin* que realiza esse monitoramento por tempo de resposta não foi desen-

Figura 18: Gerenciamento de CPEs.

volvido, pois vem juntamente com o *software* Nagios. Apesar de ser um *plugin* de gerência pró-ativa, pois detecta uma situação desfavorável antes que ela se torne um problema, este *plugin* não executa tarefa de forma automatizada. Portanto, ele foi modificado para analisar qual é o concentrador do qual o ativo gerenciado depende, e então enviar uma operação *set* ao concentrador para que este busque um arquivo de configuração que implemente controle de banda, como o arquivo apresentado no apêndice B.

A Fig. 20 demonstra o histórico do gerenciamento do objeto relacionado à temperatura de um equipamento *HeadEnd*. Essa tela permite ao administrador visualizar em um determinado intervalo de tempo todos os estados detectados.

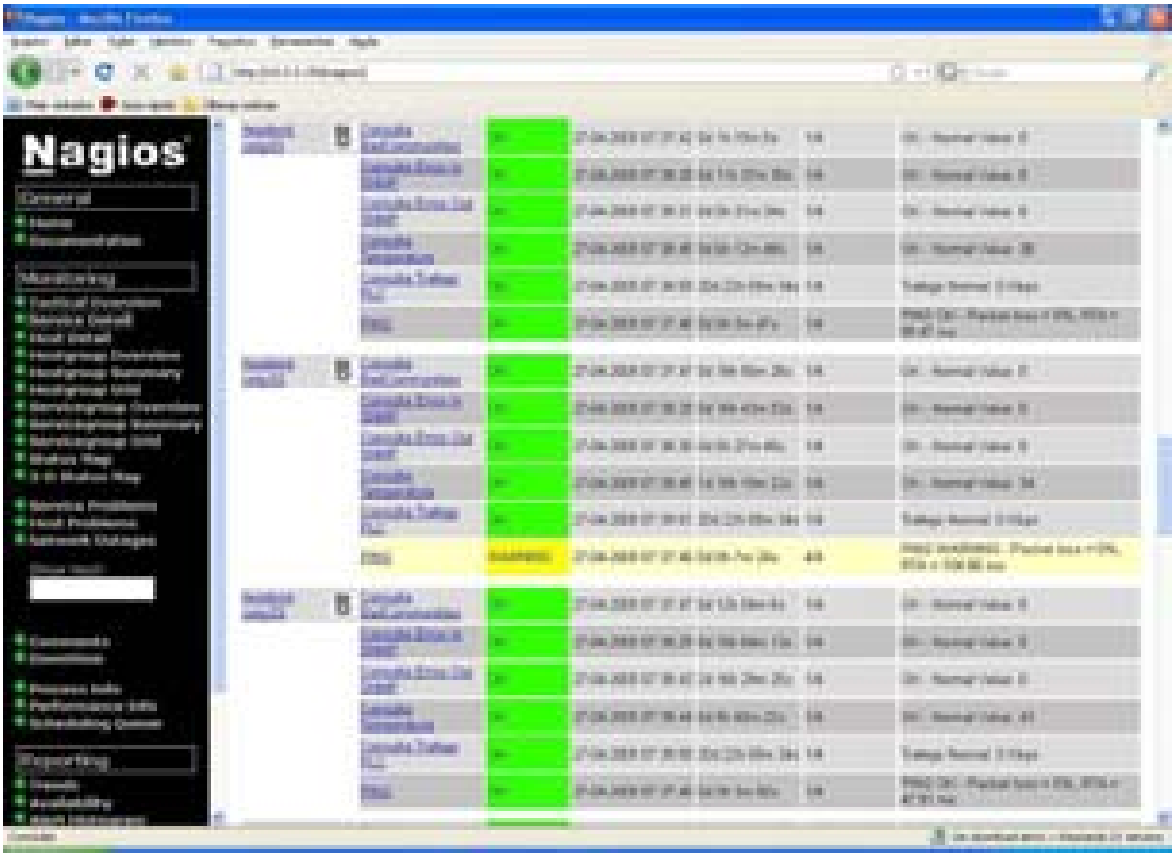

Figura 19: Gerenciamento de CPEs.

Esse *HeadEnd* atingiu estados de atenção e crítico em várias situações, o que significa que este equipamento atingiu temperaturas acima do normal, e que portanto, medidas devem ser tomadas para evitar esse aquecimento.

O gráfico apresenta resultados de monitoramento representados pelas cores verde, amarelo e vermelho. A cor verde demonstra que o equipamento estava com temperatura correta. Entretanto, em alguns momentos esse equipamento atingiu temperaturas alarmantes (cor amarela) e críticas (cor vermelha), demonstrando instabilidade no funcionamento do equipamento. Por esse motivo, esse equipamento chegou a ter seu funcionamento interrompido em vários momentos.

A detecção do problema pelo Nagios possibilitou à equipe técnica tomar con-

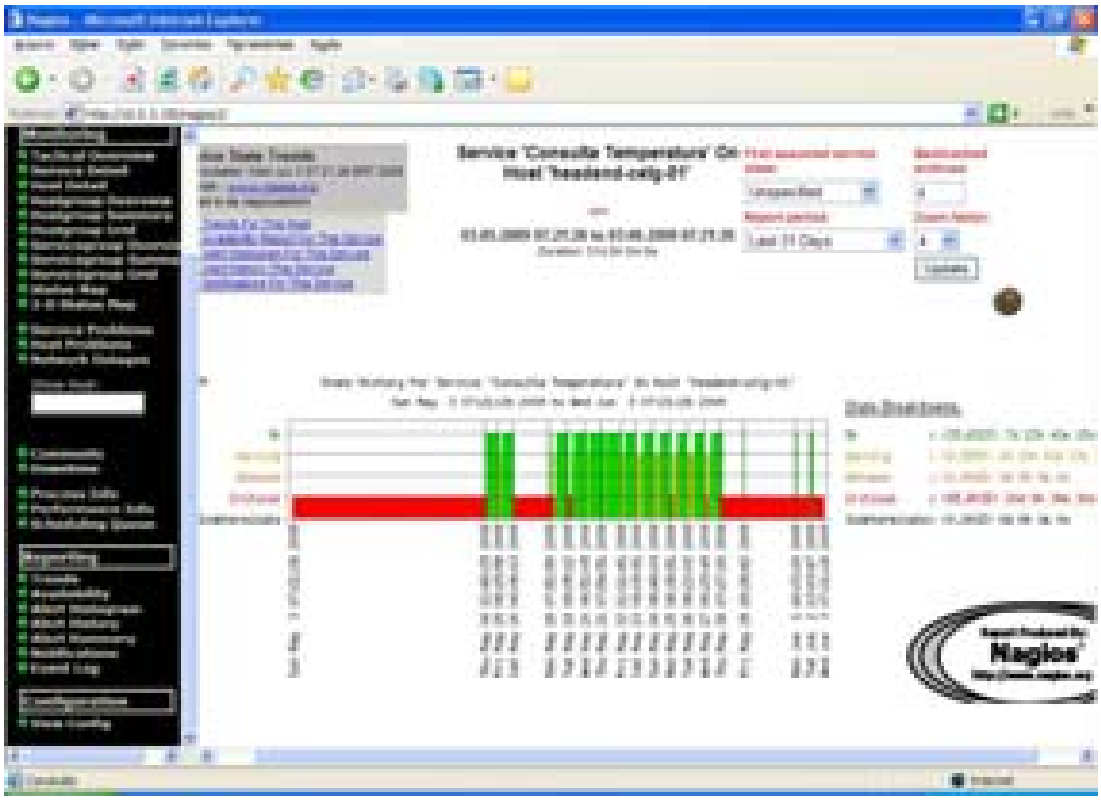

Figura 20: Aquecimento em HeadEnd.

hecimento e resolver o problema de aquecimento. A medida tomada foi a remoção do equipamento da caixa de contensão e fixado na parede, exposto ao ar. O aquecimento ocorria devido á retenção de calor causada pela caixa de contensão.

A flexibilidade do Nagios permitiu que fossem definidos os valores que classificam o estado do objeto monitorado como normal, aviso ou crítico.

O aquecimento de ativos PLC utilizados em média tensão é uma situação relativamente comum. Os ativos utilizados em média tensão, como repetidores e *HeadEnds* ficam expostos ao sol e a chuva, proporcionando o aquecimento do equipamento, e em consequência seu travamento, e permitindo também a danificação do equipamento.

6.2 O Conversor de versões SNMP

A gerência de redes PLC é realizada através do protocolo SNMP versão 2c. Como já mencionado, essa versão SNMP transmite os dados gerenciados em texto claro, sem criptografia. Para resolver esse problema, foi proposta a criação de um sistema embarcado baseado em microcontrolador PIC capaz de codificar um pacote SNMPv3 em um pacote SNMPv2c e vice-versa, e foi também implementado um simulador desse microcontrolador.

As sub-sessões subsequentes apresentam o funcionamento do microcontrolador, sua arquitetura e a simulação do mesmo.

6.2.1 Microcontroladores PIC

De acordo com (JASIO et al., 2008), a família de microcontroladores PIC é desenvolvida pela Microchip Technology Inc. Os microcontroladores PIC estão entre os mais populares, tanto em aplicações comerciais como industriais.

Ainda de acordo com (JASIO et al., 2008), a arquitetura dos microcontroladores

PIC é baseado em conjunto de instruções Harvard RISC (do inglês: *Reduced Instruction Set Computer*) modificadas com arquitetura de barramentos duplos, o que provê arquitetura flexível e proporciona uma fácil migração de um simples microcontrolador PIC de 6 pinos para um de 80 pinos, e de apenas 384 bytes de programa de memória para 128 Kbytes.

Os microcontroladores PIC estão disponíveis em várias especificações diferentes, como tipo de memória, quantidade de pinos, tamanho de memória e configurações especiais como suporte a barramento universal serial (do inglês: *Universal Serial Bus* - USB), visualização de cristal líquido (do inglês: *Liquid Crystal Display* - LCD), controle de motor, entre outros.

Uma das grandes vantagens dos microcontroladores PIC é com relação à sua portabilidade e atualização. Com relação à atualização, um programa desenvolvido para um modelo de PIC pode facilmente ser portado para outro modelo, algumas vezes até mesmo sem necessidade de modificação no código.

Todos microcontroladores PIC possuem conjunto de instruções RISC, portas digitais de entrada e saída, *reset* quando iniciado, contador de tempo, modo de economia de energia, interface de *clock* externa, memória de acesso aleatória(do inglês: *Random Access Memory* - RAM) para dados, memória de programa interna. Alguns microcontroladores PIC ainda podem possuir recursos adicionais, como canais de entrada analógica, circuitos de tempo adicionais, memória de dados externa, interrupções internas e externas, oscilador interno. Alguns PICs mais avançados podem possuir recursos mais complexos, como a interface periférica serial (do inglês: *Serial Peripheral Interface* - SPI).

Apesar dos vários recursos disponíveis em alguns PICs, algumas caracaterísticas são comumente analisadas para a escolha do microcontrolador, como quantidade de pinos de entrada e saída, periféricos necessários, quantidade mínima de memória de programa e de dados (memória RAM), necessidade de memória externa, velocidade, tamanho e custo.

Como memória de programa geralmente utiliza-se memória *flash*. Esta memória tem como finalidade armazenar o código desenvolvido para o microcontrolador. Qualquer tipo de memória permanente é gravada na memória *flash*. Atualmente é possível apagar o conteúdo da memória de programa sem nem mesmo remover o microcontrolador do circuito, através do processo denominado programação serial em circuito (do inglês: *In-Circuit Serial Programming - ICSP*). PICs atuais podem possuir até 16 Kbytes de memória *flash* interna, o que é uma grande quantidade de memória, visto que várias páginas de código podem ocupar menos que 1 Kbyte de memória de programa. Devido a existência da memória de programa, o código implementado no PIC não é perdido após uma inicialização deste microcontrolador.

A memória de dados, ou memória RAM, é utilizada para armazenar os valores voláteis, ou seja, as variáveis de programa. Ou seja, todos os dados armazenados são perdidos quando o suprimento de energia ao microcontrolador é cortado.

Os pinos de entrada e saída de dados são os pinos existentes nos microcontroladores utilizados para trocar dados. Como exemplo, um pino de entrada e saída de dados pode ser utilizado para se conectar o PIC a um *led*. Quando um sinal é enviado ao pino, então o *led* é aceso.

6.2.2 Interface Periférica Serial

A Interface Periférica Serial (do inglês: *Serial Peripheral Interface* - SPI) é uma interface utilizada para trocar dados de forma simples e rápida entre os dispositivos. O SPI é um protocolo síncrono que permite o dispositivo mestre iniciar a comunicação com o dispositivo escravo, ou secundário. O SPI é implementado em microcontroladores PIC por um módulo de *hardware* chamado Porta Serial Síncrona (do inglês: *Synchronous Serial Port*), o qual permite comunicação entre dois ou mais dispositivos a uma velocidade alta e relativa facilidade de implementação (MICROCHIP, 2009).

Por ser um protocolo síncrono, o sinal de *clock* é determinado pelo dispositivo

mestre para prover o sincronismo, e somente o mestre pode controlar a linha de *clock*, definida como SCK (do inglês: SPI *Clock*). Sendo assim, todos os escravos são controlados pelo mestre.

O SPI é um protocolo de troca de dados, o que significa que enquanto dados estão sendo enviados, dados também podem ser recebidos simultaneamente, pois são utilizados barramentos separados para transmissão e recepção. É importante ressaltar que dados estão sempre sendo trocados, ou seja, não existe um dispositivo que apenas envia dados e outro que apenas recebe.

O sinal de clock serial (do inglês: *serial clock signal* - SCK) é gerado pelo mestre e controla quando o sinal é enviado ou recebido. O barramento de entrada de dados (do inglês: *Serial Data Input* - SDI) recebe o sinal enviado pelo transmissor, enquanto o barramento de saída de dados (do inglês: *Serial Data Output* - SDO) carrega o sinal enviado até o receptor.

6.2.3 Controlador Ethernet ENC28J60

O ENC28J60 é um controlador Ethernet independente que possui interface serial SPI, completamente compatível com o padrão IEEE 802.3 e redes Ethernet com taxas de transmissão 10/100/1000 Mbps.

O ENC28J60 possui protocolo de acesso ao meio embutido, que trabalha em modo de transmissão unilateral (do inglês: *half-duplex*) e bilateral (do inglês: *full-duplex*). Ele possui também características programáveis para retransmissão automática após colisão, geração de verificação de redundância cíclica (do inglês: *Cyclical Redundance Check* - CRC) e retransmissão de pacote com erro.

A interface SPI do ENC28J60 possui *clock* de processamento de até 20 MHz. Ele possui *buffer* de 8 Kbytes para armazenar dados recebidos. Quando algum pacote é recebido, este é colocado em *buffer*. Quando o dispositivo mestre lê a informação, essa deve ser apagada do *buffer* através de instrução enviada pelo mesmo dispositivo mestre. De forma semelhante funciona o envio de pacotes para a

rede. Quando o dispositivo mestre envia um pacote, este é colocado em *buffer*. Este dispositivo mestre também deve passar instrução para que o pacote seja injetado na rede.

O ENC28J60 é necessário ao sistema embarcado para realizar a função de interface de rede, para que o PIC possa transmitir e receber dados do gerente SNMP (Nagios) e do ativo PLC gerenciado.

6.3 Proposta e Implementação de Conversor de Versões do Protocolo SNMP

Nesta sessão é apresentada a proposta de implementação do sistema embarcado para conversão de versões SNMP. Nesta sessão, e em suas sub-sessões, são apresentados um estudo da viabilidade técnica para utilização do SNMPv3 e a implementação de um simulador do equipamento conversor.

6.3.1 Estudo de Viabilidade Técnica para Utilização de SNMPv3

A utilização do SNMPv3 é importante devido à sua capacidade de autenticação e criptografia de dados. Entretanto, é necessário analisar o desempenho dos ativos de rede envolvidos e o tráfego de rede gerado pelo uso da criptografia.

Para verificar o desempenho e tráfego gerado pelo uso do SNMPv3, foram realizados testes com SNMPv2c e com SNMPv3, e então foram feitas comparações de utilização do processador, memória e tráfego de rede entre essas versões SNMP.

Entretanto, como os ativos PLC não suportam SNMPv3, os testes foram realizados em uma rede Ethernet com a estrutura apresentada na Fig. 21.

A arquitetura criada para realizar os testes é composta de seis *hosts*, onde o gerente SNMP está na mesma rede dos *hosts* PC1, *Sniffer* e Roteador. Em uma

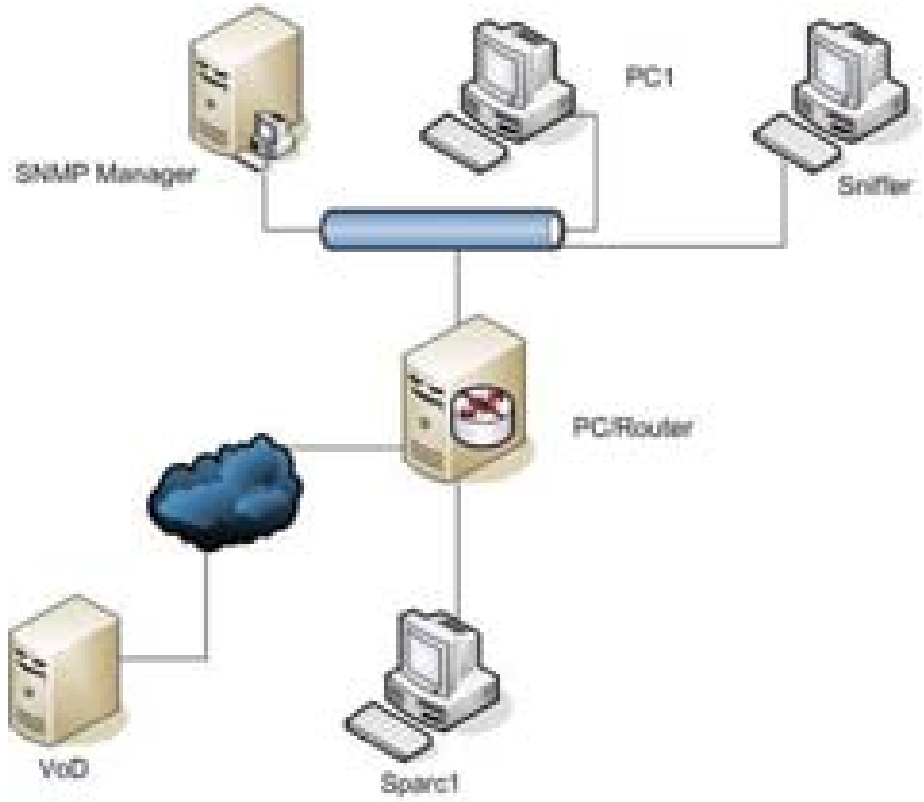

Figura 21: Arquitetura de rede de teste de gerenciamento criptográfico.

rede separada encontram-se os *hosts* de vídeo sob demanda (VoD) e Sparc1. O *host* Roteador foi utilizado para realizar o roteamento de pacotes entre as duas redes e permitir a comunicação entre elas. A tabela III apresenta suas especificações.

Tabela III: Especificações dos *hosts* da rede de teste.

Host	Sist. Operacional	*Clock* (MHz)	Memória RAM (MB)
Gerente	Linux	320	128
PC1	Windows XP	3000	512
Sniffer	Windows XP	3000	512
Roteador	Linux	3000	512
Servidor VoD	Linux	3000	3000
Sparc1	Linux	320	128

Existia uma grande preocupação com relação ao desempenho do gerenciamento

seguro dos ativos PLC após a criação do conversor, que poderia ser prejudicado pelo uso de criptografia. Apesar do gerenciamento seguro ser de extrema importância, é fundamental que esse gerenciamento ocorra com bom desempenho. Caso a velocidade no gerenciamento dos ativos fosse prejudicada devido à criptografia, algumas informações de gerência sofreriam atrasos.

O Nagios em sua versão 3, executa os *plugins* de monitoramento através de *threads*, ou seja, processos que compartilham recursos e permitem a execução simultânea de tarefas. Isso permite que vários monitoramentos sejam realizados de forma simultânea. Entretanto, vários ativos devem ser monitorados, bem como vários recursos desses ativos, o que impossibilita que todos os monitoramentos sejam executados de forma simultânea, até mesmo por limitação banda de rede.

Fez-se necessário, então, verificar qual seria o atraso causado pelo gerenciamento utilizando o SNMPv3. Entretanto, o conversor foi implementado em um *software* de simulação. A simulação não apresenta informações reais quanto à tempo de execução e resposta, pois as instruções de máquina não são passadas diretamente ao *hardware*, ou seja, o programa de simulação recebe todas as instruções e então repassa ao *hardware* associado, o que gera bastante atraso no processamento da informação. Esse é o principal motivo da utilização de uma rede Ethernet para realização dos testes, visto que os resultados de desempenho que seriam apresentados, caso fosse utilizado o simulador, não seriam próximos da realidade.

Sendo assim, foram realizados três diferentes testes para verificar o desempenho, e, portanto, a viabilidade de se utilizar o SNMPv3.

É importante lembrar que para a utilização do SNMPv3 é necessário escolher um dos métodos de controle (*noAuthNoPriv*, *authNoPriv* ou *authPriv*). Para utilizar SNMPv3 com criptografia o método utilizado deve ser *authPriv*, o qual implementa autenticação com algoritmo MD5 ou SHA, e também proporciona a cifragem dos dados através dos algoritmos DES ou AES.

O conversor de versões SNMP proposto não implementa autenticação MD5 ou SHA, pois não possui memória RAM suficiente para implementação de outro algoritmo criptográfico. Ainda assim, o MD5 é utilizado nos dois primeiros testes, enquanto o SHA é utilizado no terceiro, visto que o SNMPv3 exige o uso de um algoritmo de autenticação.

Quanto ao algoritmo de criptografia, o DES foi utilizado nos dois primeiros testes, enquanto tanto o DES quanto o AES foram utilizados no terceiro teste.

Os testes são realizados para verificar quatro características: uso de CPU, memória, tamanho dos pacotes transmitidos e a taxa de transmissão.

O primeiro teste é realizado através do monitoramento das características mencionadas durante a operação *get*, na qual o gerente busca o valor do objeto *sysDescr.0* dos ativos gerenciados. O segundo teste executa a operação *get-next*, buscando 207 objetos do ativo gerenciado. Para obter resultados mais realistas, esse teste é realizado 100 vezes, e durante essas 100 execuções o servidor de monitoramento Nagios tem seus recursos de memória RAM e processador monitorados.

Os dois primeiros testes ocorrem entre o gerente e o *host* Sparc1. Os resultados são apresentados, respectivamente, nas tabelas IV e V.

Tabela IV: Resultados da operação *get*.

Característica	SNMPv2c	SNMPv3 (MD5/DES)
Quadros	2	4
Atraso (ms)	0,75	3,7
Uso de CPU (%)	24	38
Uso de Memória (%)	1,8	1,8
Nº de Bytes Transmitidos	249	703

O sistema de gerência de redes PLC desenvolvido não realiza operações *get-next*, apenas *get* e *set*. Ainda assim, o teste envolvendo *get-next* é importante para mostrar que o resultado do teste da operação *get* que mostra a quantidade de quadros transmitidos pode gerar uma idéia errônea, pois tem-se a idéia de

Tabela V: Resultados da operação *get-next*.

Característica	SNMPv2c	SNMPv3 (MD5/DES)
Quadros	416	418
Atraso (s)	0,42	0,7
Uso de CPU (%)	24	54
Uso de Memória (%)	1,8	1,8
KBytes Transmitidos	37	77

que em uma operação SNMPv3 são transmitidos o dobro de quadros em relação a uma operação SNMPv2c, o que não é verdade. A operação SNMPv3 gera apenas 2 quadros a mais, que são utilizados para troca de informações iniciais para realização de autenticação.

O consumo de memória é o mesmo no uso de ambas as versões, entretanto, a criptografia utilizada no SNMPv3 gera maior processamento (em torno de 50% a mais) devido as operações de permutação e ou-exclusivo. Entretanto, o possível atraso gerado no processamento do pacote SNMPv3 por parte do conversor de protocolos (trabalha a 20 MHz) não gera problemas, pois tem-se um conversor para cada ativo de rede. Sendo assim, caso venha a ocorrer um atraso, será muito rápido, não afetando o gerenciamento. É importante ressaltar que apesar do *host* utilizado nos testes ter poder de processamento (320 MHz) bastante acima do microcontrolador utilizado no equipamento conversor, o desempenho do monitoramento realizado pelo *host* é prejudicado por ser realizado por *software*, enquanto o conversor é um sistema embarcado o qual passa instruções diretamente ao *hardware*, obtendo melhor desempenho.

O parâmetro "atraso" apresenta o tempo entre o envio da operação *get* e o recebimento da resposta do *host* Sparc1 através da operação *response*. Apesar de proporcionalmente o atraso gerado pelo uso do SNMPv3 frente ao SNMPv2c ser bastante superior (em torno de 50%), ainda assim é um tempo muito curto (3.7 milisegundos), que é um atraso muito baixo frente à vantagem de se utilizar um sistema de gerenciamento seguro. Da mesma forma ocorre com os *bytes* trans-

mitidos. Toda a operação de consulta SNMPv3, envolvendo o envio da operação *get* e o recebimento da operação *response* não ultrapassa 1 KByte, o que significa que nem mesmo uma fragmentação do quadro é necessária, visto que o MTU do *Ethernet* é 1.5 KBytes.

O terceiro teste é realizado através do monitoramento do consumo de processamento do servidor gerente e também do tráfego gerado na rede. Estes testes são realizados durante um período de 15 minutos para cada configuração, sendo que as configurações utilizadas foram o monitoramento através de: a) SNMPv2c; b) SNMPv3 com mecanismo SHA e criptografia DES; c) SNMPv3 com mecanismo SHA e criptografia AES. Estes testes foram realizados com o intuito de obter uma visão estatística dos resultados, sendo esses resultados apresentados nas Fig. 22 e 23. Seguindo o mesmo padrão dos dois primeiros testes, o gerenciamento utilizando SNMPv3 gera maior tráfego e consumo de processador se comparado ao SNMPv2c, entretanto este aumento não prejudica o gerenciamento, visto que um aumento em torno de 50% é viável para se obter segurança sobre as informações transmitidas.

Atavés dos resultados apresentados pelos três testes implementados, nota-se que o uso do SNMPv3 é viável e deve ser utilizado quando possível. A utilização de processador e o tráfego de rede gerados são em torno de 50% maiores que os gerados pelo SNMPv2c. Entretanto, em valores absolutos são muito bons frente à vantagem de se utilizar um sistema seguro de gerenciamento. Portanto, a implementação do sistema embarcado é tecnicamente viável.

6.3.2 Proposta de Implementação de Conversor de Versões SNMP

Os três testes realizados demonstram que a utilização do SNMPv3 para a gerência de redes é viável. Entretanto, os ativos PLC não suportam SNMPv3, apenas SNMPv2c.

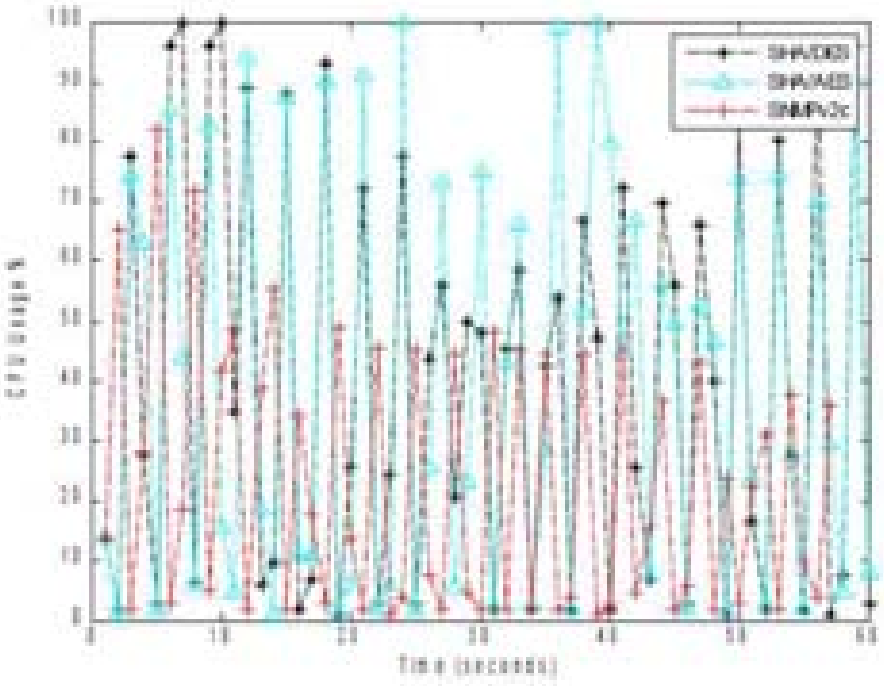

Figura 22: Utilização de processador.

Sendo assim, devido a importância de se transmitir dados de gerenciamento de forma segura, foi proposta a implementação de um sistema embarcado com microcotronlador PIC capaz de realizar a conversão de uma Unidade de Dados de Protocolo (do inglês: *Protocol Data Unit* - PDU) SNMPv2c em um PDU SNMPv3, e vice-versa.

A finalidade desse conversor não é substituir de forma completa o Modelo de Segurança de Usuário (USM), que realiza autenticação, criptografia de dados e controle de acesso. A finalidade do conversor é realizar a cifragem e decifragem dos dados, e evitar que os dados de gerenciamento não trafeguem pela rede em texto puro, sem criptografia. O algoritmo de criptografia implementado é o DES. O motivo dessa escolha, e a não implementação do AES é a limitação de memória RAM dos microcontroladores PIC.

Algumas dificuldades foram encontradas para realizar o planejamento e de-

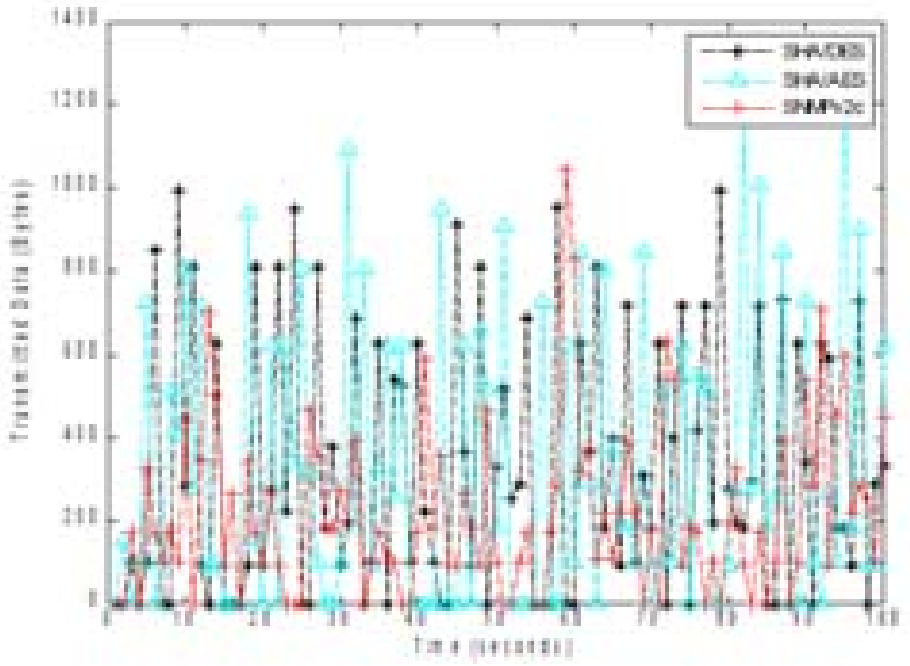

Figura 23: Tráfego de rede.

senvolvimento do conversor. A primeira dificuldade encontrada foi com relação a localização da conectividade do conversor. O servidor de gerenciamento é interligado ao equipamento concentrador como o *HeadEnd* por enlace Ethernet, que transmite os dados oriundos do servidor para os ativos PLC pela rede PLC. Sendo assim, todo o monitoramento é transmitido pela rede PLC, chegando ao ativo PLC através dessa rede.

Esta arquitetura apresenta dificuldade à implementação do conversor, pois para que o conversor ficasse localizado entre o ativo PLC e o servidor de gerência seria necessário que o conversor implementasse comunicação PLC, o que aumentaria bastante sua complexidade.

Entretanto, um ativo PLC possui duas interfaces. Uma PLC, outra Ethernet. Portanto, a utilização do ENC28J60 se apresentou como uma boa solução por possibilitar a transmissão de dados entre ativos de rede e o microcontrolador.

Portanto, a técnica adotada foi utilizar duas interfaces Ethernet ligadas ao PIC. Uma interface para comunicar com o ativo PLC e outra para transmitir dados ao ativo de rede que poderia ser conectado diretamente à interface Ethernet do ativo PLC.

Os ativos PLC funcionam no modo *bridge*, portanto os dados recebidos por uma interface são retransmitidos através da outra interface, caso o IP de destino não seja o do próprio equipamento. Devido a esse funcionamento, o gerenciamento é realizado da seguinte forma: configurar o gerente SNMP para monitorar o conversor indicando o IP deste como ativo a ser monitorado. O pacote SNMP é enviado ao ativo PLC ao qual o conversor está conectado. O ativo PLC por sua vez, repassa o pacote ao conversor. O conversor captura o pacote, processa a PDU SNMPv3 e através das informações contidas nessa PDU, ele gera uma PDU SNMPv2c. Esta PDU é enviado ao ativo PLC a ele conectado. Esse ativo processa a PDU SNMPv2c, gera a PDU SNMPv2c de resposta e envia ao conversor, que processa a PDU e cria um pacote SNMPv3 a partir das informações do pacote de resposta SNMPv2c oriundo do ativo PLC. Este pacote SNMPv3 é enviado ao gerente que recebe a PDU criptografado, decifra a mensagem e lê a resposta. O funcionamento é apresentado na Fig. 24.

Para implementar esse conversor algumas exigências quanto aos recursos do microcontrolador PIC tiveram que ser sanadas, sendo elas:

PIC família 18F: Os protocolos Ethernet, ARP, IP e UDP são essenciais para que o PIC possa transmitir e receber dados em uma rede IP. Esses protocolos implementam as funcionalidades essenciais da pilha TCP/IP para que o microcontrolador possa comunicar na rede. Esses protocolos foram aproveitados da pilha TCP/IP desenvolvida pela Microchip, pilha essa que foi portada para microcontroladores PIC. Essa pilha TCP/IP só pode ser utilizada em microcontroladores PIC família 18F ou superior. Também se torna inviável utilizar microcontroladores PIC família 24 ou 30, devido ao alto custo em grandes quantidades e complexidade de programação;

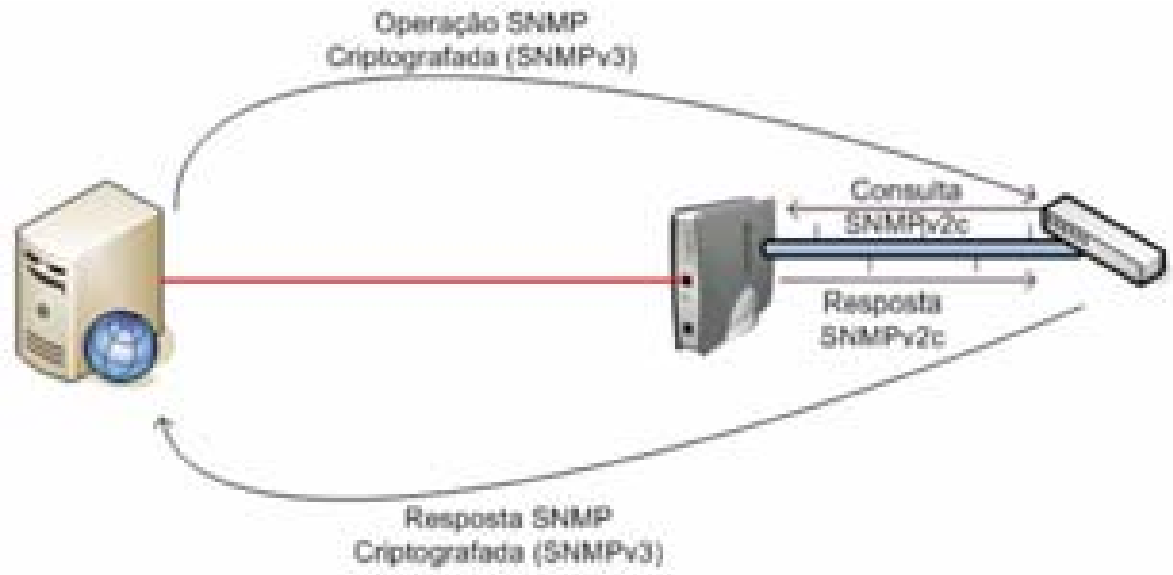

Figura 24: Arquitetura para utilização do conversor.

96 KBytes de memória de programa: o algoritmo de criptografia DES requer a criação de várias variáveis, sendo algumas delas bidiomensionais, exigindo grande quantidade de memória RAM;

2 controladores *Ethernet*: é necessário garantir que no barramento PLC trafegue apenas dados cifrados, para que esses dados não sejam interpretados por terceiros, caso o tráfego seja capturado. A comunicação sem criptografia deve ocorrer apenas na comunicação entre o equipamento conversor e o ativo PLC. Portanto, faz-se necessário a existência de um link exclusivo entre o conversor e o ativo PLC. Desta forma, é necessário que o conversor possua duas interfaces de rede. Uma que comunique diretamente ao ativo PLC e outra que comunique com outro ativo de rede, como uma estação de trabalho.

2 barramentos SPI: Os controladores *Ethernet* comunicam com o PIC através de barramento SPI. Devido a necessidade de se utilizar 2 controladores Ethernet ENC28J60, são necessários pelo menos 2 barramentos SPI;

Frente a essas exigências o PIC escolhido foi o PIC18F6627, que possui 64 pinos, 2 barramentos SPI, 96 *KBytes* de memória de programa e 3936 *Bytes* de memória RAM.

Devido a dificuldade de encontrar microcontroladores PIC família 18F com maiores recursos no Brasil, como é o caso do PIC18F6627, foi utilizado um *software* de simulação de componentes elétricos e microcontroladores PIC. Através da simulação todo o equipamento conversor pôde ser testado.

O *software* de simulação permite indicar o arquivo compilado em hexadecimal a ser gravado no microcontrolador. Isso permite testar não somente a arquitetura e o *hardware*, mas também o *software* desenvolvido. A simulação permite também associar os controladores Ethernet ENC28J60 às placas de rede físicas existentes no computador. Desta forma, é possível integrar entre o equipamento simulado com dados reais trafegados pela rede, o que permite ainda a realização de testes de conversão de versões SNMP de forma real.

O apêndice E apresenta o esquema elétrico do conversor de versões SNMP proposto utilizando PIC. Um cristal de 20 MHz é ligado ao microcontrolador, o que faz com que este trabalhe na mesma frequência do cristal. Uma fonte de alimentação de 5V é ligada ao pino MCLR (do inglês: *Master Clear*), para alimentar o microcontrolador. O cristal e a alimentação são suficientes para fazer com que o microcontrolador trabalhe.

Para implementar o conversor proposto, serão necessários dois controladores Ethernet. A tarefa de recepção e transmissão de dados na rede é realizada através do componente ENC28J60. Dois desses componentes são necessários. Um ENC28J60 é conectado aos pinos 30, 47, 34 (SPI *clock*), 35 (entrada de dados SPI), 36 (Saída de Dados SPI) e 55 do PIC. O ENC28J60 utiliza o pino SCK (SPI Clock) para realizar o sincronismo entre ele e o microcontrolador. O pino SI (entrada de dados SPI) recebe dados enviados pelo microcontrolador, enquanto o pino SO (saída de dados SPI) envia dados ao microcontrolador. O pino CS é utilizado pelo ENC28J60 para controlar qualquer operação, como transmissão e recepção. Quando uma op-

eração é realizada, o pino CS deve ser mantido em nível baixo, e deve retornar para o nível alto quando nenhuma operação estiver sendo realizada. Os pinos LEDA e LEDB são conectados a *leds* que acendem para indicar a transmissão e recepção de dados.

Outro controlador Ethernet ENC28J60 é conectado aos pinos 29, 48, 50 (SPI *clock* 2), 51 (entrada de dados SPI 2) e 52 (saída de dados SPI 2) do PIC, seguindo o mesmo funcionamento do primeiro ENC28J60.

6.3.3 Pseudo-Algoritmo do Código Implementado no Microcontrolador

O *hardware* conversor não realiza a tarefa de conversão, ele apenas proporciona a arquitetura eletrônica necessária para a solução proposta. Para realizar a conversão de versões necessita-se de um código capaz de interpretar as informações lógicas, ou dados, e então remontar a PDU SNMP na versão 2c ou 3.

O equipamento conversor de versões SNMP será patenteado por possuir uma arquitetura eletrônica inovadora, bem como seu código. A estrutura eletrônica simulada foi apresentada no apêndice E, entretanto, o código-fonte do *software* implementado no microcontrolador será preservado. Para a completa compreensão do funcionamento do conversor, o apêndice F apresenta o pseudo-algoritmo do *software*, ou seja, apenas um pequeno algoritmo explicando o funcionamento lógico do microcontrolador no tratamento dos dados de rede.

6.3.4 Resultados de Simulação

Para testar o funcionamento do simulador, foi utilizado um micro computador com duas interfaces de rede. Foram necessárias duas interfaces de rede que são associadas aos controladores Ethernet ENC28J60.

Portanto, cada controlador Ethernet ENC28J60 simulado foi associado a uma

interface de rede presente no computador.

Essa associação possibilita que todo o tráfego de rede real que chega a uma interface de rede, seja repassado ao controlador Ethernet ENC28J60 associado a essa interface física. E como resultado, os dados são encaminhados ao PIC18F6627, o que possibilita o tratamento dos pacotes.

No computador utilizado para simulação foi executado também o *software* Wireshark, que por sua vez foi configurado para capturar pacotes enviados pelo microcontrolador.

É importante perceber que o computador realizou o papel de um ativo de rede, enquanto o PIC simulado é outro ativo. O computador foi configurado com o endereçamento IP 10.0.2.199, enquanto o PIC foi configurado com o endereçamento IP 10.0.2.15.

Um segundo computador foi configurado para consultar o objeto *sysUpTime.0* do ativo 10.0.2.15 (o PIC simulado), utilizando SNMPv3.

Como foi abordado no pseudo-algoritmo, uma vez que o PIC recebe uma consulta SNMPv3 tendo seu próprio IP como destino, ele deve montar um pacote SNMP que consulta a mesma informação (*sysUpTime.0*), mas na versão 2c, e então enviar esse pacote ao ativo pré-definido como o ativo que ele deve gerenciar, que é o ativo ao qual o PIC está diretamente conectado.

Sendo assim, o PIC deve montar um pacote SNMPv2c buscando o objeto *sysUpTime.0* e enviá-lo ao computador 10.0.2.199.

Para facilitar o entendimento de cada valor, o *software* Wireshark foi utilizado para capturar o tráfego enviado pelo PIC para o computador gerenciado, como apresenta a Fig. 25.

O retângulo vermelho na parte inferior da Fig. 25 apresenta o conteúdo do pacote SNMPv2c em hexadecimal.

Ainda na Fig. 25 foram sublinhadas na cor preta, na parte superior da imagem,

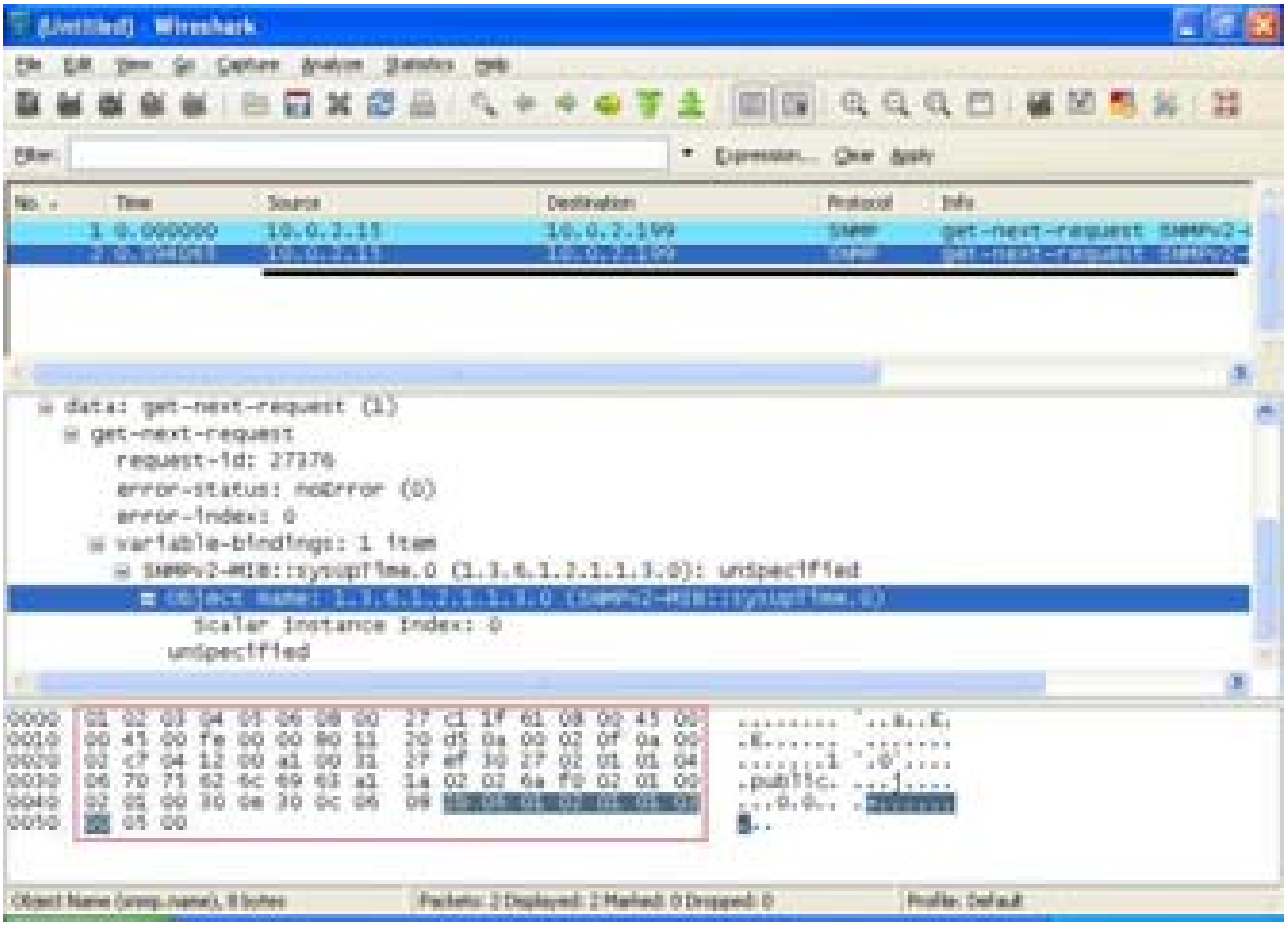

Figura 25: Captura de pacote SNMPv2c enviado pelo PIC.

as informações que mostram que o pacote recebido é um pacote do protocolo SNMP versão 2c, e que foi enviado pelo ativo com endereçamento IP 10.0.2.15 para o computador que possui o endereçamento IP 10.0.2.199.

Como resultado, tem-se que o simulador foi capaz de obter uma informação originada em SNMPv3 e então montar um pacote com a mesma informação, entretanto na versão 2c do protocolo SNMP.

7 Conclusões

Esta dissertação apresentou um sistema de gerenciamento desenvolvido especificamente para o gerenciamento de rede *Power Line Communications*. As redes PLC necessitam de um sistema de gerenciamento desenvolvidos dedicados a elas, pois esta tecnologia ainda está suscetível aos problemas de ruído e clima, o que causa falhas e degradação de desempenho.

Os equipamentos de média tensão geralmente são fixados a postes de eletricidade, tornando-os vulneráveis devido à exposição ao calor e chuva. A possibilidade de adaptação desses equipamentos em caixas de contensão os protege da chuva, mas pode aumentar a temperatura interna. Problemas causados por fatores naturais podem causar o travamento e até mesmo danificação dos equipamentos.

Outro grande empecilho ao avanço da tecnologia PLC é a estrutura elétrica existente no Brasil. As redes elétricas existentes, em sua maioria, não seguem os padrões normativos, causando ruído na transmissão dos dados, mesmo com os filtros atuais implementados nos equipamentos.

Quanto aos sistemas de gerência de redes PLC, comumente utiliza-se solições proprietárias. Esta prática não é apropriada, visto que as soluções proprietárias não permitem o gerenciamento único, que seja independente do fabricante do equipamento, e principalmente por não serem capaz de realizar o gerenciamento pró-ativo.

O gerenciamento pró-ativo foi o foco principal no desenvolvimento do sistema de gerência desenvolvido, e pôde ser implementada através da criação de *plugins*

pró-ativos e automatizados capazes de alterar configurações dos ativos PLC de forma dinâmica.

A segurança no gerenciamento dos ativos PLC se apresenta como um problema crítico, pois apenas a versão 2c do protocolo SNMP é suportada nesses equipamentos. Esta versão é bastante falha, pois transmite dados em texto puro não-cifrados. Por esse motivo, foi proposto e avaliado através de simulação um equipamento conversor de versões SNMP para permitir que a gerência da rede PLC possa ser realizada de forma segura através do uso do SNMP versão 3, o qual implementa criptografia. Ainda que futuramente sejam lançados equipamentos PLC com suporte a SNMPv3, o investimento no conversor de versões SNMP é baixo e viável. O custo de produção do conversor de versões SNMP é estimado em menos de R$ 60,00. Mesmo que os fabricantes de *chipsets* para equipamentos PLC comecem a implementar SNMPv3 nos *chipsets*, o custo de produção do equipamento conversor é menor que a troca do ativo PLC.

7.1 Trabalhos Futuros

O equipamento conversor está em fase de criação. Esse equipamento não foi apenas uma proposta, mas virá a se tornar um produto e que já está em processo de desenvolvimento. Este equipamento se mostra promissor por permitir sua utilização para várias outras finalidades, como por exemplo, um pequeno roteador embarcado.

Para ampliar a capacidade de criptografia dos dados no uso do SNMPv3, estuda-se a possibilidade de adaptação do algoritmo de criptografia AES para que este possa ser implementado no PIC18F6627.

Referências

ABREU, F.; PIRES, H. *Gerência de Redes SNMP*. Dissertação (Mestrado) — Universidade Federal Fluminense, 2005.

ALLIANCE, H. P. *HomePlug Powerline Alliance*. jun. 2009. Disponível em: <http://www.homeplug.org>. Acesso em: 31 de jul. 2009.

ALLIANCE, H. P. *Powerline Networking - The HomePlug Experience*. 2009. Disponível em: <http://www.homeplug.org/products>. Acesso em: 31 de jul. 2009.

ALMEIDA, I. L. de; SILVA, F.; MACHADO, D. C. *Critérios de Projeto de Iluminação Pública*. nov. 2006. Disponível em: <http://celgd.celg.com.br/arquivos/dadosTecnicos/normasTecnicas/NTC14.pdf>. Acesso em: 31 de jul. 2009.

ANDRADE, R.; SOUZA, R. de. *Visão Geral Sobre a Tecnologia PLC*. Tese (Doutorado) — Escola de Engenharia Elétrica da UFG, 2004.

ANEEL. *Mercado de Distribuição*. jun. 2009. Disponível em: <http://www.aneel.gov.br/area.cfm?idArea=48>. Acesso em: 31 de jul. 2009.

ANVIN, P. *TFTPd - System Users Manual*. 2004. Disponível em: <http://linuxcommand.gds.tuwien.ac.at/man_pages/tftpd8.html>. Acesso em: 31 de jul. 2009.

APACHE. *Apache HTTP Server Project*. jul. 2009. Disponível em: <http://httpd.apache.org>. Acesso em: 31 de jul. 2009.

BLUMENTHAL, U.; MAINO, F.; MCCLOGHRIE, K. *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*. jun. 2004. Disponível em: <http://www.ietf.org/rfc/rfc3826.txt>. Acesso em: 31 de jul. 2009.

BLUMENTHAL, U.; WIJNEN, B. *User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*. 1999. Disponível em: <http://www.ietf.org/rfc/rfc2574.txt>. Acesso em: 31 de jul. 2009.

BORBA, D.; SILVA, R.; ELIAS, R. *VOIP Sobre PLC*. Dissertação (Mestrado) — CEFET-GO, 2007.

BRUEY, D. *SNMP: Simple Network Management Protocol*. 2005. Disponível em: <http://www.rane.com/note161.html>. Acesso em: 31 de jul. 2009.

CACTI. *Cacti*. jul. 2009. Disponível em: <http://www.cacti.net>. Acesso em: 31 de jul. 2009.

CANETE, F. et al. Modeling and evaluation of the indoor power line transmission medium. *IEEE Communications Magazine*, p. 42–47, 2003.

CASE, J. et al. *A Simple Network Management Protocol (SNMP)*. 1990. Disponível em: <http://www.ietf.org/rfc/rfc1157.txt>. Acesso em: 31 de jul. 2009.

CASE, J. et al. *Management Information Base for Version 2 of The Simple Network Management Protocol*. jan. 1996. Disponível em: <http://www.ietf.org/rfc/rfc1907.txt>. Acesso em: 31 de jul. 2009.

CASE, J. et al. *Protocol Operations for Version 2 of The Simple Network Management Protocol*. jan. 1996. Disponível em: <http://www.ietf.org/rfc/rfc1905.txt>. Acesso em: 31 de jul. 2009.

CASE, J. et al. *Transport Mappings for Version 2 of The Simple Network Management Protocol*. jan. 1996. Disponível em: <http://www.ietf.org/rfc/rfc1906.txt>. Acesso em: 31 de jul. 2009.

CAVALIERE, F.; BANDIM, C. *Comentários Sobre o Uso de Redes de Distribuição como Meio de Comunicação de Dados*. 2007. Disponível em: <http://www.aneel.gov.br/arquivos/PDF/8 - Fábio - CEPEL.pdf>. Acesso em: 31 de jul. 2009.

CELG. *Modelo Prático de Gerência para Plataformas de Telecomunicações Envolvendo Tecnologia PLC*. Goiânia, GO, dez 2008.

CELG. *Modelo Prático de Gerência para Plataformas de Telecomunicações Envolvendo Tecnologia PLC*. Goiânia, GO, jul 2008.

CELG. *CELG - Companhia Energética de Goiás*. jun. 2009. Disponível em: <http://www.celg.com.br>. Acesso em: 31 de jul. 2009.

DOSTERT, K. *Powerline Communications*. New Jersey, EUA: Prentice Hall, 2001.

ELETROPAULO. *Eletropaulo Inicia Teste em São Paulo*. jan. 2007. Disponível em: <http://www.eletropaulotelecom.com.br/website/artigo.asp?cod=279&idi=1&id=3093>. Acesso em: 31 de jul. 2009.

ETSI. *ETSI*. jun. 2009. Disponível em: <http://www.etsi.org/WebSite/homepage.aspx>. Acesso em: 31 de jul. 2009.

FREERADIUS. *The FreeRADIUS Project*. jul. 2009. Disponível em: <http://www.freeradius.org>. Acesso em: 31 de jul. 2009.

FSF. *GNU Licenses*. mar. 2009. Disponível em: <http://www.gnu.org/licenses/>. Acesso em: 31 de jul. 2009.

GOIáS, C. E. de. *CELG Distribuição - Apresentação CELG D*. jun. 2009. Disponível em: <http://celgd.celg.com.br>. Acesso em: 31 de jul. 2009.

GOLDEN, P.; DEDIEU, H.; JACOBSEN, K. *Implementation and Applications of DSL Technology*. New York, EUA: Taylor and Francis Group, 2008.

HAYKIN, S. *Digital Communications*. New Jersey, EUA: John Wiley and Sons, 1988.

HELD, G. *Ethernet Networks: Design, Implementation, Organization and Management*. 4. ed. New Jersey, EUA: John Wiley and Sons, 2003.

HELD, G. *Understanding Broadband over Power Line*. New York, EUA: Auerbach Publications, 2006.

HEWLETT-PACKARD. *HP OpenView*. jul. 2009. Disponível em: <http://www.openview.hp.com>. Acesso em: 31 de jul. 2009.

HRASNICA, H.; HAIDINE, A.; LEHNERT, R. *BroadBand Powerline Communications - Network Design*. New Jersey, EUA: John Wiley and Sons, Ltd, 2004.

JASIO, L. D. et al. *PIC Microcontrollers - Know It All*. Missouri, EUA: Elsevier, 2008.

KOZIEROK, C. *TCP/IP Internet Standard Management Framework and SNMP Versions (SNMPv1, SNMPv2 Variants, SNMPv3)*. 2005. Disponível em: <http://www.tcpipguide.com/free/t_TCPIPInternetStandardManagementFrameworkandSNMPVer-3.htm>. Acesso em: 31 de jul. 2009.

KUROSE, J.; ROSS, K. *Redes de Computadores e a Internet. Uma nova Abordagem*. 3rd. ed. São Paulo, SP: Pearson Education, 2005.

LEE, J.-J. et al. Power line communication network trial and management in korea. *International Journal of Network Management*, v. 16, 2006.

LEWINE, D. *Posix Programmers Guide*. California, EUA: OŔeilly, 1991.

MARSHALL, R. *The Simple Book: An Introduction to Networking Management of TCP/IP-based internets. Revised Second Edition*. New Jersey, EUA: Prentice Hall, 1996.

MAURO, D.; SCHMIDT, K. *Essential SNMP*. California, EUA: OŔeilly, 2001.

MCCLOGHRIE, K.; ROSE, M. *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. mar. 1991. Disponível em: <http://www.ietf.org/rfc/rfc1213.txt>. Acesso em: 31 de jul. 2009.

MENEZES, A.; OORSCHOT, P. van; VANSTONE, S. *Handbook of Applied Cryptography*. Massachussets, EUA: Mit Press, 1996.

MICROCHIP. *SPI - Overview and Use of the PICmicro Serial Peripheral Interface*. jun. 2009. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/spi.pdf>. Acesso em: 31 de jul. 2009.

MILLER, M. *Managing Internetworks with SNMP*. 2nd. ed. Massachussets, EUA: IDG Books Worldwide, INC, 1997.

MOURA, A. *Estudo do Estado da Arte e Análise de Desempenho de Sistema de Comunicação PLC de Banda Larga*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2005.

NAGIOS. *Nagios*. jul. 2009. Disponível em: <http://www.nagios.org>. Acesso em: 31 de jul. 2009.

NET-SNMP. *Net-SNMP*. mar. 2007. Disponível em: <http://www.net-snmp.org>. Acesso em: 31 de jul. 2009.

NORTEL. *Nortel Networks*. jun. 2009. Disponível em: <http://www.nortel.com>. Acesso em: 31 de jul. 2009.

NORWEB. *Business Communications Services*. jun. 2008. Disponível em: <http://www.yourcommunications.co.uk/yc_communications/business_communications_services.html>. Acesso em: 31 de jul. 2009.

OLIVEIRA, D. et al. A study of snmp developments regarding to security and performance. *Congreso Argentino de Ciencia de la Computación*, 2008.

OPENNMS. *OpenNMS*. jul. 2008. Disponível em: <http://www.opennms.org>. Acesso em: 31 de jul. 2009.

OPERA. *Opera*. 2007. Disponível em: <http://www.ist-opera.org>. Acesso em: 31 de jul. 2009.

PAVLIDOU, N. et al. Power line communications: Sate of art and future trends. *IEEE Communications Magazine*, p. 34–40, 2003.

PLCFORUM. *PLC Forum About Us*. jun. 2009. Disponível em: <http://www.plcforum.org>. Acesso em: 31 de jul. 2009.

POSTGRESQL. *PostgreSQL*. jun. 2009. Disponível em: <http://www.postgresql.org>. Acesso em: 31 de jul. 2009.

PRAS, A. *Network Management Architectures*. Tese (Doutorado) — University of Twente, 1995.

PUPAK, D.; GOMES, H. *Estudo e Implementação de Ferramentas de Gerenciamento de Redes de Computadores*. Dissertação (Mestrado) — CEFET-GO, 2006.

RODRIGUES, E. *PLC - Power Line Communications*. 2005. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialplc/pagina_3.asp>. Acesso em: 31 de jul. 2009.

RODRIGUES, L. F. N.; SILVA, M. R. da. *Fornecimento de Energia Elétrica em Tensão Primária de Distribuição*. 2003. Disponível em: <http://celgd.celg.com.br/arquivos/dadosTecnicos/normasTecnicas/NTD05.pdf>. Acesso em: 31 de jul. 2009.

RODRIGUES, L. F. N.; SILVA, M. R. da. *Transformadores para Redes Aéreas de Distribuição - Classes 15 e 36,2 kV - Especificação e Padronização - Revisão 3*. jun. 2004. Disponível em: <http://celgd.celg.com.br/arquivos/dadosTecnicos/normasTecnicas/NTC10.pdf>. Acesso em: 31 de jul. 2009.

SCHMIDT, W. *Materiais Elétricos*. 2. ed. [S.l.]: Edigar Blucher, 1979.

SCHNEIDER. *Ilevo*. 2006. Disponível em: <http://support.ilevo.com/access/en/>. Acesso em: 31 de jul. 2009.

SCHNEIER, B. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. New Jersey, EUA: Wiley Computer Publishing, 1996.

SCRIMGER, R. et al. *TCP/IP, A Bília*. 4. ed. New Jersey, EUA: John Wiley and Sons, 2002.

STALLINGS, W. A security enhancement for snmp. *IEEE Communications Surveys*, 1998.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 2. ed. New Jersey, EUA: Prentice Hall, 1999.

STALLINGS, W. *SNMP, SNMPv2, SNMPv3, and RMON1 and 2*. 3. ed. New Jersey, EUA: Prentice Hall, 1999.

STALLINGS, W. *Data & Computer Communications*. 6. ed. New Jersey, EUA: Prentice Hall, 2000.

SUN. *MySQL*. jul. 2009. Disponível em: <http://www.mysql.org>. Acesso em: 31 de jul. 2009.

TANENBAUM, A. S. *Redes de Computadores*. 4. ed. New Jersey, EUA: Prentice Hall, 2003.

ÁVILA, F.; PEREIRA, C. E. *Tecnologia PLC - A Nova Era da Comunicação de Dados em Banda Larga*. jul. 2007. Disponível em: <http://www6.ufrgs.br/norie/tic2007/artigos/A1126.pdf>. Acesso em: 31 de jul. 2009.

VUKSAN, V. *DHCP Mini-HowTo*. 2002. Disponível em: <http://www.tldp.org/HOWTO/DHCP/>. Acesso em: 31 de jul. 2009.

WARRIER, U. et al. *The Common Management Information Services and Protocols for the Internet (CMOT and CMIP)*. 1990. Disponível em: <http://www.ietf.org/rfc/rfc1189.txt>. Acesso em: 31 de jul. 2009.

WIRESHARK. *Wireshark*. jul. 2009. Disponível em: <http://www.wireshark.org>. Acesso em: 31 de jul. 2009.