

UNIVERSIDADE REGIONAL DE BLUMENAU
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
CURSO DE CIÊNCIAS DA COMPUTAÇÃO – BACHARELADO

SOFTWARE DE INVENTÁRIO DE SOFTWARE DE
EQUIPAMENTOS DE REDE UTILIZANDO *SESSION*
MESSAGE BLOCK

JOSÉLIO KREUCH

BLUMENAU
2007

2007/1-20

JOSÉLIO KREUCH

**SOFTWARE DE INVENTÁRIO DE SOFTWARE DE
EQUIPAMENTOS DE REDE UTILIZANDO *SESSION*
*MESSAGE BLOCK***

Trabalho de Conclusão de Curso submetido à
Universidade Regional de Blumenau para a
obtenção dos créditos na disciplina Trabalho
de Conclusão de Curso II do curso de Ciências
da Computação — Bacharelado.

Prof. Francisco Adell Péricas, Titulação - Orientador

**BLUMENAU
2007**

2007/1-20

**SOFTWARE DE INVENTÁRIO DE SOFTWARE DE
EQUIPAMENTOS DE REDE UTILIZANDO *SESSION*
*MESSAGE BLOCK***

Por

JOSÉLIO KREUCH

Trabalho aprovado para obtenção dos créditos
na disciplina de Trabalho de Conclusão de
Curso II, pela banca examinadora formada
por:

Presidente: _____
Prof. Francisco Adell Péricas, Mestre – Orientador, FURB

Membro: _____
Prof. Sérgio Stringari, Mestre – FURB

Membro: _____
Prof. Paulo Fernando da Silva, Mestre – FURB

Blumenau, 28 de junho de 2007

Dedico este trabalho a minha esposa, filhos e amigos pelo apoio e compreensão ao longo deste desafio.

AGRADECIMENTOS

À Deus, pelo seu imenso amor e graça.

À minha família, que sempre esteve presente.

À minha querida esposa Juliana, que com paciência e confiança me apoiou em todas as horas dedicadas neste trabalho.

Aos meus filhos, por compreenderem a minha falta no decorrer deste curso.

Aos meus amigos, pelos empurrões e cobranças.

Ao meu orientador, Francisco Adell Péricas pelo apoio durante a execução deste trabalho.

Os bons livros fazem “sacar” para fora o que a
pessoa tem de melhor dentro dela.

Lina Sotis Francesco Moratti

RESUMO

Este trabalho apresenta o desenvolvimento de um software para inventário de patrimônio de rede. Dentre os diversos protocolos existentes para executar a gerência de rede, neste projeto foi utilizado o protocolo *Session Message Block* (SMB) que envia as informações extraídas do Registro do Windows para uma base de dados centralizada. Também é apresentado como foi implementado o software que faz a gerência de patrimônio de rede e suas funcionalidades.

Palavras-chave: Protocolo de rede. Inventário de computadores. Patrimônio. SMB.

ABSTRACT

This work presents the development of software to inventory the patrimony of net. Among the diverse existing protocols that can execute the management of the net, in this project was used the protocol Session Message Block (SMB) that send the extracted information of the Windows Registry to a central database. It is also presented how it was implemented a software archetype that makes the management of a net patrimony and its functionalities.

Key-words: Computer inventory. Networks protocol. Patrimony. SMB.

LISTA DE ILUSTRAÇÕES

Figura 1 – Comunicação entre entidades de gerência.....	14
Figura 2 – Elementos de uma arquitetura geral de solução de gerência.....	16
Figura 3 – Estrutura do Registro do Windows	19
Figura 4 – Funcionamento do protocolo SMB	20
Figura 5 – Módulo Gerente WEB.....	26
Figura 6 – Módulo Agente.....	27
Figura 7 – Tela do Gerenciador, apresentando o inventário das estações.	28
Figura 8 – Apresentada ao usuário da estação de rede pelo Agente.	29
Figura 9 - Esquema de funcionamento entre agente e gerente	30
Figura 10 – Diagrama de casos de uso	32
Figura 11 – Diagrama de classes	34
Figura 12 – Diagrama de atividades	35
Figura 13 – Esquema de funcionamento entre software cliente e software servidor.....	38
Figura 14 – Software Cliente	39
Figura 15 – Tela software servidor	40
Figura 16 – Relatório de Histórico de Softwares Inventariados Estações	41

LISTA DE TABELAS E QUADROS

Tabela 1 – Estrutura de mensagem SMB utilizando a linguagem C	23
Quadro 2 – Procedimento que lê as informações do Registro sobre softwares instalados	36
Quadro 3 – Procedimento que lê as informações do Registro sobre softwares instalados	37
Quadro 4 – Resultado dos testes em laboratório.....	42

LISTA DE SIGLAS

CD-R – *Compact Disk Recordable*

ISO – *International Standards Organization*

LAN - *Local Area Network*

OID – *Object Identifier*

OSI – *Open Systems Interconnection*

PID – *Process Identifier*

SMB – *Session Message Block*

SNMP – *Simple Network Management Protocol*

TCP – *Transmission Control Protocol*

TID – *Tree Identifier*

UDP – *User Datagram Protocol*

UID – *Unique Identifier*

UML – *Unified Modeling Language*

USB – *Universal Serial Bus*

SUMÁRIO

1 INTRODUÇÃO	11
1.1 OBJETIVOS DO TRABALHO	12
1.2 ESTRUTURA DO TRABALHO	12
2 GERENCIAMENTO DE REDES	14
2.1 O PAPEL DO GERENTE DE REDES	17
2.2 REGISTRO DO WINDOWS	18
2.2.1 Estrutura do Registro	19
2.3 PROTOCOLO SMB	20
2.3.1 Segurança do SMB	21
2.3.2 Arquitetura do SMB	21
2.3.3 Gerenciamento de processos do SMB	22
2.3.4 Formato de mensagem do protocolo SMB	23
2.3.5 Comando de controle de sessão	23
2.4 TRABALHOS CORRELATOS	25
2.4.1 PROTÓTIPO DE SOFTWARE PARA GERÊNCIA DE PATRIMÔNIOS DOS EQUIPAMENTOS DE UMA REDE UTILIZANDO <i>SESSION MESSAGE BLOCK</i>	27
3 DESENVOLVIMENTO DO TRABALHO	31
3.1 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO	31
3.2 ESPECIFICAÇÃO	32
3.2.1 Diagrama de casos de uso	32
3.2.2 Diagrama de Classe	33
3.2.3 Diagrama de Atividades	34
3.3 IMPLEMENTAÇÃO	35
3.3.1 Técnicas e ferramentas utilizadas	35
3.3.2 Operacionalidade da implementação	37
3.4 RESULTADOS E DISCUSSÃO	41
4 CONCLUSÕES	43
4.1 EXTENSÕES	43
REFERÊNCIAS BIBLIOGRÁFICAS	45

1 INTRODUÇÃO

Com a grande facilidade oferecida pelas redes de computadores e periféricos portáteis como *pen driver*, *Compact Disc Recordable* (CD-R), fica muito difícil para grandes empresas gerenciar e saber o que está instalado em cada uma das estações de trabalhos e servidores do seu parque de computadores.

A utilização de Notebooks e outros portáteis utilizados em redes de computadores desprotegidas, sem a mínima segurança, comum em aeroportos e hotéis, tornando muito mais fácil a invasão por softwares maliciosos para coletar informações sigilosas. Outro problema que grandes instituições vêm enfrentando é o de evitar o uso de softwares piratas. Sem um bom software para auxiliar, não se consegue avaliar se o número de licenças adquiridas é suficiente para atender a demanda da empresa, que em muitos casos é multada mesmo que a pirataria seja de forma não intencional.

O gerenciamento de uma grande rede é sempre difícil e cara sem ajuda de um software que mostre a realidade dos equipamentos conectados na rede, principalmente na hora de tomar uma decisão estratégica quanto à substituição de computadores ou softwares em grande escala. Não tendo estas informações de uma forma fácil e imediata, pode-se atrasar um grande projeto cooperativo.

Baseado nas dificuldades citadas acima, de gerenciar os softwares instalados nos computadores, o software apresentado neste trabalho foi desenvolvido como continuidade daquele descrito em Oliveira Junior (2005) que trata do levantamento patrimonial do parque de hardware. O protocolo *Session Message Block* (SMB) será utilizado para prover a comunicação entre estação servidora e estações clientes, disponibilizando de forma rápida e eficiente para o administrador de rede um completo detalhamento de componentes de hardware (desenvolvido por Oliveira Junior) e de softwares (proposto neste trabalho) que compõem cada computador. As informações serão coletadas de forma automática na inicialização da estação.

1.1 OBJETIVOS DO TRABALHO

O objetivo deste trabalho foi desenvolver um software servidor¹ e um software cliente para levantamento de inventário de software nos computadores de uma rede empresarial.

Os objetivos específicos do trabalho são:

- a) rastrear os softwares instalados nas estações através de um software cliente instalado nos computadores de rede;
- b) concentrar estas informações em um banco de dados centralizado para torná-las persistentes utilizando um software servidor;
- c) ter disponível a qualquer momento o inventário de software de cada estação da rede;
- d) disponibilizar relatórios dos softwares instalados em cada computador conectado à rede.

1.2 ESTRUTURA DO TRABALHO

O capítulo 1 apresenta a estrutura geral do trabalho, a introdução, os objetivos que se quer alcançar, a localização dos assuntos abordados e a organização do trabalho.

No capítulo 2 é apresentado um estudo sobre Gerenciamento de Redes, abordando a importância do operador e do gerente de rede, como é formado uma equipe de gerência, o funcionamento do Registro do Windows, o protocolo de gerência (SMB) com todas as suas propriedades e funcionalidades, bem como suas aplicações e forma de operação. Também nesse capítulo são apresentados os trabalhos correlatos CACIC, Trauma Zer0 e o trabalho de conclusão de curso de Oliveira Junior (2005), Protótipo de Software para Gerência de Patrimônios dos Equipamentos de uma Rede Utilizando o Session Message Block, utilizado como base para este trabalho.

O capítulo 3 descreve como foi desenvolvido o software, apresentando os seus requisitos, a especificação através dos diagramas de classe, de atividades, de sequência e de casos de uso. Também são apresentadas as suas funcionalidades e todo o esquema de

funcionamento.

O capítulo 4 apresenta as conclusões sobre o trabalho e sugestões para extensões e trabalhos futuros.

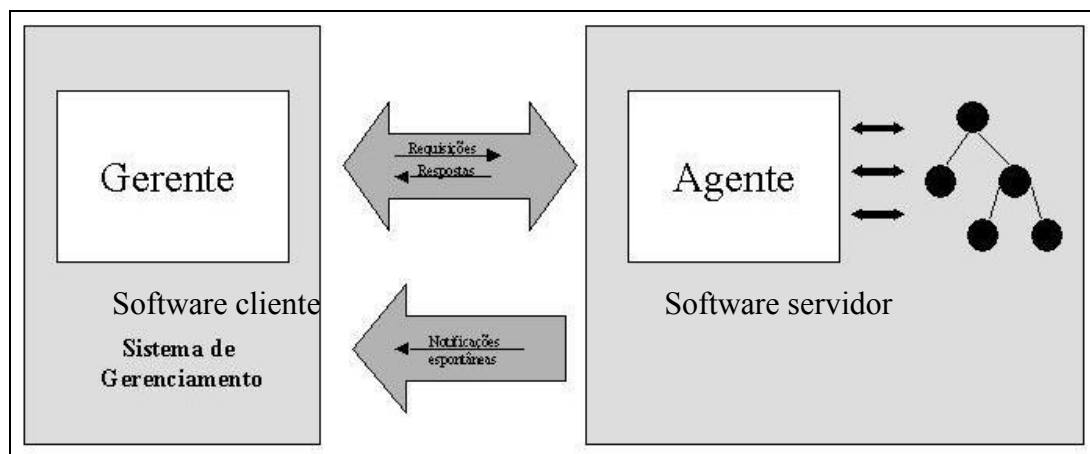
¹ Entende-se por software cliente o software instalado no computador que se quer extrair as informações e software servidor o software instalado na estação de gerência que recebe as informações dos softwares clientes.

2 GERENCIAMENTO DE REDES

Com a grande necessidade de troca de informações entre computadores, as grandes empresas têm investido muito para integrar seus equipamentos mesmo que em regiões geográficas diferentes e distantes. Com isso tem-se a necessidade de centralizar informações comuns para uma melhor administração e compartilhamento de recursos, como sistemas de missão crítica que podem influenciar diretamente no objetivo da empresa. Estes recursos podem ser compartilhados por diversas pessoas em diversos lugares, tornando cada vez mais difícil de gerenciá-los e mantê-los seguros.

Segundo Péricas (2003, p. 121–122), a gerência de redes é dividida em gerência de falhas, gerência de configuração, gerência de contabilização, gerência de desempenho e gerência de segurança. A gerência de segurança permite prevenir e detectar o uso impróprio ou não autorizado de recursos numa rede, assim como sua administração.

Conforme descreve Péricas (2003, p. 125), a infra-estrutura de gerenciamento especificada pela *International Organization for Standardization* (ISO) define que gerente é uma aplicação de gerência (software cliente) que faz as requisições de operações, recebe notificações, enquanto que o agente (software servidor) é que recebe e processa estas operações e envia as respostas e emite as notificações. Na figura 1 pode-se ver um exemplo de comunicação entre as aplicações gerente e agente.



Fonte: Péricas (2003, p. 125).

Figura 1 – Comunicação entre entidades de gerência

Lopes, Sauv  e Nilletti (2003, p. 4-5) a arquitetura geral dos sistemas de ger ncia de redes apresenta quatro componentes b sicos: elementos gerenciados, esta  es de ger ncia, protocolo de ger ncia e informa  es de ger ncia.

Os elementos gerenciados possuem um software especial chamado agente. Este

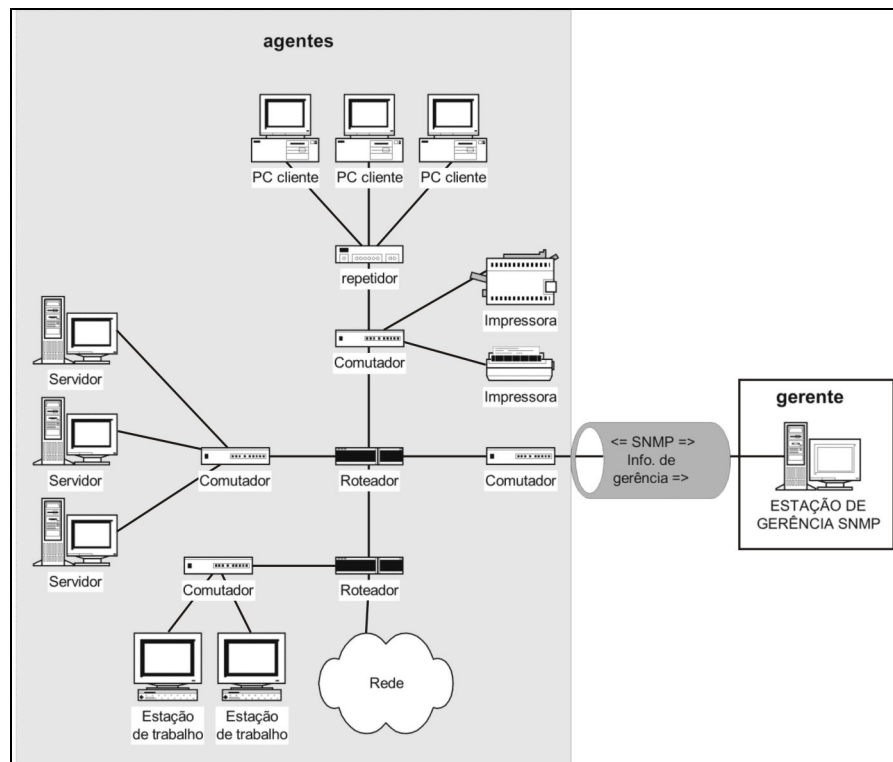
software permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência.

Em um sistema de gerência de redes deve haver pelo menos uma estação de gerência. Em sistemas de gerência distribuídos existem duas ou mais estações de gerência e em sistemas centralizados, que é o mais comum, existem apenas uma. Chamamos de gerente o software da estação de gerência que conversa diretamente com os agentes nos elementos gerenciados, seja com o objetivo de monitorá-los, seja com o objetivo de controlá-los. A estação de gerência oferece uma interface através da qual somente usuários autorizados podem gerenciar a rede.

Para que a troca de informações entre gerente e agentes seja possível é necessário que eles falem o mesmo idioma. O idioma que eles falam é um protocolo de gerência. Este protocolo permite operações de monitoramento como leitura e operações de controle como escrita.

Os gerentes e os agentes podem trocar informações, mas não qualquer tipo de informação. As informações de gerência definem os dados que podem ser referenciados em operações de protocolo de gerência, isto é, dados sobre os quais gerentes e agentes conversam.

Na figura 2 vemos roteadores, comutadores, repetidores, impressoras, servidores e estações clientes. Todos estes equipamentos podem ter agentes instalados. A estação de gerência deve obter informações de gerência destes agentes usando o protocolo *Simple Network Management Protocol* (SNMP).



Fonte: Lopes, Sauvé e Nicolletti (2003, p. 5)

Figura 2 – Elementos de uma arquitetura geral de solução de gerência

A padronização de solução de gerência mais usada chama-se *Simple Network Management Protocol*. Esta solução é mais conhecida como gerência SNMP. SNMP é o protocolo de gerência deste padrão. Este padrão descreve não apenas o protocolo de gerência, mas também um conjunto de regras que são usadas para definir as informações de gerência e um conjunto inicial de informações de gerência que já podem ser utilizadas.

Através da estação de gerência pode-se obter informações tais como: taxa de erros, estado operacional de enlaces e equipamentos, utilização de enlaces, dentre outras. Tão importante quanto obter estas informações é saber interpretá-las. Por exemplo, em um determinado momento, a estação de gerência informa que a taxa de erros de um certo enlace é 1%. Esta é uma taxa de erros aceitável?

Para muitas informações de gerência estabelece-se valores limites. Se o valor da informação obtida for maior que o limite estabelecido, algo anormal está ocorrendo na rede. Estes limites chamam-se de limiares (*thresholds*). Assim, quando se diz que limiares foram excedidos, diz-se que se obteve valores de informações de gerência que não estão dentro da faixa de normalidade e, portanto, são indicativos de problemas. Limiares excedidos e outros eventos podem gerar alarmes na estação de gerência. Quando a estação de gerência percebe que uma interface parou de operar, por exemplo, um alarme pode ser gerado.

Além do sistema de gerência de redes, outras ferramentas auxiliam a gerenciar uma

rede. Dentre elas encontram-se analisadores de protocolos e outras ferramentas mais simples, como o comando *ping*, *traceroute* e *netstat*, disponíveis nos vários sistemas operacionais.

Com os analisadores de protocolos podemos ver quais dados estão trafegando na rede, eles permitem tirar raios-X da rede, sendo, portanto, ferramentas importantes de gerência. Certas tarefas da gerência só podem ser realizadas com o auxílio de um analisador de protocolos (LOPES; SAUVÉ; NICOLLETTI, 2003).

2.1 O PAPEL DO GERENTE DE REDES

Um dos objetivos da gerência de redes é prevenir e solucionar problemas na rede. Geralmente esta tarefa é realizada por uma equipe. Não existe uma regra rígida sobre os profissionais que fazem parte desta equipe. Cada organização tem autonomia para criar seu próprio time de gerência de redes de acordo com suas conveniências. Porém, é comum que nesta equipe existam profissionais que executem quatro tarefas distintas: o pessoal de *help desk*, o operador da rede, a equipe de suporte técnico e o gerente da equipe de gerência.

Quando os usuários enfrentam problemas relacionados à tecnologia de informação, eles pedem auxílio ao *help desk*. Em algumas organizações o *help desk* é composto por apenas uma pessoa, que atende chamadas telefônicas de usuários e tem certo grau de conhecimento para lidar com alguns problemas que forem reportados. Em organizações maiores, o *help desk* é composto por um grupo de pessoas um pouco mais especializadas, auxiliadas por aplicações que ajudam a gerenciar os problemas reportados. Além disso, esta equipe pode ser auxiliada por outras ferramentas que ofereçam informações que possam ajudar a localizar e/ou solucionar os problemas. Por exemplo: ferramentas que apresentam o estado operacional das interfaces e equipamentos da rede. Geralmente esta equipe é capaz de solucionar os problemas mais simples e os erros pelos próprios usuários. Quando o *help desk* existe, os usuários nunca têm contato com a equipe de suporte técnico ou com o operador da rede; apenas com o próprio *help desk*.

O operador do sistema é o profissional encarregado de acompanhar os alarmes gerados pela estação de gerência. Quando, por exemplo, um equipamento passa para o estado não operacional, o operador da rede perceberá um alarme na estação de gerência. Alarmes podem ser informados de diversas formas: mudança de cores no mapa da rede, por e-mail, celular etc. Quando o operador percebe que o problema está ocorrendo ou pode ocorrer, ele tenta resolver

o problema ou então encaminha-o à equipe de suporte técnico.

O gerente da equipe de gerência de rede não é, necessariamente, um técnico em redes. O gerente tem um certo conhecimento em redes, mas não no nível do suporte técnico. Dentre as atividades deste gerente encontram-se: avaliar o desempenho da equipe de suporte, solicitar compra de equipamentos, aplicações ou outros recursos necessários, providenciar treinamento adequado para a equipe, reescalonar a solução de problemas para outros membros da equipe quando a solução demora. Para avaliar o desempenho da equipe de gerência, o gerente pode se valer de certas métricas tais como: o tempo médio entre falhas e o tempo médio para correção de falhas na rede, percentual de problemas resolvidos em menos de 1 hora, entre outras (LOPES; SAUVÉ; NICOLLETTI, 2003).

2.2 REGISTRO DO WINDOWS

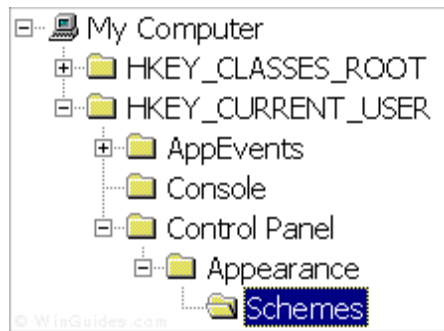
O *Microsoft Computer Dictionary* (MICROSOFT CORPORATION, 2005a) define o Registro como “um banco de dados hierárquico central usado no Windows 9x, Windows CE, Windows NT e Windows 2000, usado para armazenar as informações necessárias à configuração do sistema para um ou mais usuários, aplicativos e dispositivos de hardware”.

O Registro contém informações que o Windows utiliza continuamente durante a operação, como os perfis de cada usuário, os aplicativos instalados no computador e os tipos de documentos que cada um pode criar, configurações de propriedades para ícones de pastas e aplicativos, hardware existente no sistema e portas que são usadas. Os dados do Registro são armazenados em arquivos binários.

Resumindo, o Registro do Windows nada mais é que uma base de dados que guarda todas as informações do sistema. Quando um novo software é instalado em um sistema operacional Windows as mudanças são refletidas e armazenadas no seu Registro. Na Arquitetura Windows NT/2000/XP, o Registro fica armazenado dentro do diretório “%SystemRoot% \ System32 \ Config”. Não se consegue editar estes dados diretamente sem um editor de registro (WINGUIDES NETWORK FOR WINDOWS, 2006).

2.2.1 Estrutura do Registro

Registro é organizado em uma estrutura hierárquica de subárvores e suas chaves, subchaves e entradas. Na figura 3 pode-se observar que o registro do Windows possui uma estrutura hierárquica como o gerenciador de arquivos Microsoft Windows Explorer.



Fonte: Winguides Network for Windows (2006).

Figura 3 – Estrutura do Registro do Windows

O conteúdo do Registro pode variar amplamente de um computador para outro, dependendo dos dispositivos, serviços e programas instalados em cada computador.

As chaves podem ter subchaves e as subchaves, por sua vez, podem ter subchaves. Embora a maioria das informações do Registro esteja armazenada no disco e seja considerada permanente, algumas informações, armazenadas em chaves voláteis, são sobrescritas sempre que o sistema operacional é iniciado.

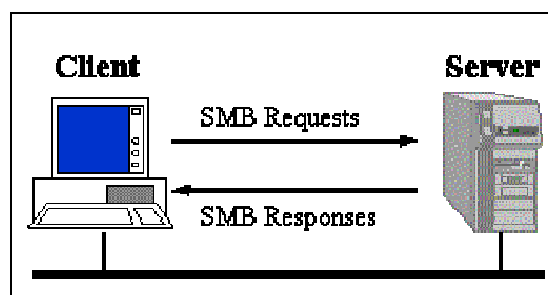
Para que as informações do registro do Windows possam ser facilmente encontradas o editor do Registro exibe cinco subárvores, três das quais são *alias* de outras partes do Registro. As cinco subárvores estão listadas e descritas na tabela a seguir:

- a) HKEY_LOCAL_MACHINE - Contém informações sobre o sistema do computador local, incluindo dados de hardware e sistema operacional, como tipo de barramento, memória do sistema, *drivers* de dispositivo e dados de controle de inicialização;
- b) HKEY_CLASSES_ROOT - Contém informações usadas por várias tecnologias OLE e dados de associação de classe de arquivo. Haverá determinada chave ou determinado valor em HKEY_CLASSES_ROOT se houver uma chave ou um valor correspondente em HKEY_LOCAL_MACHINE\SOFTWARE\Classes ou HKEY_CURRENT_USER\SOFTWARE\Classes. Se houver uma chave ou um valor em ambos, a versão de HKEY_CURRENT_USER será a exibida em HKEY_CLASSES_ROOT;

- c) HKEY_CURRENT_USER - Contém o perfil do usuário que está conectado interativamente, incluindo variáveis de ambiente, configurações da área de trabalho, conexões de rede, impressoras e preferências de programas. Esta subárvore é um alias da subárvore HKEY_USERS e aponta para HKEY_USERS\ID de segurança do usuário atual;
- d) HKEY_USERS - Contém informações sobre os perfis de usuários carregados ativamente e o perfil padrão. Inclui informações que também aparecem em HKEY_CURRENT_USER - Os usuários que estiverem acessando remotamente um servidor não terão perfis nessa chave no servidor; seus perfis serão carregados no Registro dos seus próprios computadores;
- e) HKEY_CURRENT_CONFIG - Contém informações sobre o perfil de hardware usado pelo sistema do computador local na inicialização. Essas informações são usadas para definir a configuração, como os *drivers* de dispositivo que devem ser carregados e a resolução de vídeo que deve ser usada. Essa subárvore faz parte da subárvore HKEY_LOCAL_MACHINE e aponta para HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current (MICROSOFT CORPORATION, 2005b).

2.3 PROTOCOLO SMB

O *Session Message Block* (SMB) é um protocolo para compartilhamento de arquivos, impressoras, portas seriais e para abstração de comunicação entre computadores. O SMB é um protocolo cliente/servidor, conhecido também como *request-response*, onde o cliente faz uma requisição ao servidor e o servidor retorna uma resposta. Na figura 4 pode-se observar o funcionamento do SMB.



Fonte: Samba (2002).

Figura 4 – Funcionamento do protocolo SMB

Os clientes utilizam o *NetBios over TCP/IP* para se conectarem ao servidor. Depois de estabelecida a conexão, os clientes já podem utilizar os comandos SMB para compartilhar pastas, arquivos e impressoras (SAMBA, 2002).

2.3.1 Segurança do SMB

O SMB é definido por dois níveis de segurança, chamados de *Share Level* e *User Level*. No *Share Level*, a proteção é aplicada no compartilhamento do servidor, onde cada compartilhamento possui uma senha e os clientes só conseguem acessar todo o conteúdo deste compartilhamento se possuírem a senha. Já no *User Level*, a proteção é aplicada individualmente para cada arquivo baseado nos direitos de acesso do usuário (cliente). Todos os usuários precisam se autenticar em um servidor e depois de autenticados recebem uma identificação única (UID) que será utilizada nos próximos acessos ao servidor (SAMBA, 2002).

2.3.2 Arquitetura do SMB

Um cliente é um sistema que solicita serviços de arquivos da rede e um servidor é um sistema que entrega serviços de arquivos da rede. Os clientes e os servidores são sistemas lógicos: um cliente e um servidor podem coexistir em um único sistema físico, ou seja, no mesmo computador. Os clientes são responsáveis por dirigir seus pedidos ao servidor apropriado. O mecanismo de endereçamento de rede ou convenção de nomes com que o servidor é identificado é tratado pela própria rede. Cada servidor disponibiliza à rede uma estrutura *self-contained* de arquivos. Não há dependência de outros servidores, nem por armazenamento nem por serviço. Um arquivo deve ser alocado inteiramente por um único servidor. Um arquivo compartilhado requer uma autenticação do servidor antes que os acessos pelos clientes sejam permitidos. Cada processo no servidor autentica seu próprio cliente. Um cliente deve efetuar a autenticação em cada servidor que deseja utilizar.

Este modelo de autenticação supõe que a LAN conecta os sistemas autônomos que disponibilizarem algum subconjunto de seus arquivos locais aos servidores remotos. Os seguintes ambientes existem no ambiente de compartilhamento de arquivo do protocolo:

- a) *Virtual Circuit Environment* - consiste em um Circuito Virtual estabelecido entre

um sistema do cliente consumidor e o sistema do servidor. Os clientes podem ter somente um único pedido ativo em qualquer tempo, isto é, um segundo pedido não pode ser iniciado até que a resposta ao primeiro esteja recebida. Um Circuito Virtual representa os dados que usam o serviço de transporte;

- b) *Logon Environment* - é representado por uma árvore de ID (TID). Um TID identifica excepcionalmente um arquivo que compartilha uma conexão entre um cliente e um servidor. Identifica também o espaço e o tipo de acesso permitido através da conexão;
- c) *Ambiente Process* – é representado por um identificador de processo (PID). Um PID identifica um processo do cliente dentro de um ambiente;
- d) *File Environment* - é representado por um *file handle* (FID). Um FID identifica um arquivo aberto que é único dentro de um ambiente.

Quando um destes ambientes é terminado, todos os ambientes contidos dentro dele estarão terminados. Por exemplo, se um canal virtual for encerrado, todos os PIDs, TIDs e FIDs dentro dele serão invalidados.

2.3.3 Gerenciamento de processos do SMB

Como e quando os servidores criam e destroem processos é, naturalmente, uma implementação da execução e não há nenhuma exigência que este processo seja amarrado à gerência de processos do cliente. Entretanto é necessário que o servidor esteja ciente das atividades da gerência do processo do cliente porque os arquivos são acessados pelo nome do cliente. Conseqüentemente, o arquivo que compartilha o protocolo inclui notificações apropriadas. Todas as mensagens, exceto negociações, incluem uma identificação do processo (PID) para indicar que processo do servidor iniciou um pedido. Os clientes informam aos servidores da criação de um processo novo simplesmente introduzindo um PID novo no diálogo. A destruição do processo deve explicitamente ser indicada por "*Process Exit*", comando específico para esta finalidade. O servidor deve emitir um comando no processo de saída sempre que um processo do cliente é destruído. Isto permite que o servidor se livre de todos os recursos reservados por este processo e possa executar quaisquer atividades locais de gerência de processo que possa ser requerido.

2.3.4 Formato de mensagem do protocolo SMB

Cada mensagem tem um formato comum. Na tabela 1 pode-se ver um exemplo com a linguagem C.

Data type	Field	Value
BYTE	smb_fid[4];	contains 0xFF, 'SMB'
BYTE	smb_com;	command code
BYTE	smb_rcls;	error code class
BYTE	smb_reh;	reserved (contains AH if DOS INT-24 ERR)
WORD	smb_err;	error code
BYTE	smb_res;	reserved
WORD	smb_res[7];	reserved
WORD	smb_tid;	tree id number
WORD	smb_pid;	caller's process id number
WORD	smb_uid;	user id number
WORD	smb_mid;	multiplex id number
BYTE	smb_wct;	count of parameter words
WORD	smb_vwv[];	variable number words of params
WORD	smb_bcc;	number of data bytes following
BYTE	smb_data[];	data bytes

Fonte: Microsoft Corporation, Intel Corporation (1988).

Tabela 1 – Estrutura de mensagem SMB utilizando a linguagem C

2.3.5 Comando de controle de sessão

Os tópicos abaixo explicam os comandos de controle de sessão aceitos pelo protocolo SMB:

- a) compartilhamento de arquivos: as redes que usam compartilhamento de arquivos do protocolo conterão não somente sistemas multi-usuários com modelos baseados no servidor de proteção, mas os sistemas mono-usuário que não têm nenhum conceito das identificações únicas ou das permissões. Uma vez que estas máquinas são conectadas à rede, estão em um ambiente multi-usuários e necessitam um método do controle de acesso. Primeiro, as máquinas desprotegidas necessitam permissão para fornecer a outras máquinas da rede que

têm permissões; segundo, as máquinas desprotegidas necessitam controlar o acesso a seus arquivos por outro. Este protocolo define um mecanismo que habilita o software de rede a fornecer a proteção onde falta o sistema operacional e suporte à proteção do servidor fornecido pelo sistema operacional. O mecanismo permite também que as máquinas com nenhum conceito do UID demonstrem a autorização de acesso às máquinas que têm um mecanismo de permissão. Finalmente, o protocolo de permissão está projetado de modo que possa ser omitido se ambas as máquinas compartilharem de um mecanismo comum da permissão. Este protocolo, chamado de *tree connection*, não especifica uma interface de usuário;

- b) acesso a servidores desprotegidos: a requisição deve ser feita pelo nome da máquina fornecido pelo comando NET USE, e associá-la com o valor de índice retornado pelo servidor. Os pedidos subsequentes que usam este índice devem incluir somente o caminho relativo à sub-árvore conectada enquanto o servidor trata a sub-árvore como o diretório de raiz. Quando a requisição tem um pedido de acesso ao arquivo para o servidor, localiza através de sua lista dos prefixos para essa máquina e o seleciona. Inclui então o índice associado com este prefixo em seu pedido junto com o restante do caminho. Ele oferece sempre um diretório e todas os arquivos debaixo desse diretório são afetados. Se um arquivo particular estiver dentro da escala de múltiplas ofertas, conectando-se a qualquer uma das escalas da oferta, se ganha o acesso ao arquivo com as permissões especificadas para a oferta nomeada no NET USE. O servidor não verificará para ver se há diretórios com as permissões mais restritivas;
- c) acesso a servidores protegidos: os servidores com esquemas baseados na proteção de arquivos interpretarão a *tree connect* com o comando ligeiramente diferente dos sistemas com os esquemas orientados à proteção de arquivos. Eles interpretam o “nome” como um *username* melhor que um *pathname*. Quando este pedido é recebido, o *username* será validado e um TID representando a autenticidade do servidor, que é retornada. Este TID deve ser incluído em todas as requisições feitas ao servidor. O sistema *permission-based* não necessita executar o comando NET SHARE;
- d) comando de negociação: o cliente emite uma lista das primitivas com que pode comunicar-se. A resposta é uma seleção de uma daquelas primitivas (numeradas de 0 à n) ou -1 que indica que nenhum das primitivas são aceitáveis. A mensagem

de negociação está ligada ao Circuito Virtual que deve ser enviada. Somente uma mensagem de negociação pode ser enviada: mensagens de negociação subsequente serão rejeitadas com uma resposta de erro e nenhuma ação será tomada. O protocolo não impõe nenhuma estrutura particular às mensagens;

- e) comando de atribuição de atributos no servidor: este comando é usado para determinar a capacidade total do servidor e o espaço livre restante. A distinção entre alocação unitária e blocos do disco permite o uso do protocolo com sistemas operacionais que alocam o espaço de disco nas unidades maiores do que o bloco físico do disco. As unidades de bloco/alocação usadas nesta resposta podem ser independentes do algoritmo físico ou lógico real de bloco/alocação usado internamente pelo servidor. Entretanto, devem refletir a quantidade de espaço no servidor;
- f) comando de checagem do caminho: mensagem de checagem do caminho é usada para verificar se um caminho existe e é um diretório. Nenhum erro é retornado se o caminho existir e a requisição tiver o acesso a ele. Os servidores não têm um conceito de “*working directory*”, o cliente deve sempre fornecer os caminhos completos (relativo ao TID);
- g) comando de conexão com a TID: o caminho/usuário deve ser especificado da raiz da rede. O campo da TID na requisição da mensagem é ignorado pelo servidor. O tamanho máximo transmitido na resposta indica o tamanho máximo da mensagem que o servidor aceita. O cliente não deve gerar mensagens, nem esperar receber as respostas maiores do que esta. Isto deve ser constante no servidor. Uma *Tree Conect* deve ser emitida para todos os *subtrees* alcançados, mesmo se contém uma senha nula (MICROSOFT CORPORATION, INTEL CORPORATION, 1988).

2.4 TRABALHOS CORRELATOS

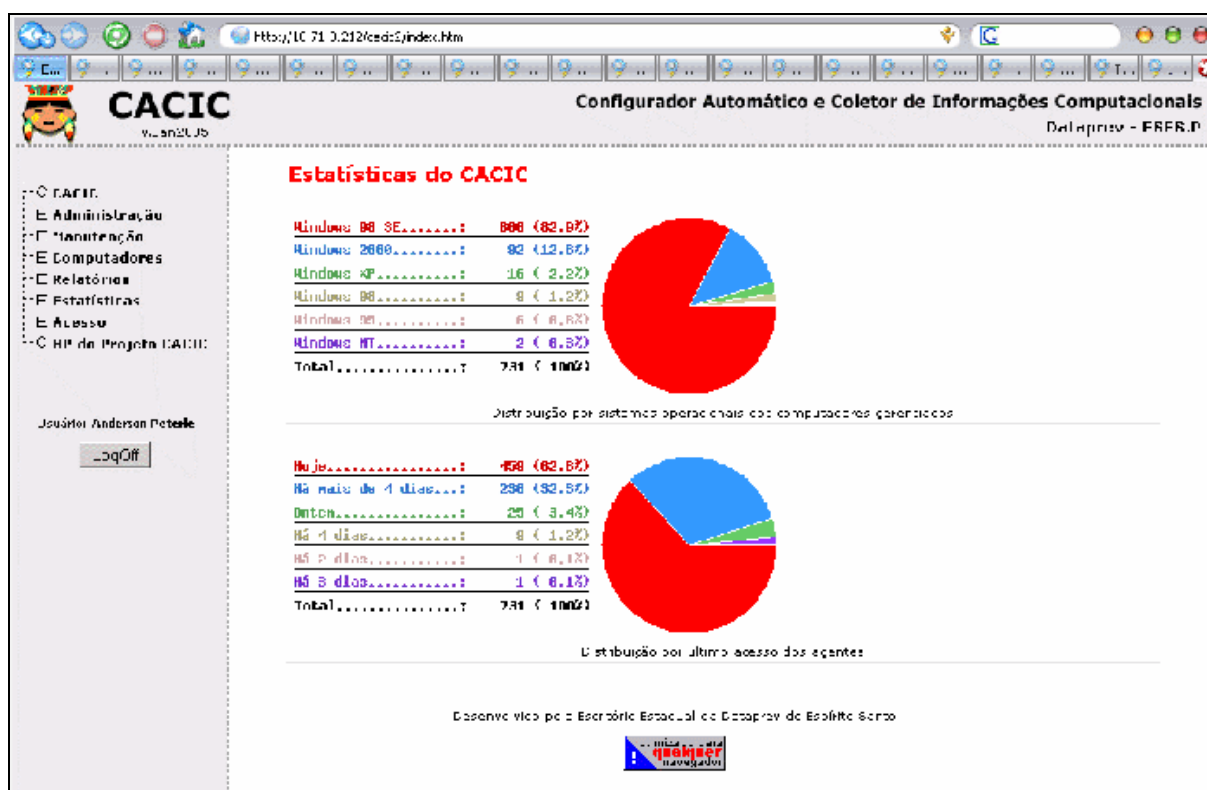
A seguir estão descritos alguns softwares com características semelhantes ao proposto neste TCC.

CACIC é o primeiro software público do governo federal desenvolvido em consórcio de cooperação entre a Secretaria de Logística Tecnológica de Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão (MPOG) e a Empresa de Tecnologia e

Informação de Previdência Social (DATAPREV). CACIC é capaz de fornecer um diagnóstico preciso do parque computacional e disponibilizar os tipos de softwares utilizados e licenciados, configurações de hardwares, entre outras. As principais funções do CACIC são:

- coletar e disponibilizar informações sobre softwares instalados nas estações de trabalho e servidores;
- coletar informações sobre configurações de hardware;
- alertar aos administradores de sistemas, sempre que forem detectadas situações anormais ou de risco;
- prover aos administradores informações para que sejam realizadas ações proativas.

O CACIC é dividido em dois componentes, módulo Gerente e módulo Agente. O módulo Gerente reside em qualquer plataforma Linux que possua servidor Web Apache, banco de dados MySQL e linguagem de script PHP. O módulo Gerente é acessado por uma interface Web, onde é possível a administração de todos os Agentes, permitindo consultas parametrizadas como informações de determinados softwares instalados nos Agentes. A figura 5 mostra a tela principal do módulo Gerente.

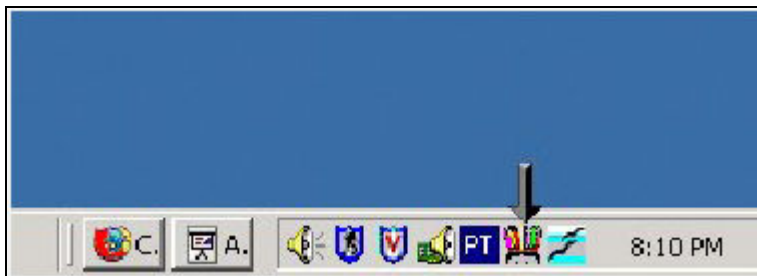


Fonte: Dataprev(2005).

Figura 5 – Módulo Gerente WEB

O módulo Agente pode ser instalado em qualquer plataforma Windows 9x/ME/NT/2000/XP e GNU/Linux. O módulo Agente Windows foi desenvolvido em Delphi

utilizando apenas bibliotecas livres ou gratuitas e o GNU/Linux foi desenvolvido em PERL e Python. Este módulo é responsável por coletar as informações dos computadores e enviar para o Gerente (DATAPREV, 2005).



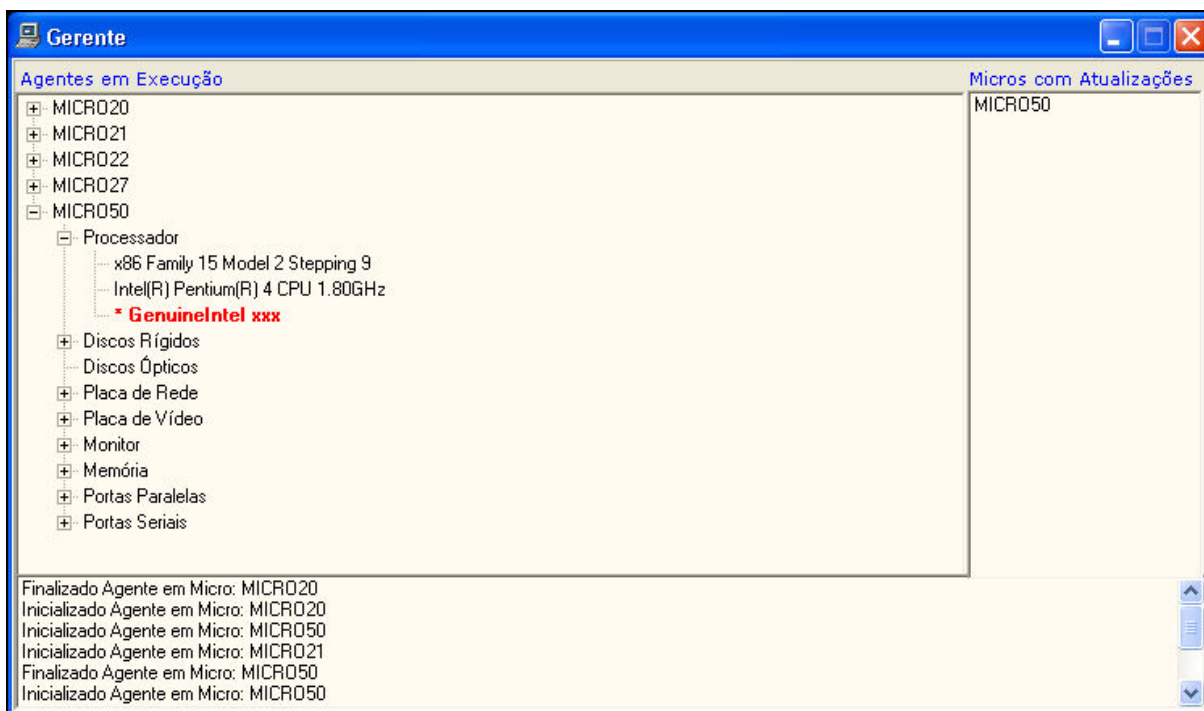
Fonte: Dataprev(2005).

Figura 6 – Módulo Agente

A Suite Trauma Zer0 é um software para gerenciamento de redes que dentre suas funcionalidades está o inventário de hardware e software, rastreamento de localização física, auditoria remota, distribuições de softwares, bloqueio de aplicações e outras funcionalidades mais. Possibilita a visualização em tempo real das alterações realizadas nos itens de configurações de hardware e softwares nos computadores. A Suíte Trauma Zer0 ainda exige que todos os softwares instalados sejam certificados, impedindo que softwares sem licença sejam instalados (IVIRTUA SOLUTIONS, 2006). Trauma Zer0 é um software eficiente por conseguir extrair muitas informações dos computadores, mas o custo para aquisição e implantação é muito elevado.

2.4.1 PROTÓTIPO DE SOFTWARE PARA GERÊNCIA DE PATRIMÔNIOS DOS EQUIPAMENTOS DE UMA REDE UTILIZANDO *SESSION MESSAGE BLOCK*

O protótipo implementado por Oliveira Junior (2005) foi desenvolvido em Delphi 7 utilizando o protocolo SMB e tem como finalidade coletar dados de computadores conectados em uma rede, basicamente fazendo um inventário de hardware e disponibilizando-o em uma console de gerenciamento, onde um administrador de rede pode avaliar as configurações naquele momento e verificar se houve alguma alteração com um inventário feito anteriormente.



Fonte: Oliveira Junior (2005).

Figura 7 – Tela do Gerenciador, apresentando o inventário das estações

Para a leitura do Registro do Windows no Agente, foi criado um componente (uInformacoes.pas) para ler as informações do Registro através de suas chaves específicas que guardam as informações desejadas para fazer o levantamento de patrimônio do computador. As informações lidas por este componente são armazenadas temporariamente em suas propriedades que em seguida são armazenadas no próprio Registro do Windows numa chave específica de sua propriedade criada para armazenar persistentemente as informações colhidas. Estas informações armazenadas no Registro do Windows pelo componente, servem posteriormente para fazer a comparação entre as informações que estão sendo lidas e as informações lidas anteriormente, permitindo com que se possa efetuar uma comparação entre as duas e afirmar se houve ou não mudanças nos componentes instalados no computador. O Agente fica instanciado apresentando um ícone junto a barra de tarefas do Windows. Clicando neste ícone o usuário local pode visualizar as informações de hardware do seu computador, conforme pode ser visto na figura 8.

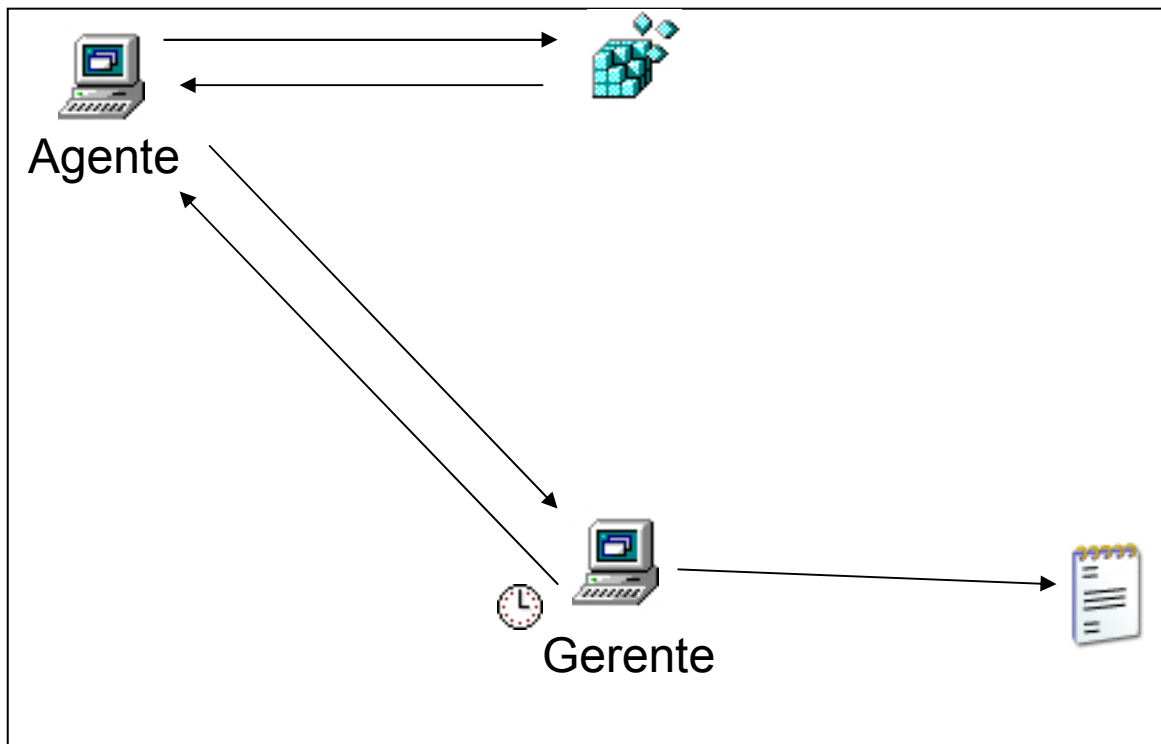


Fonte: Oliveira Junior (2005).

Figura 8 – Apresentada ao usuário da estação de rede pelo Agente

No Gerente, o componente utilizado no Agente é utilizado para receber as informações e montar estas informações no mesmo formato em que o Agente as tratou, ou seja, o Gerente enxerga as informações dos componentes da estação do mesmo modo que foi definido pelo servidor (OLIVEIRA JUNIOR, 2005).

A figura 9 abaixo mostra o funcionamento do Agente e Gerente.



Fonte: Oliveira Junior (2005).

Figura 9 - Esquema de funcionamento entre agente e gerente

Mas o software não guarda os dados coletados em nenhum banco de dados que possa manter um histórico para futuras consultas, se por algum motivo venha a ocorrer um problema com alguma estação ou a mesma estiver desligada não será possível consultar as informações. O software não possui nenhum relatório para consultar as configurações de uma estação, apenas permite consultar informações na *console* de gerenciamento quando a estação estiver ligada e com o software Gerente executando.

3 DESENVOLVIMENTO DO TRABALHO

Neste capítulo são abordados aspectos relevantes e detalhes sobre as funcionalidades do software desenvolvido. Serão vistos também os requisitos do software, sua especificação através de *Unified Modeling Language* (UML), ferramentas de desenvolvimento utilizadas e resultados.

3.1 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Este software deve ter os seguintes requisitos funcionais:

- a) coleta de informações: o software cliente instalado nos computadores de rede deverá coletar informações de softwares instalados e enviá-las ao software servidor instalado em uma estação de gerência;
- b) armazenamento dos dados: o software servidor instalado na estação de gerência deverá armazenar os dados coletados no Registro do Windows em um servidor para futuras consultas em caso de perdas de dados na estação;
- c) notificação ao administrador: o software servidor deverá notificar o administrador com uma mensagem de alerta no *console* de administração ou por correio eletrônico quando houver mudanças de software em alguma estação da rede;
- d) relatórios: a estação de gerência deverá permitir ao administrador de rede gerar relatórios diversos com as informações coletadas no inventário, sendo possível gerar relatório de softwares instalados por computador, relatório de computadores por softwares e relatório de alterações de softwares por computador.

Os requisitos não funcionais são:

- a) usabilidade: o software cliente deverá ser de fácil instalação, apenas copiando um arquivo executável no computador. O software servidor deverá ter uma interface amigável e intuitiva ao usuário e deverão ser usados ícones e menus para acessar as funcionalidades;
- b) software: tanto o software servidor quanto o cliente deverão se comunicar utilizando o protocolo SMB e deverão funcionar em sistemas operacionais Windows 2000 e Windows XP.

3.2 ESPECIFICAÇÃO

Para especificação do software adotou-se a *Unified Modeling Language* (UML), utilizando os diagramas de casos de uso, de classe e de atividades. Foi utilizada a ferramenta Enterprise Architect para o desenvolvimento dos diagramas.

3.2.1 Diagrama de casos de uso

A Figura 10, diagrama de casos de uso, especifica o funcionamento do software cliente e servidor que tem por finalidade coletar as informações das estações e cadastrá-las em um banco de dados.

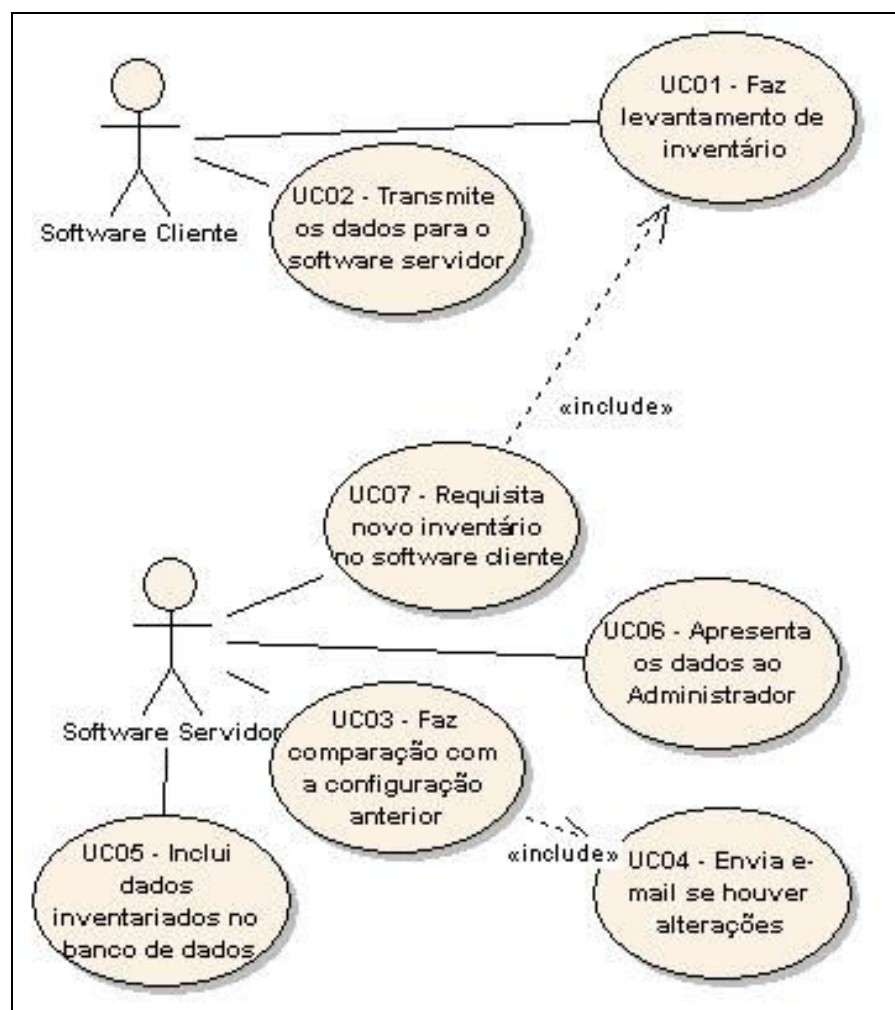


Figura 10 – Diagrama de casos de uso

Abaixo seguem o detalhamento de cada caso de uso encontrado na figura 10:

- a) UC01 - faz levantamento de inventário: efetua o levantamento das informações de inventário para enviar posteriormente;
- b) UC02 - transmite os dados para o software servidor: faz a transmissão dos dados para o gerenciador através da rede;
- c) UC03 - faz comparação com a configuração anterior: compara o inventário atual com o inventário armazenado no banco de dados;
- d) UC04 - envia e-mail se houver alterações: envia um e-mail para o administrador sempre que houver alguma alteração de software, seja uma nova instalação ou uma desinstalação;
- e) UC05 - inclui dados inventariados no banco de dados: faz a inclusão de todos os dados inventariados no banco de dados;
- f) UC06 - apresenta dados ao Administrador: possibilita ao Administrador consultar os dados de todas as estações de rede através da *console* ou através de relatórios;
- g) UC07 - requisita novo inventário no software cliente: faz uma solicitação para o software cliente na estação de rede para que seja feito um levantamento de inventário.

3.2.2 Diagrama de Classe

O diagrama de classes demonstra a estruturação das classes utilizadas na implementação do software. Na figura 11 pode-se ver a classe *TInfHardware* e suas subclasses.

A classe *TInfHardware* é a principal classe do sistema, sendo instanciada tanto no software cliente quanto no software servidor. Esta classe possui subclasses especializadas para todos os itens encontrados no equipamento de rede, seja hardware ou software.

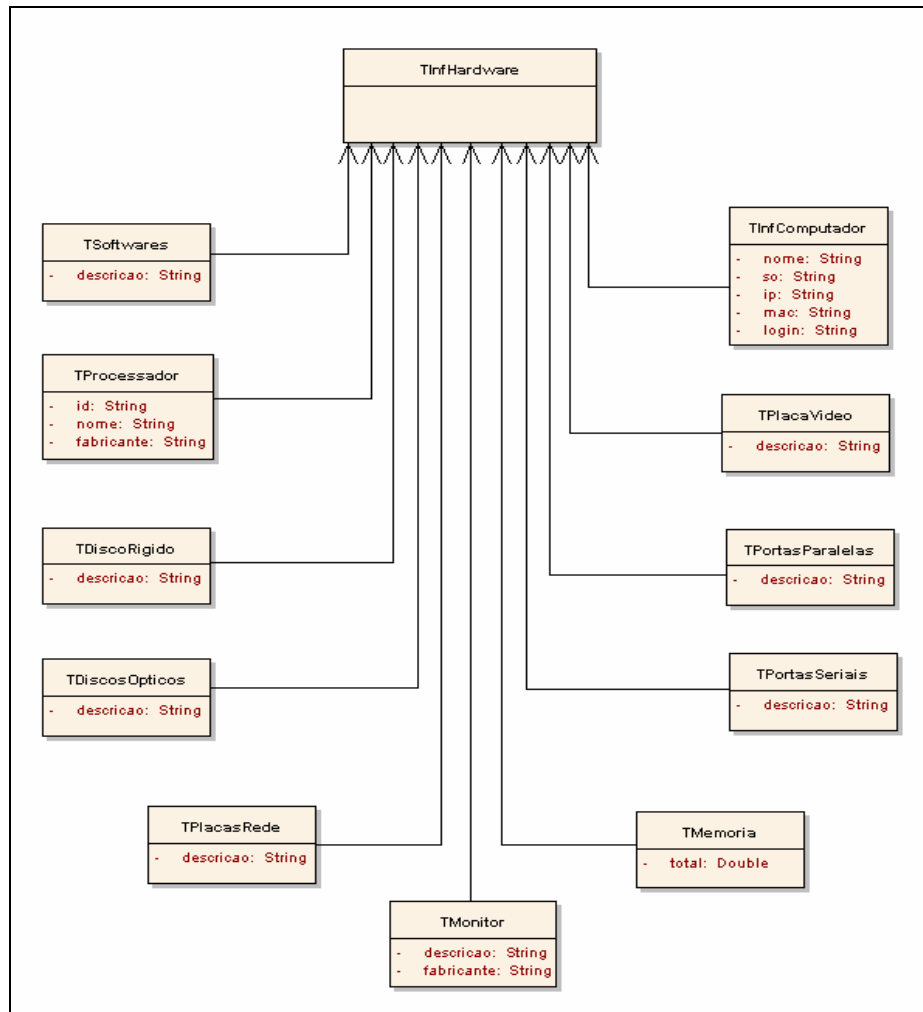


Figura 11 – Diagrama de classes

3.2.3 Diagrama de Atividades

O diagrama de atividades apresentado na figura 12 demonstra os procedimentos executados no software cliente e software servidor, e também como ocorre a interação entre os dois.

Quando o software cliente é executado em um computador de rede, automaticamente é feito um inventário de hardware e software e enviado para a estação servidora (software servidor). O software servidor, após receber os dados, compara os softwares com o que já estavam cadastrados para o computador no banco de dados e caso algum software tiver sido removido ou instalado, envia um e-mail para o administrador de rede e depois salva no banco de dados as alterações.

O inventário dos computadores poderá ser acessado pelo administrador de rede pela

console através das telas de consultas ou pelos relatórios.

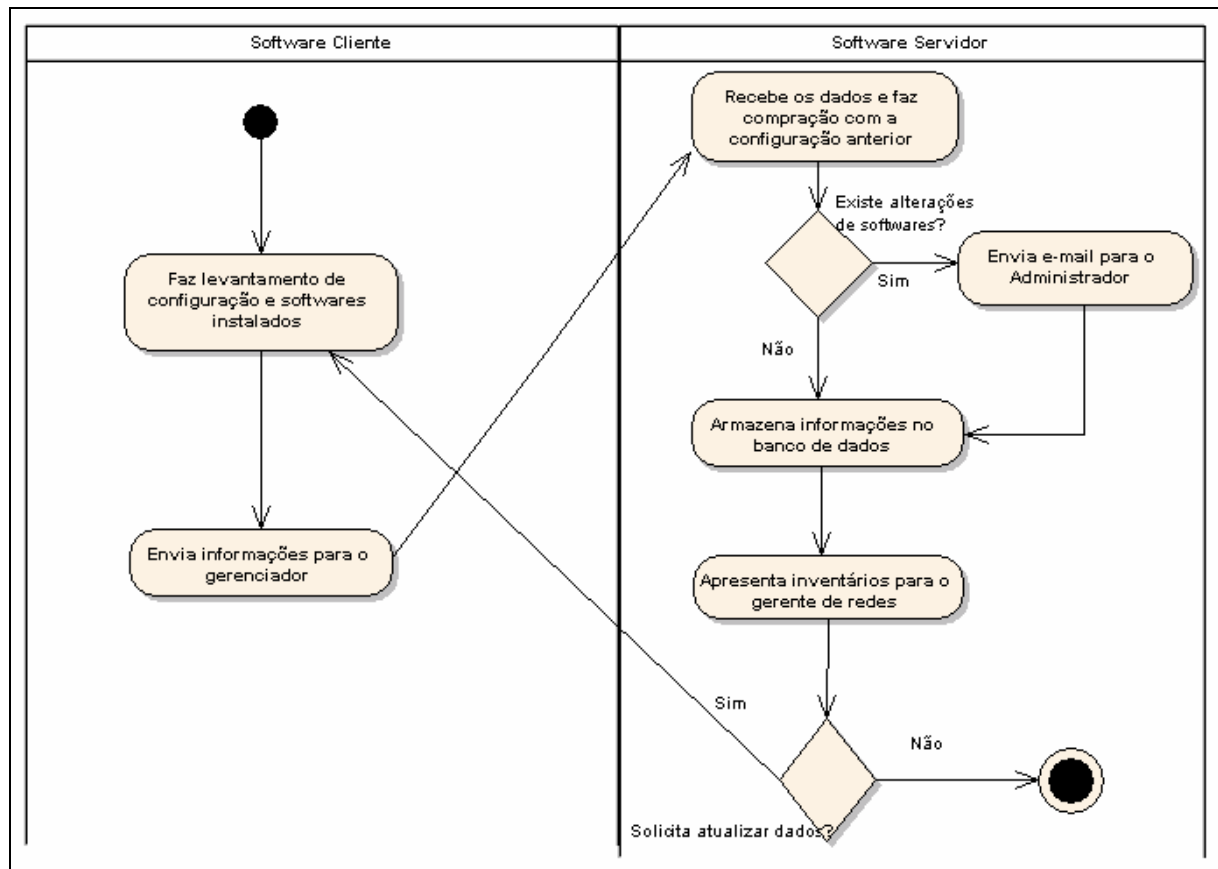


Figura 12 – Diagrama de atividades

3.3 IMPLEMENTAÇÃO

A seguir é apresentado o detalhamento da implementação do software, de acordo com as especificações apresentadas neste documento.

3.3.1 Técnicas e ferramentas utilizadas

Para implementação do software cliente e software servidor foi utilizada a linguagem *Object Pascal DELPHI 7* da Borland (CANTU, 2003), visto que o trabalho desenvolvido é continuação do desenvolvido por Oliveira Junior (2005). Para armazenar as informações coletadas foi utilizado o banco de dados MySQL. O Delphi possui recursos que facilitam a manipulação de informações contidas no Registro do Windows e é compatível com o

Windows 2000 e XP. O componente uInformacoes.pas contém toda a implementação necessária para coletar as informações do Registro do Windows no software cliente. As informações lidas por este componente são armazenadas temporariamente em suas propriedades que em seguida são enviadas para o software servidor. O quadro 2 abaixo mostra uma parte do método LeRegistro que faz toda a leitura de informações sobre componentes e softwares instalados no computador, onde são lidas informações sobre os softwares instalados.

```

procedure AchaSoftwares(prChave : String);
var
  wContadorChaves : Integer;
  wSubKeys      : TStringList;
  wValor        : String;
begin
  if Self.FRegistro.KeyExists(prChave) then
  begin
    Self.FRegistro.OpenKey(prChave,False);
    wSubKeys := TStringList.Create;
    Self.FRegistro.GetKeyNames(wSubKeys);
    if wSubKeys.Count <> 0 then
    begin
      for wContadorChaves := 0 to wSubKeys.Count - 1 do
        AchaSoftwares(prChave + '\' + wSubKeys.Strings[wContadorChaves]);
      end
    else
      if Self.FRegistro.ReadString('DisplayName') <> '' then
      begin
        wValor := Self.FRegistro.ReadString('DisplayName');
        Self.FSoftwares.add;
        TSoftwares(Self.FSoftwares.items[Self.FSoftwares.count - 1]).descricao := wValor;
      end;
    end;
  end;
end;

```

Quadro 2 – Procedimento que lê as informações do Registro sobre softwares instalados

No software servidor foi utilizado o mesmo componente uInformacoes.pas para receber as informações e montar no mesmo formato em que o software cliente as coletou, ou seja, o software servidor trata as informações da mesma forma em que o software cliente as tratou.

Para a transmissão das informações entre o software cliente e o software gerente foi utilizado o componente uMailSlot.pas desenvolvido por Oliveira Junior (2005). Este componente quebra as informações em partes porque não é possível transmitir todas as informações de uma estação de uma só vez. No quadro 3 pode ser observado que a mensagem é enviada em partes para que o software servidor receba as informações do inventário completas.

```

procedure TMailSlot.EnviaMensagem(Destino: String; Mensagem: TStrings);
var
  wContador,
  wTamanho : Integer;
begin
  if length(TrimLeft(TrimRight(Destino))) = 0 then
    exit;
  Self.FMicroDestino := Destino;
  wTamanho := length(Mensagem.Text);

  if wTamanho <= 255 then
    begin
      with Self.FMensagemEnviar do
        begin
          Clear;
          AddStrings(Mensagem);
          Insert(0,Self.FMicroOrigem);
          Insert(1,Self.FUsuario);
        end;
      Self.Envia;
    end
  else
    begin
      with Self.FMensagemEnviar do
        begin
          Clear;
          Add('#INICIO#');
          Insert(0,Self.FMicroOrigem);
          Insert(1,Self.FUsuario);
          Self.Envia;

          for wContador := 0 to Mensagem.Count - 1 do
            begin
              Clear;
              Add(Mensagem.Strings[wContador]);
              Insert(0,Self.FMicroOrigem);
              Insert(1,Self.FUsuario);
              Insert(2,'#CONTINUA#');
              Self.Envia;
            end;
            Clear;
            Add('#FIM#');
            Insert(0,Self.FMicroOrigem);
            Insert(1,Self.FUsuario);
            Self.Envia;
          end;
        end;
    end;
end;

```

Quadro 3 – Procedimento que lê as informações do Registro sobre softwares instalados

3.3.2 Operacionalidade da implementação

Conforme descrito no diagrama de caso de uso, o “Software de Inventário de Software de Equipamentos de Rede Utilizando *Session Message Block*” é dividido em duas partes:

software cliente e software gerente.

O software cliente é o programa que é instalado em todas as estações e logo após a sua inicialização, faz a leitura nas chaves do Registro do Windows para colher informações de inventário e em seguida envia os dados para o software servidor instalado em uma estação de gerencia. O software cliente além de colher informações do computador e enviar ao software servidor também é responsável por apresentar ao próprio operador da estação os dados de inventário da estação.

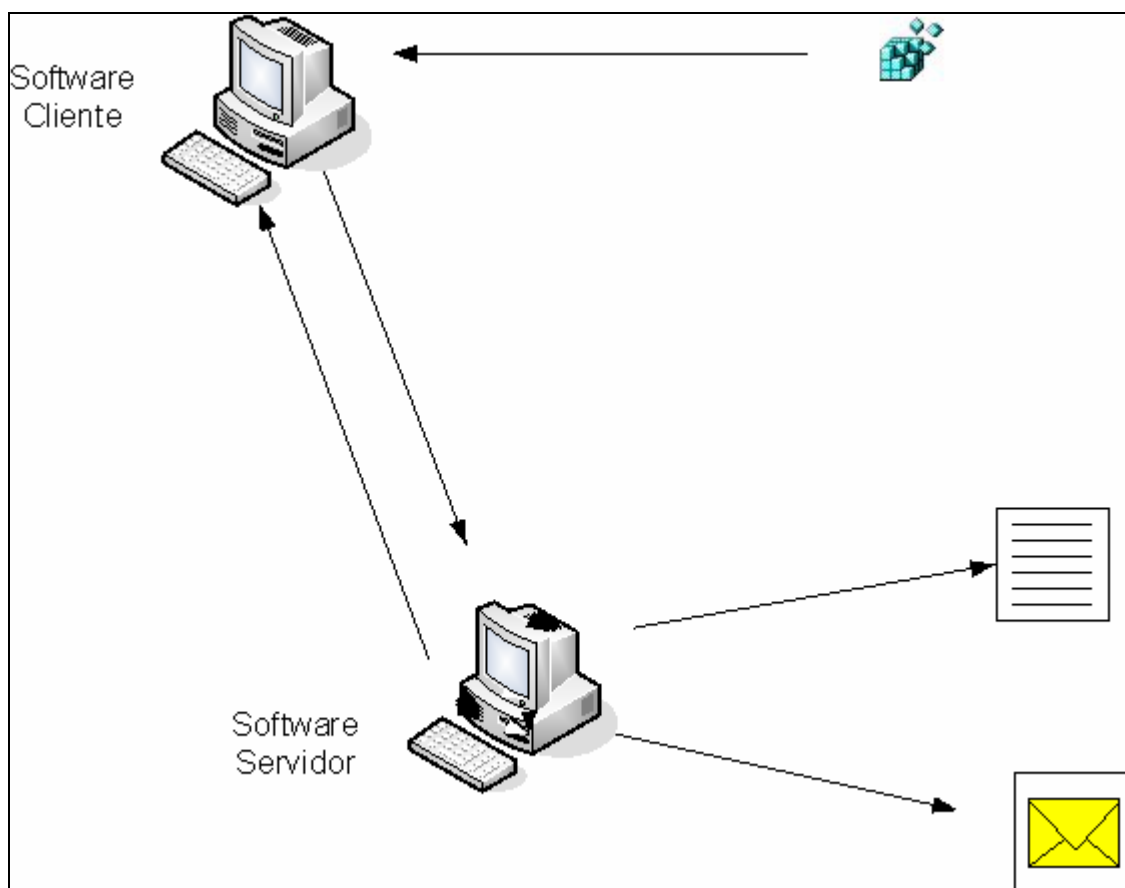


Figura 13 – Esquema de funcionamento entre software cliente e software servidor

O software cliente cria o arquivo ConfigMicroServ.ini no diretório C:\WINDOWS onde grava o nome da estação servidora para qual vai enviar as informações de inventário. O software cliente quando instanciado apresenta um ícone junto à barra de tarefas do windows e clicando neste ícone o usuário local pode visualizar as informações de hardware e de softwares instalados no seu computador, conforme pode ser visto na figura 14.

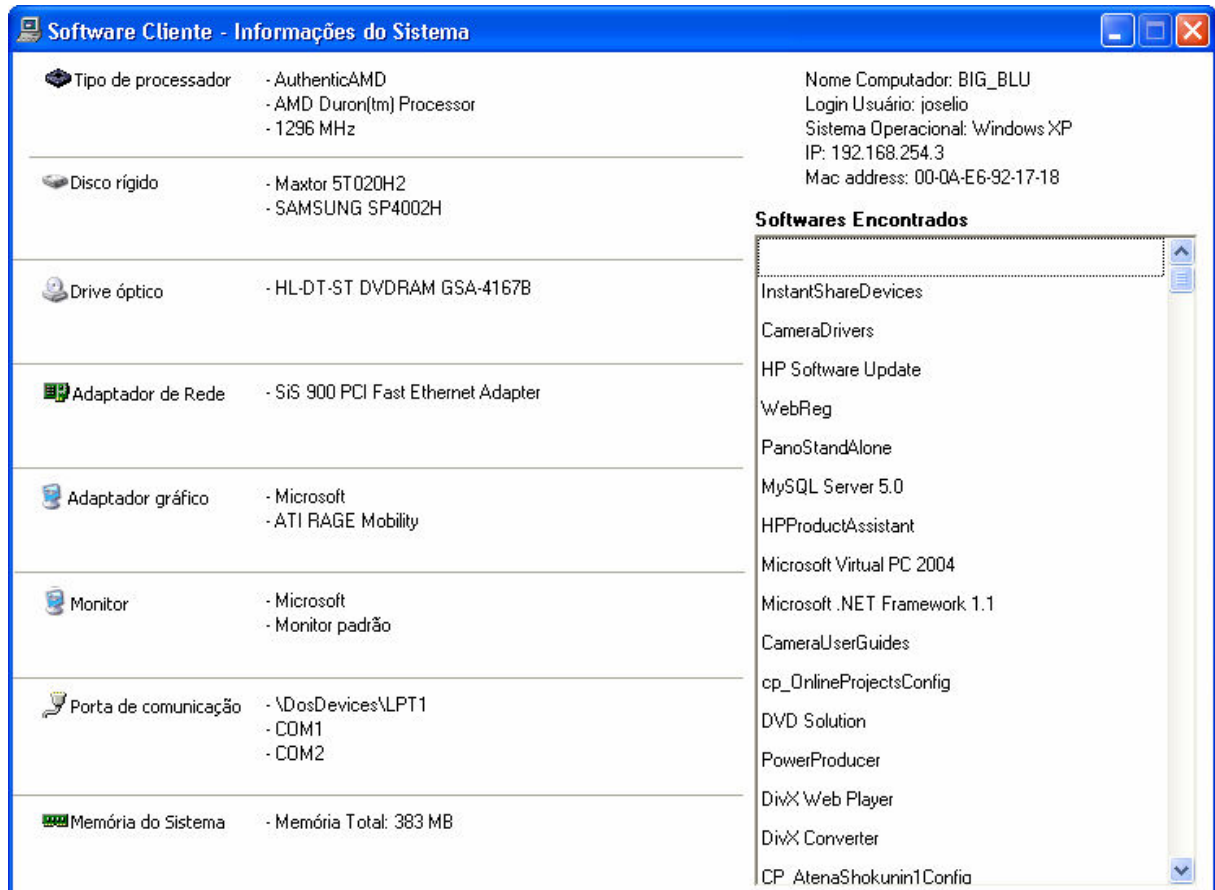


Figura 14 – Software Cliente

O software servidor é responsável por receber e tratar todas as informações de inventários recebidas das estações de rede, salvá-las no banco de dados e as apresentar ao Gerente de Redes. Esta apresentação pode ser por uma tela principal do software servidor onde o inventário de cada estação de rede é apresentado separadamente através de um menu *Tree-View*, tornando simples a sua operação e visualização, como pode ser visto na figura 15.

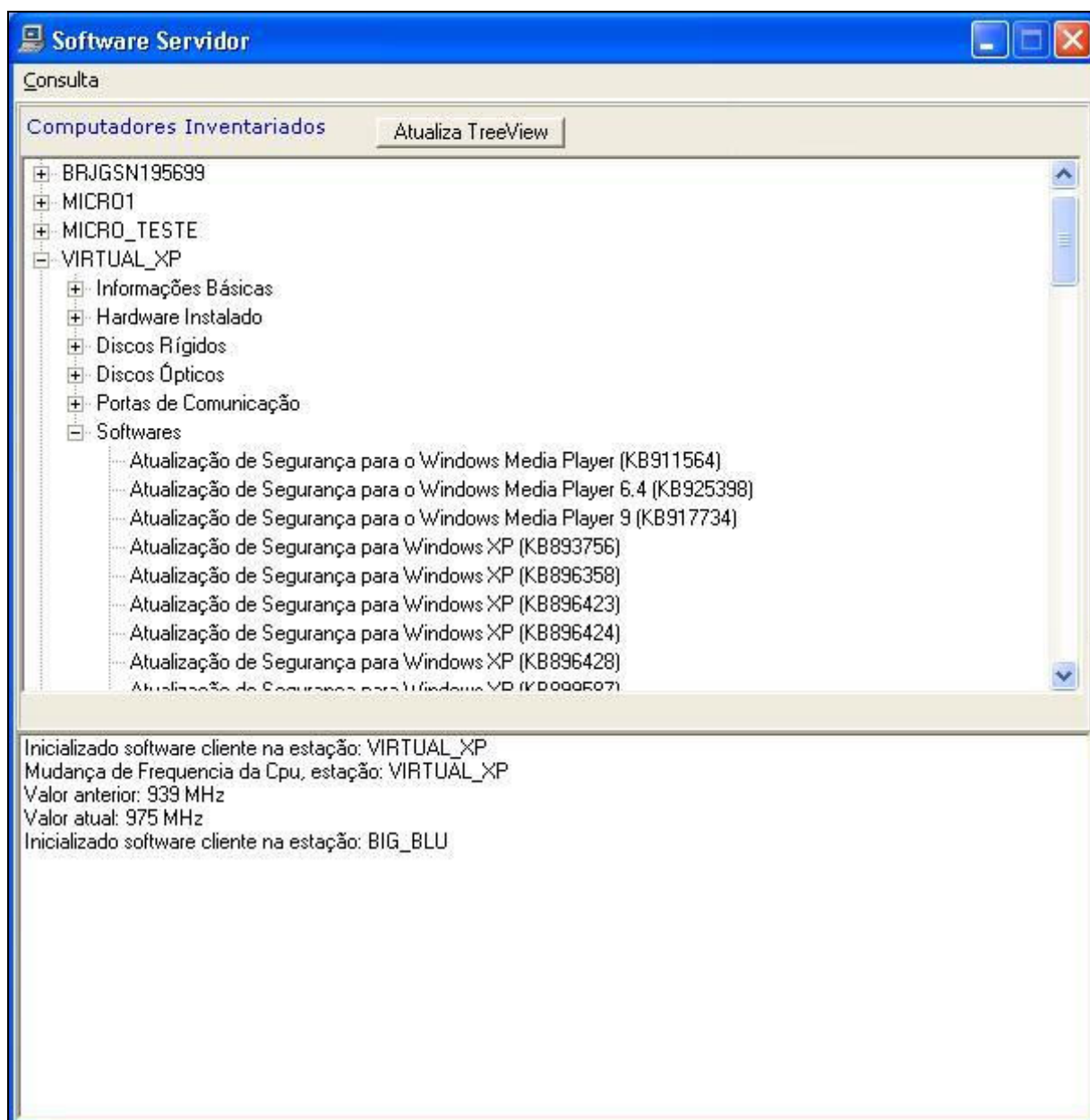
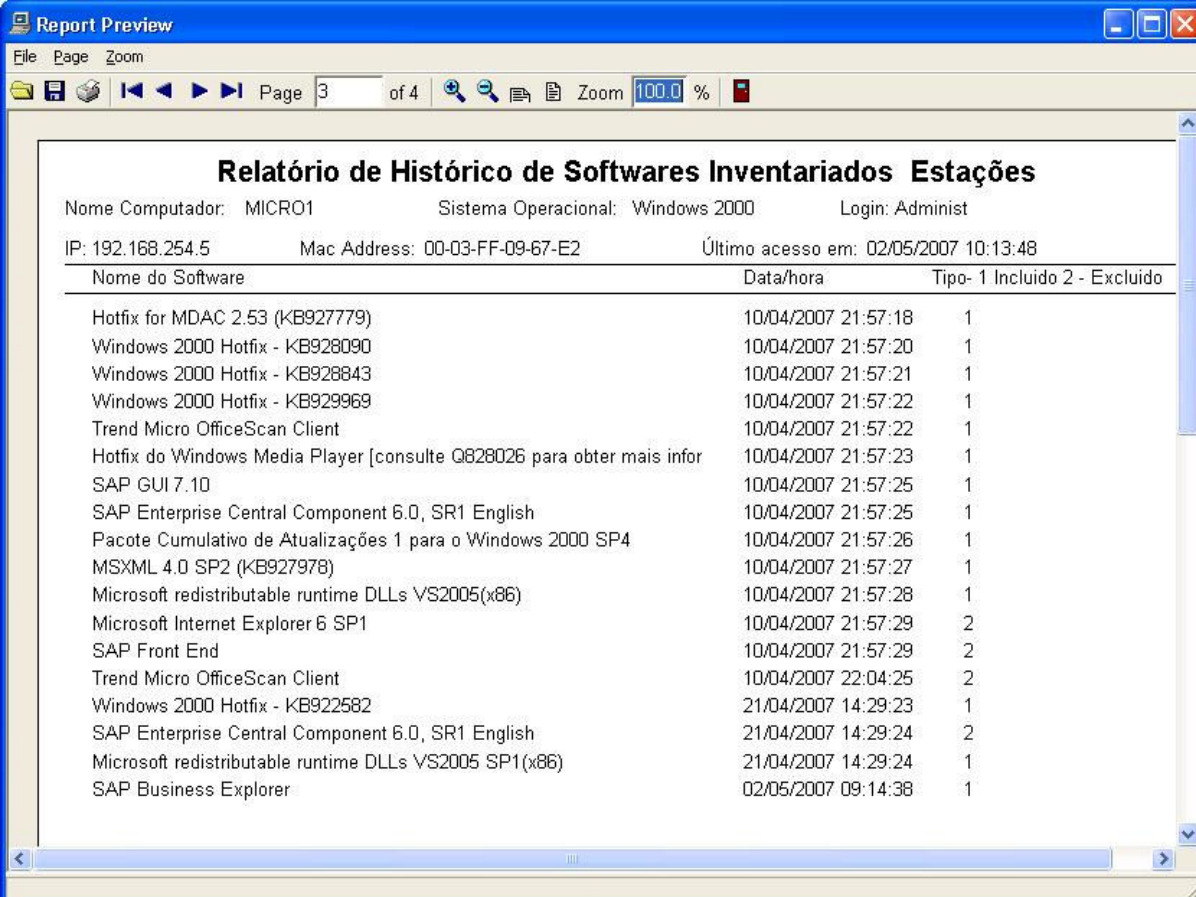


Figura 15 – Tela software servidor

Também, se for de interesse do Gerente de Redes, ele poderá consultar as mesmas informações em relatórios de consultas agrupados por estações ou softwares, e relatórios que refletem a situação atual nas estações de rede ou relatório de históricos de softwares instalados e removidos em todas as estações de rede. Na figura 16 pode-se observar um exemplo do relatório, onde é mostrado o nome do software, data, hora e se ele foi removido ou instalado, possibilitando ao Gerente de Redes um melhor entendimento das ocorrências nos computadores inventariados.



The screenshot shows a 'Report Preview' window with a menu bar (File, Page, Zoom) and a toolbar. The report title is 'Relatório de Histórico de Softwares Inventariados Estações'. It displays metadata for computer 'MICRO1' (IP: 192.168.254.5, Mac: 00-03-FF-09-67-E2, OS: Windows 2000, Login: Administ) and the last access time (02/05/2007 10:13:48). The main table lists software updates with columns for software name, date/time, and type (1: Included, 2: Excluded).

Nome do Software	Data/hora	Tipo- 1 Incluído 2 - Excluído
Hotfix for MDAC 2.53 (KB927779)	10/04/2007 21:57:18	1
Windows 2000 Hotfix - KB928090	10/04/2007 21:57:20	1
Windows 2000 Hotfix - KB928843	10/04/2007 21:57:21	1
Windows 2000 Hotfix - KB929969	10/04/2007 21:57:22	1
Trend Micro OfficeScan Client	10/04/2007 21:57:22	1
Hotfix do Windows Media Player [consulte Q828026 para obter mais infor	10/04/2007 21:57:23	1
SAP GUI 7.10	10/04/2007 21:57:25	1
SAP Enterprise Central Component 6.0, SR1 English	10/04/2007 21:57:25	1
Pacote Cumulativo de Atualizações 1 para o Windows 2000 SP4	10/04/2007 21:57:26	1
MSXML 4.0 SP2 (KB927978)	10/04/2007 21:57:27	1
Microsoft redistributable runtime DLLs VS2005(x86)	10/04/2007 21:57:28	1
Microsoft Internet Explorer 6 SP1	10/04/2007 21:57:29	2
SAP Front End	10/04/2007 21:57:29	2
Trend Micro OfficeScan Client	10/04/2007 22:04:25	2
Windows 2000 Hotfix - KB922582	21/04/2007 14:29:23	1
SAP Enterprise Central Component 6.0, SR1 English	21/04/2007 14:29:24	2
Microsoft redistributable runtime DLLs VS2005 SP1(x86)	21/04/2007 14:29:24	1
SAP Business Explorer	02/05/2007 09:14:38	1

Figura 16 – Relatório de Histórico de Softwares Inventariados Estações

O software servidor ao receber as informações de inventário das estações também faz uma comparação com as informações já cadastradas no banco de dados para cada estação para descobrir se houve modificações nos softwares instalados na estação de rede desde o último inventário e grava estas alterações em uma tabela de históricos de softwares. Após isto, envia um e-mail para o Gerente de Redes para notificar o ocorrido.

Foi configurado no software servidor que num intervalo de 3 horas solicite a cada software cliente da rede os dados do inventário para que as informações no banco de dados fiquem sempre atualizadas.

3.4 RESULTADOS E DISCUSSÃO

Nos testes executados em laboratório, tanto o software cliente quanto o software servidor mostraram-se eficientes ao executar os inventários em computadores com Windows 2000 e Windows XP. Foram realizados testes de inventário de hardware e softwares e

confrontados os resultados nas estações inventariadas.

No software servidor foram testados os relatórios Softwares por Computador, Computadores por Software e Histórico de Softwares Inventariados nas Estações.

Os principais testes realizados e seus resultados são demonstrados no quadro 4:

Descrição do teste	Resultado obtido
Executar software cliente em estações Windows 2000 e Windows XP	O inventário coletou as informações e enviou para o software servidor utilizando o protocolo SMB sem apresentar erros.
Executar software servidor	O software servidor recebeu as informações inventariadas nas estações e cadastrou no banco de dados.
Simulação de instalação e remoção de softwares	Foi feita a simulação de instalação e remoção de software nas estações e em seguida executado um novo inventário. As informações foram cadastradas com sucesso na tabela historico_softwares_inventariados_estações.
Envio de e-mail alertando alterações de softwares nas estações	O software servidor enviou e-mails todas as vezes que houve mudanças nos softwares nas estações.

Quadro 4 – Resultado dos testes em laboratório

Comparando o software desenvolvido neste trabalho com o desenvolvido por Oliveira Junior (2005), pode-se observar principalmente o inventário de softwares que não existia, assim como o envio de e-mail ao Gerente de Rede, um item importante implementado neste software. Todas as alterações de softwares nas estações são facilmente consultadas no relatório de históricos que pode ser acessado a qualquer momento mesmo que a estação de que se deseja as informações estiver desligada.

4 CONCLUSÕES

A realização deste trabalho demonstrou a possibilidade de executar um inventário de hardware e software em uma rede de computadores e disponibilizar estas informações para o Gerente de Rede de forma simples, auxiliando e evitando o uso indevido de softwares não licenciados. Este tipo de gerenciamento está se tornando cada vez mais comum em empresas preocupadas em manter o uso de softwares legalizados em seu parque de computadores.

Como foi relatado ao longo deste trabalho, as informações do inventário foram extraídas do Registro do Windows sem maiores complicações, visto que existe documentação farta em livros e na própria Internet para ajudar a entender como é o seu funcionamento.

O protocolo SMB utilizado para implementar a comunicação entre o software cliente e o software servidor é um protocolo específico para compartilhamento de arquivos e comunicação entre computadores que é parte integrante dos sistemas operacionais Windows. Por isso mostrou-se muito eficiente e flexível, podendo-se executar com ele quase tudo em um gerenciador de arquivos, não comprometendo o desempenho dos computadores e da própria rede.

Todos os requisitos elencados neste trabalho foram implementados no software, cujo objetivo final é um software que forneça o inventário completo dos computadores ligados a uma rede por meio de uma console ou relatórios que poderão ser analisados a qualquer momento.

Uma limitação do software desenvolvido neste trabalho é a de funcionar somente em sistemas operacionais Windows, mais especificamente Windows 2000 e Windows XP.

O trabalho do Oliveira Junior (2005) que foi utilizado como base para este trabalho foi uma ótima escolha, pois o software foi muito bem desenvolvido com componentes que funcionaram com algumas modificações e inclusões para suprir as novas necessidades deste software.

4.1 EXTENSÕES

Como sugestão para extensão deste trabalho, sugere-se a implementação do software cliente e software servidor para o sistema operacional Linux. Também sugere-se a

implementação de uma *console* de gerenciamento via WEB para facilitar o acesso do Gerente de Redes aos dados mesmo estando distante da estação servidora.

REFERÊNCIAS BIBLIOGRÁFICAS

CANTU, M. **Dominando o Delphi 7: a bíblia**. Tradução Kátia Aparecida Roque. São Paulo: Pearson, 2003.

DATAPREV. **CACIC: Configurador Automático e Coletor de Informações Computacionais**. [S.l.], [2005?]. Disponível em: <<http://guialivre.governoeletronico.gov.br/cacic/sisp2>>. Acesso em: 26 ago. 2006.

IVIRTUA SOLUTIONS. **Trauma zer0**. Montenegro, [2006?]. Disponível em: <<http://www.traumazero.com.br/index.php?conteudo=solutions&pg=dif>>. Acesso em: 26 ago. 2006.

LOPES, R. V.; SAUVÉ, J. P.; NICOLLETTI, P. S. **Melhores práticas para Gerência de Redes de Computadores**. Rio de Janeiro: Campus, 2003. 373 p.

MICROSOFT CORPORATION. **Descrição do Registro do Microsoft Windows**. [S.l.], 2005a. Disponível em: <<http://support.microsoft.com/kb/256986>>. Acesso em: 26 ago. 2006.

_____. **Estrutura do Registro**. [S.l.], 2005b. Disponível em > <<http://technet2.microsoft.com/WindowsServer/pt-BR/Library/28e3337c-70ff-41e1-86ef-2581350712a91046.mspx?mfr=true>>. Acesso em: 11 mar. 2007.

MICROSOFT CORPORATION, INTEL CORPORATION, **File Sharing Protocol: help**. Version 2.0, 1988. [S.l.], 1994. Disponível em: <<ftp://ftp.microsoft.com/developr/drg/CIFS/SMBHLP.ZIP>>. Acesso em: 26 ago. 2006.

OLIVEIRA JUNIOR, E. N. **Protótipo de software para gerência de patrimônios de equipamentos de uma rede utilizando session message block**. 2005. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

PÉRICAS, F. A. **Redes de computadores: conceitos e a arquitetura internet**. Blumenau: EdiFURB, 2003. 158 p.

SAMBA. **Just what is SMB?**. [S.l.], 2002. Disponível em: <<http://samba.anu.edu.au/cifs/docs/what-is-smb.html>>. Acesso em: 26 ago. 2006.

WINGUIDES NETWORK FOR WINDOWS. **Registry guide for Windows**. [S.l.], 2006. Disponível em: <<http://www.winguides.com/article.php?id=1&guide=registry>>. Acesso em: 26 ago. 2006.