

**FACULDADE ESTÁCIO DE SÁ DE OURINHOS
TECNOLOGIA EM REDES DE COMPUTADORES**

**PAULO HENRIQUE SALANDIN
RICARDO JOSÉ DAS CHAGAS**

PROJETO SNMP

**OURINHOS
2010**

**FACULDADE ESTÁCIO DE SÁ DE OURINHOS
TECNOLOGIA EM REDES DE COMPUTADORES**

**PAULO HENRIQUE SALANDIN
RICARDO JOSÉ DAS CHAGAS**

PROJETO SNMP

**Trabalho apresentado à Profª Esp.
Maria Alessandra Dubowski Nascimento
como requisito parcial à aprovação na
disciplina de protocolos de comunicação**

Professor: Regiane

**OURINHOS
2010**

SUMÁRIO

1 INTRODUÇÃO	3
2 CLIENTE	4
3 IDENTIFICAÇÃO DOS EQUIPAMENTOS	5
3.1 TOPOLOGIA.....	6
4 NECESSIDADES	7
5 ÁREAS DA GERENCIA	8
5.1 GERÊNCIA DE SEGURANÇA	8
5.1.1 Software de gerência de segurança.....	9
5.1.1.1 Active Directory (AD)	9
5.1.1.2 Kaspersky.....	10
5.2 GERÊNCIAS DE FALHAS.....	12
5.2.1 SOFTWARE DE GERENCIA DE FALHAS	13
5.2.1.1 Spectrum's Alarm	13
6 CONCLUSÃO.....	15
7 REFERÊNCIAS.....	16

1 INTRODUÇÃO

O gerenciamento de uma rede de local, vem tendo uma grande preocupação atualmente em relação a segurança, falhas, desempenho, configuração entre outros. Neste projeto, iremos implementar o protocolo SNMP na rede de um cliente tendo em vista a segurança e a facilidade em detecção de falhas e defeitos isolados.

2 CLIENTE

A Empresa Inter Seguros Ltda., situada na Av. Brasil, nº 1507, Centro da cidade de Santa Cruz do Rio Pardo-SP, com o telefone (14) 3333-7070, atua na área de Seguros Empresariais.

A Inter Seguros Ltda. trabalha com o comércio e vendas de seguros empresarias a onze anos.

Fundada na cidade de Santa Cruz do Rio Pardo no fim do ano de 1999, tem como proprietários os irmãos Henrique, Humberto e Fernando da Silva. Hoje a empresa é constituída de cinco funcionários e três sócios. A Inter Seguros consiste de cinco departamentos: Administrativo, Financeiro, Sinistro, Calculo e Recepção.

3 IDENTIFICAÇÃO DOS EQUIPAMENTOS

Equipamentos: Seis notebooks, um computador, um Servidor, um Switch 10/100 3com.

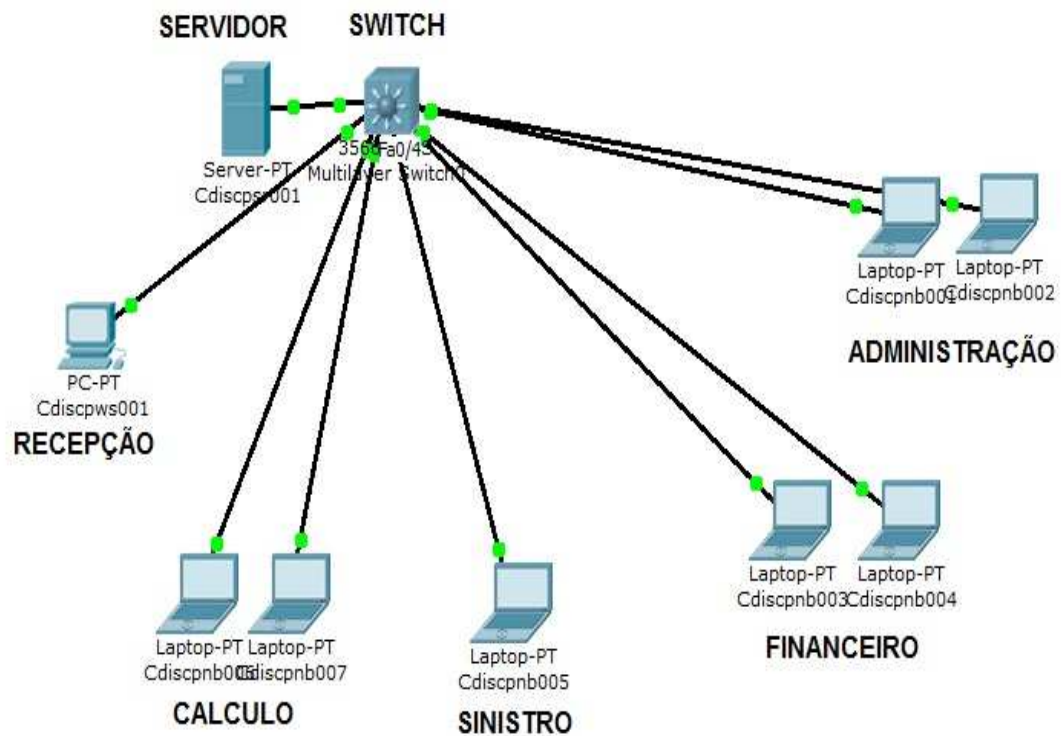
Conexão: A conexão é feita somente via cabo. O servidor está configurado como servidor de DHCP, dando IP as máquinas na faixa de 10.20.30.50 a 10.20.30.100, essa faixa de IP é somente para os computadores, ficando o servidor com o IP fixo 10.20.30.254.

Servidor: Sistema Operacional: Server 2008.

Sistema: Os computadores do cliente, possuem o Windows XP PRO.

3.1 TOPOLOGIA

A rede possui um servidor de DHCP que está distribuindo o IP para os micros. Segue o mapa da rede a baixo:



4 NECESSIDADES

Freqüentemente ocorrem falhas nos dispositivos da rede, e geralmente é gasto um tempo excessivo desde a detecção da falha quanto a resolução da mesma. Com isso havendo a necessidade de a implementação de um sistema que gerencie e isole as falhas da rede local para que ela consiga continuar funcionando, mesmo havendo uma falha na rede e obter uma solução rápida das falhas.

Outro ponto que está preocupando o cliente, é em relação a “vazamento” de informação, onde um funcionário outra pessoa qualquer pode ter acesso a uma máquina e copiar as informações para vender ou para uso impróprios. Necessitando então bloquear todo e qualquer tipo de conexão externa com a empresa e fazer a filtragem da internet.

5 ÁREAS DA GERENCIA

Devido a necessidade do cliente, será implementada em sua rede a Gerência de Segurança e Gerência de Falhas e Defeitos, que nada mais é que as áreas que englobam melhor o requerimento do mesmo.

5.1 GERÊNCIA DE SEGURANÇA

O objetivo do gerenciamento de segurança é o de dar subsídios à aplicação de políticas de segurança, que são os aspectos essenciais para que uma rede baseada no modelo OSI seja operada corretamente, protegendo os objetos gerenciados e o sistema de acessos indevidos de intrusos. Deve providenciar um alarme ao gerente da rede sempre que se detectarem eventos relativos à segurança do sistema.

São distinguidos dois conceitos no modelo OSI em relação à segurança:

- Arquitetura de Segurança do Modelo OSI;
- Funções de Gerenciamento de Segurança, estas compondo a área funcional de gerência de segurança.

O objetivo da Arquitetura de Segurança do modelo OSI é o de dar uma descrição geral dos serviços de segurança e dos mecanismos associados a este, e de definir em que posição do modelo de referência situam-se os serviços de segurança e os seus mecanismos associados. Para isso, definem-se os seguintes serviços:

- Autenticação tanto de entidades pares quanto da origem dos dados (authentication);

- Controle de acesso aos recursos da rede (access control);
- Confidencialidade dos dados (confidentiality);
- Integridade dos dados (integrity);
- A não-rejeição ou não-repudição (non-repudiation);

Então, os objetivos do gerenciamento de segurança são:

- O fornecimento de relatórios de eventos relativos à segurança e o fornecimento de informações estatísticas;
- A manutenção e análise dos registros de histórico relativos à segurança;
- A seleção dos parâmetros dos serviços de segurança;
- A alteração, em relação à segurança, do modo de operação do sistema aberto, pela ativação e desativação dos serviços de segurança.

5.1.1 Software de gerência de segurança

5.1.1.1 Active Directory (AD)

O Active Directory (AD), é uma maneira de organizar e simplificar o acesso aos recursos de sua rede centralizando-os; Bem como, reforçar a segurança e dar proteção aos objetos da database contra intrusos, ou controlar acessos dos usuários internos da rede.

Após analisar as necessidades do cliente, foi identificado que seria necessário a implementação de um Domínio usando o Active Directory, onde haveria políticas de

segurança, que se aplicaria em senhas, acesso a determinados arquivos e algumas restrições, tais como: uso de pen drive, disquete, gravar DVD, etc.

Cada usuário terá uma conta com senha para acessar a sua máquina e essa conta somente irá acessar somente a máquina desse usuário, essa senha será trocada de quinze em quinze dias e mínimo de um dia para permanecer com a senha, haverá a necessidade de caracteres especiais (@, #, &, etc...), ela não poderá ser repetida em uma dessas trocas antes de ter mudado a senha mais de vinte e cinco vezes, e o mínimo de sete caracteres por senha. Cada setor da empresa, terá uma pasta criada no servidor, onde somente o funcionário do setor terá acesso a essa pasta, os únicos que terão acesso total serão os proprietários da empresa.

5.1.1.2 Kaspersky

Outra necessidade seria um antivírus corporativo, que no caso seria o Kaspersky Total Space Security, que será implementado junto ao servidor de domínio, para uma análise profunda da rede do cliente e com mais segurança nos dados.

O Kaspersky Total Space Security fornece proteção integrada para redes corporativas de qualquer tamanho ou nível de complexidade, contra todos os tipos de ameaças atuais da Internet.

O Kaspersky Total Space Security controla todos os dados enviados e recebidos, incluindo e-mails, p tráfego da Web e todas as interações de rede. O produto compreende componentes para a proteção de estações de trabalho e dispositivos móveis, garantindo aos usuários um acesso seguro e rápido aos

recursos de informação da empresa e à Internet, além da comunicação segura por e-mail.

Destaques do Produto

- Proteção integrada contra vírus, spyware, ataques de hackers e spam em todos os níveis da rede corporativa, das estações de trabalho aos gateways da Internet

- Proteção proativa contra os programas mal-intencionados mais recentes
- Proteção para servidores de arquivos e servidores de e-mail
- Verificação do tráfego da Web (HTTP/FTP) em tempo real
- Escalabilidade
- Quarentena de estações de trabalho infectadas
- Bloqueio de epidemias de vírus
- Relatórios centralizados sobre o status do sistema

Recursos Adicionais

- Instalação e administração centralizadas
- Suporte para Cisco® NAC (Network Admission Control)
- Suporte para equipamentos de hardware de proxy
- Filtragem do tráfego da Internet de acordo com listas de servidores, tipos de objetos e grupos de usuários confiáveis
- Tecnologia iSwift, que evita a repetição desnecessária de verificações de dados na rede
- Redistribuição inteligente de recursos durante as verificações completas do sistema

- Firewall pessoal com IDS e IPS
- Segurança ao trabalhar em qualquer tipo de rede, incluindo WiFi
- Proteção contra ataques de phishing e spam
- Neutralização remota usando o Intel® Active Management (Intel® vPro™)
- Reversão das alterações mal-intencionadas feitas ao sistema
- Tecnologia de autodefesa contra programas mal-intencionados para a solução antivírus
- Suporte total para plataformas de 64 bits
- Atualização automática dos bancos de dados

5.2 GERÊNCIAS DE FALHAS

A gerência de falhas tem a responsabilidade de monitorar os estados dos recursos, da manutenção de cada um dos objetos gerenciados, e pelas decisões que devem ser tomadas para restabelecer as unidades do sistema que venham a dar problemas.

Opcionalmente, pode-se aqui gerar um registro das ocorrências na rede, um diagnóstico das falhas ocorridas, e uma relação dos resultados deste diagnóstico com as ações posteriores a serem tomadas para o reparo dos objetos que geraram as falhas.

O 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. Pode-se conseguir este ideal através da monitoração das taxas de erro do sistema, e da evolução do nível de severidade gerado pelos alarmes (função de

relatório de alarme), que permite emitirmos as notificações de alarme ao gerente, que pode definir as ações necessárias para corrigir o problema e evitar as situações mais críticas.

Benefícios Estratégicos

- Minimizar o tempo de downtime da rede.
- Proporcionar apoio na identificação das origens dos problemas.
- Mostrar um retrato da disponibilidade dos dispositivos da rede.

Benefícios Operacionais

- Identificar o “estado de saúde” dos elementos.
- Atuar pro ativamente no isolamento de problemas.
- Facilitar a visualização e o acompanhamento da resolução do problema.
- Oferecer dados para auxiliar nos procedimentos de análise de problemas.
- Manter um histórico do comportamento

5.2.1 SOFTWARE DE GERENCIA DE FALHAS

5.2.1.1 Spectrum's Alarm

O software CA SPECTRUM® Network Fault Manager oferece serviço automatizado, gerenciamento de falhas e de configuração por redes de multitecnologia diversas para garantir a disponibilidade de serviços de rede críticos essenciais aos aplicativos dos

seus negócios. A tecnologia patenteada de análise de impacto e causa básica aponta imediatamente o componente de rede com falhas ou danificado, indica quem e o que foi afetado e oferece uma correção. Os recursos de criação de relatórios fornecem informações acionáveis imediatas com relação a ativos de TI, disponibilidade, eventos e alarmes e métricas de desempenho.

6 CONCLUSÃO

O gerenciamento de uma rede é algo muito complexo, onde deveremos estar atentos e prevenidos a todo e qualquer tipo de ocorrência que ocorra, para implementar maior segurança e evitar tais falhas.

7 REFERÊNCIAS

<http://technet.microsoft.com/pt-br/library/cc668412.aspx>

<http://www.esy.com.br/kasperskyr-total-space-security.htm>

<http://www.shammas.eng.br/acad/sitesalunos0106/012006gr/seguranca.htm>

<http://www.shammas.eng.br/acad/sitesalunos0106/012006gr/falhas.htm>

http://www.ca.com/files/productbriefs/ca_spectrum_nfm_pfb_por_223567.pdf