Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Elizeu Pereira Loureiro Filho

Localização de usuários em rede:

Um método para descobrir e identificar a localização física de usuários e/ou computadores conectados em uma rede local.

Rio de Janeiro

2006

Elizeu Pereira Loureiro Filho

Localização de usuários em rede: Um método para descobrir e identificar a localização física de usuários e/ou computadores conectados em uma rede local.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:
Prof. Carlos Eduardo Mendes de Azevedo, UFRJ, Brasil.

Rio de Janeiro

2006

Elizeu Pereira Loureiro Filho

Localização de usuários em rede: Um método para descobrir e identificar a localização física de usuários e/ou computadores conectados em uma rede local.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Fevereiro de 2006:

Carlos Eduardo Mendes Azevedo

Prof. Carlos Eduardo Mendes de Azevedo, UFRJ, Brasil.

AGRADECIMENTOS

Agradeço a minha mãe pelo apoio em todos os momentos da minha vida, aos colegas de turma, a todos os professores do MOT pela ajuda e dedicação, e uma dedicatória especial a minha ex-esposa Luciana Mota pelo incentivo e pela paciência durante todo o período de estudos.

RESUMO

LOUREIRO Fº, Elizeu Pereira. **Localização de usuários em rede: Um método para descobrir e identificar a localização física de usuários e/ou computadores conectados em uma rede local.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

O presente trabalho pretende descrever os passos necessários para se tentar identificar a localização física de usuários e computadores conectados em uma rede local.

O nosso estudo se restringirá à rede de tecnologia *Ethernet*, com equipamentos ativos de rede *Switchs* CISCO, protocolo de rede e endereçamento lógico TCP/IP e servidor de rede Novell Netware 6.0. Será usado também o protocolo SNMP para coleta de informações dos equipamentos ativos de rede.

A estrutura física da rede local em questão possui o cabeamento estruturado, com planta baixa dividida em quadrantes, com os pontos de rede assinalados.

ABSTRACT

LOUREIRO Fº, Elizeu Pereira. **Localização de usuários em rede: Um método para descobrir e identificar a localização física de usuários e/ou computadores conectados em uma rede local.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

This work tries to describe the necessary steps to identify the physical location of users and computers on the LAN.

This study is restricting about Ethernet technology, CISCO equipments, logical net protocol TCP/IP and Novell Netware 6.0 server. We also use SNMP protocol to discover and require information from LAN equipments.

The physical LAN in this work is structured cabling, with dividable maps, with assigns points.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANSI	American Nacional Standards Institute
ARP	Address Resolution Protocol
EIA	Eletronic Industries Alliance
DOS	Disk Operation System
IDS	Intrusion Detection System
LAN	Local Área Network
MAC	Media Access Control
MIB	Management Information Base
NDS	Novell Directory Services
OID	Object Identifiers
TIA	Telecommunications Industry Association
TC	Telecommunication Closet
TCP/IP	Transport!Control Protocol and Internet Protocol
SNMP	Simple Network Management Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Área

SUMÁRIO

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

A segurança das redes de computadores é fundamental para a garantia das informações que nela transitam, e garantir a confidencialidade, integridade e disponibilidade é a principal tarefa do administrador de redes.

Para garantir essa segurança são necessários vários mecanismos, procedimentos, que vão desde a verificação física, no controle do acesso físico, até a monitoração lógica da rede e seus acessos.

A proteção da rede a determinados tipos de ameaças se faz de forma reativa, dependente do monitoramento constante, manual ou automático.

O escopo deste trabalho restringe-se à investigação através do monitoramento de *logs* de acesso e *Firewall*, para determinar a localização física na rede da ameaça .

1.2 DESCRIÇÃO DO PROBLEMA E OBJETIVOS

O advento da Internet e a disseminação dos conhecimentos de uso de ferramentas de ataque, do modismo de se tornar um “*hacker*”, e da fascinação pelo uso de redes, seja para fins educativos ou de entretenimento, trazem um desafio para os administradores de rede. Sem falar nas atividades realmente criminosas que tentam de várias formas obter vantagens, sejam ela financeira ou não.

O principal objetivo deste trabalho é fornecer um conjunto de técnicas, procedimentos e “dicas”, referente ao ambiente interno da rede, para facilitar a detecção e a eliminação de possíveis ameaças.

Esta monografia visa responder à seguinte pergunta:

Quais os métodos para se tentar identificar os usuários conectados em uma rede Novell com infra-estrutura CISCO e estabelecer a sua localização física?

1.3 Metodologia

O projeto será dividido em três partes:

A primeira parte, teórica, consiste na apresentação dos conceitos e tópicos relacionados aos conhecimentos necessários para a correta compreensão das ferramentas, técnicas e “dicas” descritas mais a seguir.

A segunda parte, prática, diz respeito à realização de uma investigação, enfatizando a localização física da ameaça.

Com o objetivo de agregar valor prático e validar o projeto proposto, este trabalho utilizará uma rede semelhante à utilizada em meu ambiente de trabalho.

Na terceira parte será apresentada uma conclusão das soluções propostas e dos resultados obtidos.

1.4 Organização da Monografia

Esta monografia foi dividida em cinco capítulos e mais apêndices, sendo estes últimos indispensáveis à compreensão deste trabalho.

O presente capítulo faz uma pequena introdução ao tema proposto e relata os objetivos do trabalho.

O capítulo 2 contém os conceitos relacionados ao trabalho, onde serão apresentadas informações sobre o referencial teórico necessário ao estudo deste trabalho.

O capítulo 3 trata da descrição das ferramentas utilizadas, características, técnicas, procedimentos necessários e extração das informações, referente às fontes apresentadas no capítulo anterior.

No capítulo 4 é apresentado o resultado prático do uso das ferramentas descritas no capítulo 3, mostrando de forma objetiva e detalhada passo a passo, seqüências de procedimentos utilizados para se tentar identificar a origem da ameaça.

O capítulo 5 tem como objetivo apresentar a conclusão do projeto.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 CONSIDERAÇÕES INICIAIS

Neste capitulo serão apresentados os conceitos necessários para o entendimento da proposta deste trabalho.

2.2 MONITORAMENTO DA REDE

A monitoração da rede é muito importante: deve-se realizar o levantamento dos *logs*, guarda, confecção de relatórios, extração de dados desse *logs*.

2.3 TECNOLOGIAS ENVOLVIDAS

Uma rede local de computadores é composta de “Computadores autônomos interconectados por uma única tecnologia” – (TANENBAUM, 2003, p.2). Estes computadores podem compartilhar dados e trocar informações. Basicamente uma rede local serve como ferramenta de produtividade. Entretanto vários são os requisitos para que esta rede opere de forma segura e confiável. E, ainda que todos os requisitos atendidos, é necessário promover uma monitoração constante pois “Pessoas que penetram em sistemas de computadores simplesmente para ‘olhar’ causam um dano real, mesmo que não acessem informações confidenciais ou removam arquivos”- (GARFINKEL, SPAFFORD e SCHWARTZ, 2003, p.3).

2.3.1 A Tabela ARP

Para que exista a comunicação entre os computadores de uma rede local é necessário que haja um mapeamento dos endereços físicos com os endereços lógicos.

Este mapeamento entre o endereço do protocolo de alto nível (IP) e o de baixo nível (MAC) é efetuado pelo protocolo ARP (Address Resolution Protocol).

"O ARP, descobre o endereço de hardware associado a um endereço IP em particular. Isso pode ser utilizado em qualquer tipo de rede que suporte *Broadcasting*. Contudo, é mais comumente descrito em termos de *Ethernet*" (NEMETH, GARTH, SCOTT e TRENT, 2001, p.327).

Para que haja comunicação entre os equipamentos da rede física citada e o roteador, e desse roteador para uma outra rede física, é necessário o mapeamento entre o endereço lógico e o endereço físico relacionados aos equipamentos envolvidos. Em cada um desses equipamentos o protocolo ARP preenche uma tabela com estes endereços e suas correlações. Esta tabela é conhecida como tabela ARP.

Tomemos como exemplo a figura 1 abaixo, onde a estação "A", com endereço IP 1.2.3.4, quer se comunicar com a estação "C", cujo IP é 2.3.4.5, a comunicação obrigatoriamente deve ser através do roteador "R", cujo endereço IP é 1.2.3.5 na interface eth0 e 2.3.4.6 na interface eth1, é necessário que seja conhecido o endereço físico da rede para o endereçamento do quadro *Ethernet*.

A estação "A" primeiramente envia, através do protocolo ARP, uma requisição para descobrir o endereço físico do roteador "R" que dá acesso à rede onde se encontra a estação "C". Em seguida a estação "A" transmite o pacote destinado à estação "C" através do quadro Ethernet direcionado para o roteador "R". O roteador

“R” por sua vez recebe o quadro Ethernet e verifica o endereço lógico do pacote IP encapsulado. O pacote IP tem como destino a estação “C”, como o roteador “R” recebeu este pacote ele tem de repassar para a estação “C”, então ele antes requisita através do protocolo ARP o endereço físico da estação “C”, após a descoberta ele encapsula o pacote IP dentro do quadro Ethernet e o encaminha para a estação “C”.

A tabela ARP no roteador “R” ficaria assim.

Quadro 1 – Exemplo de Tabela ARP

Equipamento	Endereço Lógico	Endereço físico
Estação A	1.2.3.4	00.aa.bb.cc.dd.ff
Estação C	2.3.4.5	00.bb.cc.dd.ff.gg

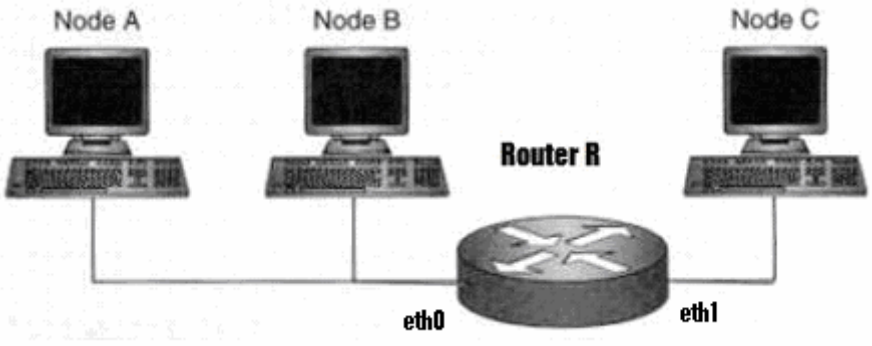

Figura 1 – Exemplo de rede local

Este mapeamento de endereços, a tabela ARP, é essencial para o nosso estudo.

2.3.2 A Tabela MAC nos *Switchs*

O equipamento *Switch* permite a ligação das estações simulando um barramento Ethernet. A ligação da estação ao *Switch* se dá por cabos par trançado de 8 fios, ou 4 pares. Em cada porta de *Switch* da rede citada está apenas uma estação, de modo que a comunicação entre estações, e entre as estações e o roteador seja comutada. A comutação significa que a comunicação é direta, isto é, unicast será somente entre as estações fim e destino, não havendo tráfego para outras estações da rede como numa rede *Ethernet* típica(TANENBAUM, 2003, p.300).

O *Switch* sabe qual ou quais estações estão conectadas em cada porta, e mantém esta informação em uma tabela interna de Porta/*MAC Address*.

Esta é outra tabela importante em nosso estudo.

2.3.3 Documentação da rede

Na rede citada é utilizado cabeamento estruturado padrão ANSI/EIA/TIA 568A. Este padrão define a estrutura de cabeamento para redes de computadores em prédios comerciais(DERFLER, FREED, 1996, p.111) .

A estrutura básica é a utilização de *Patch Panel*, um painel de metal onde se conectam os cabos de par trançado. Sendo que parte desses painéis terá a ponta dos cabos ligada às estações, e a outra parte terá painéis ligados às portas dos *Switchs*, de modo que a ligação da porta de *Switch* a estação seja efetuado por um cabo de manobra ligando um *patch panel* a outro.

A localização desses painéis será na sala de telecomunicações (TELECOMMUNICATIONS CLOSET - TC), ou em armários próprios.

Na rede citada todos os *patch panel*s são numerados. Todos os pontos têm numeração e os painéis têm identificação do ponto ou da porta de *Switch* a que se referem.

Existe uma documentação dessas ligações para que a consulta seja feita sem que haja necessidade de locomoção até os TCs.

Existe também uma planta baixa dos andares onde se encontra a rede estruturada. Esta planta baixa está dividida em quadrantes, coordenadas, onde os pontos são de fácil localização, a numeração dos pontos faz referência à localização dos quadrantes do mapa.

A tabela é apresentada da seguinte forma:

Quadro 2 – Exemplo de quadro de pontos de rede

Ponto de rede	Localização	Quadrante
TC1-04A	Setor de Laboratório	A3 – planta 01
TC1-07B	Setor Técnico	D1 – planta 01
TC2-10ª	Setor Administrativo	C9 – planta 02

Ponto de rede: TCX-99A ou TCX-99B – onde X é o armário de localização do ponto.

A para o edifício/prédio 1 e B para o edifício/prédio 2.

Localização : Nome do setor

Quadrante : Coordenadas na planta baixa.

2.3.4 NDS – Novell Directory Service

O servidor de rede possui o serviço de diretório com uma estrutura hierárquica de dados chamada de NDS (Novell Directory Service), atualmente este produto é conhecido como *eDirectory*. O NDS pose ser implementado em servidores Windows (NT, Win2000, Win2003) e Unix (Linux – Red Hat e Suse, Solaris, HP-UX, AIX e outros). A NSD é organizada de forma semelhante a uma árvore, nela está espelhada toda a estrutura da empresa, representada por objetos. Estes objetos podem ser relacionados de forma organizada, de acordo com o organograma da empresa, em diretorias, gerências, grupos de trabalho, usuários, etc...

“Para simplificar, o Diretório do NDS* é uma lista de objetos que representam recursos da rede, tais como usuários da rede, servidores, impressoras, filas de impressão e aplicativos.” Retirado do *Help* do aplicativo Administrador da NDS.

Cada objeto tem seus atributos individuais, o que importa para este estudo é o endereço da estação onde o usuário está conectado, tanto o endereço MAC quanto o endereço IP da estação ficam armazenados como atributos do usuário enquanto ele estiver conectado à rede Novell.

Para o usuário se conectar na rede é necessária uma autenticação nessa árvore NDS.

O diretório é uma base de dados especializada com o propósito de prover o acesso rápido aos dados de uma maneira padronizada. Exemplos de diretórios *off-line* (impressos): guia telefônico, guia de TV, etc.

O serviço de diretório provê, por meios de ferramentas, o acesso ao diretório através de uma rede de computadores.

O serviço de diretório provê um lugar para guardar informações sobre entidades da rede como aplicações, arquivos, impressoras e pessoas. Ele provê um meio consistente de nomear, descrever, localizar, acessar, gerenciar e proteger informações sobres esses recursos individuais.

A escolha da tecnologia NDS da Novell deve-se ao seu pioneirismo e estabilidade, bem como exemplo para os atuais produtos como o AD da Microsoft e do Open LDAP. Pode haver um paralelo e adaptação do presente trabalho para qualquer dessas plataformas, entretanto foge ao escopo do presente trabalho esta comparação ou adaptação.

2.3.5 SNMP

O SNMP (Simple Network Management Protocol) é o protocolo de gerência recomendado para o gerenciamento de redes TCP/IP. O SNMP é um protocolo de gerência definido a nível de aplicação, utilizando os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar suas mensagens através da rede. Sua especificação está contida no RFC 1157 (NEMETH, SNYDER, SEEBASS, HEIN, 2001, p.681). Este protocolo é o centro do desenvolvimento do gerenciamento SNMP. Através do SNMP é possível consultar a tabela ARP de um roteador descobrindo qual endereço MAC está relacionado a qual endereço IP, pode-se descobrir em que porta de *Switch* esta conectada a máquina que possui determinado endereço MAC, a partir daí localizar fisicamente onde esta determinado endereço IP.

2.3.5.1 MIB e OID

Antes de definir o que é uma MIB, introduziremos o conceito de objetos gerenciados.

Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso.

Dessa forma, a MIB é o conjunto dos objetos gerenciados, uma base de dados, que procura abranger todas as informações necessárias para a gerência da rede.

Dentro da MIB cada objeto tem o seu identificador (OID - Object Identifier) para pesquisa (NEMETH, SNYDER, SEEBASS, HEIN, 2001, p.682).

Na MIB serão pesquisadas as informações determinantes para o presente trabalho, nela estão as informações que nos darão a indicação da localização física do endereço IP procurado.

O RFC (Request For Comment) 1066 apresentou a primeira versão da MIB, a MIB I. Este padrão explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas na pilha de protocolos TCP/IP. A evolução aconteceu com o RFC 1213 que propôs uma segunda MIB, a MIB II, para uso baseado na pilha de protocolos TCP/IP.

Basicamente são definidos três tipos de MIBs: MIB II, MIB experimental, MIB privada.

A MIB II, que é considerada uma evolução da MIB I, fornece informações gerais de gerenciamento sobre um determinado equipamento gerenciado. Através das MIB II podemos obter informações como: número de pacotes transmitidos, estado da interface, entre outras (NEMETH, SNYDER, SEEBASS, HEIN, 2001, p.683).

A MIB experimental é aquela em que seus componentes (objetos) estão em fase de desenvolvimento e teste. Em geral, eles fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

MIB privada é aquela em que seus componentes fornecem informações específicas sobre os equipamentos gerenciados, como configuração, colisões e também é possível reinicializar, desabilitar uma ou mais portas de um roteador.

As MIBs Pesquisadas e os respectivos OIDs usados nesta trabalho constam do Anexo 1. Estes itens foram pesquisados no site da CISCO www.cisco.com e referem-se aos equipamentos deste fabricante, podendo haver coincidência ou não com outros equipamentos similares de outros fabricantes.

Além do padrão MIB que especifica variáveis de gerenciamento de rede e seus significados, um outro padrão especifica um conjunto de regras usadas para definir e identificar as variáveis da MIB. As regras são conhecidas como a especificação da SMI (Structure of Managment Information). Para manter os protocolos de gerenciamento da rede simples, a SMI faz restrições quanto ao tipo de variáveis permitidas na MIB, especifica as regras para atribuir nome a essas variáveis e cria regra para definir tipos de variáveis (COMER, 1998, p. 503).

2.3.5.2 Operações Suportadas pelo SNMP

Get: uma estação de gerenciamento recupera um valor do objeto escalar de um agente.

Set: uma estação de gerenciamento atualiza um valor do objeto escalar de um agente.

Trap: um agente envia um objeto escalar não solicitado para uma estação de gerenciamento da rede.

Não é possível mudar a estrutura de uma MIB adicionando ou removendo instâncias de objetos. Nem é possível emitir comandos de uma ação para serem efetuados. Além disso, o acesso é provido somente para objetos folhas da árvore identificadora de objetos. Entretanto, por convenção, é possível executar operações em tabelas bi-dimensional simples. Estas restrições simplificam grandemente a implementação do SNMP, mas, por outro lado, impõem limites na capacidade do sistema de gerenciamento da rede (NEMETH, SNYDER, SEEBASS, HEIN, 2001, p.683).

2.4 Considerações Finais

A conceituação técnica fornecida neste capítulo é fundamental para a compreensão do trabalho apresentado. Devido ao crescimento da Internet e em conseqüência dos ataques a computadores, fica claro a necessidade de desenvolvimento de técnicas de abordagem de detecção das ameaças, em nosso trabalho restritas as ameaças internas.

Neste capítulo foram apresentados os conceitos técnicos que serão de grande utilidade no decorrer deste trabalho.

3. METODOLOGIA DE PESQUISA E FERRAMENTAS

3.1 Considerações iniciais

Neste capítulo mostraremos como usá-las, extrair as informações e os passos necessários, em uma ordem lógica, de utilização, para chegarmos à localização física do usuário/máquina na rede.

3.2 A pesquisa na rede

A localização de uma máquina na rede pode ser feita de vários modos, desde a ida máquina a máquina, em uma pequena rede é claro, um catalogo de endereços de cada máquina, sua localização e endereço físico e lógico, ou através de pesquisas nos equipamentos ativos de rede.

A metodologia usada será a de um estudo de caso, com caráter de detalhamento e aprofundamento, baseando-se em poucas unidades de investigação, não permitindo a generalização dos resultados.(ALVES, 2003)

Em nossa metodologia, a partir de uma suspeita de um ataque à nossa rede, ataque este limitado às estações internas, faremos diversas pesquisas, no servidor da rede, nos *switchs*, na documentação da rede, nas plantas, de forma a localizar de forma precisa e tempestiva a localização física do referido ataque.

Inicialmente se faz necessário um monitoramento da rede, que pode ser efetuado pessoalmente ou através de ferramentas que avisem na presença de determinados eventos. Na presença de um evento significativo, este sempre constando o endereço IP de origem, efetuamos as pesquisas.

Faremos inicialmente uma pesquisa na árvore da NDS, através do comando NLIST, de forma a detectar se existe um usuário conectado usando o endereço IP procurado.

Havendo resultado positivo ou negativo, passamos a pesquisa nos *Switchs* da rede através dos comandos SNMP, iniciando pelo *Switch* central, onde se encontra o roteador da rede. No roteador podemos identificar qual o endereço físico (*MAC address*) associado ao endereço IP procurado.

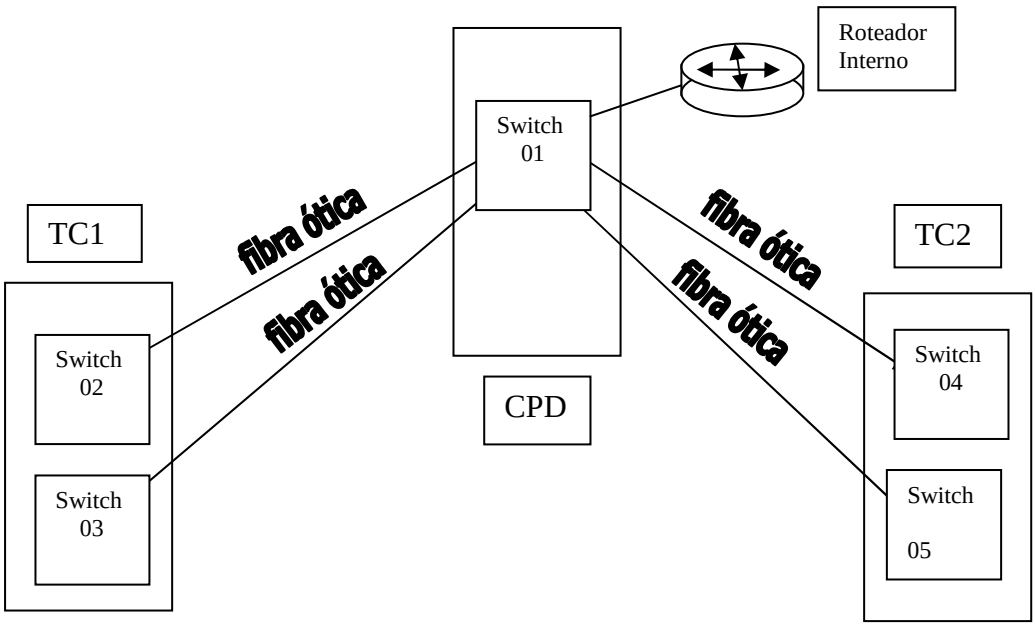

Figura 2 – Ligação entre os switchs

Pela faixa de endereçamento IP determinamos a qual *Vlan* o endereço pertence.

De posse do endereço MAC, da *Vlan* e do endereço IP, pesquisamos no *Switch* de borda, onde estão conectadas as estações.

Obs.: Lembramos que na rede descrita cada estação está ligada a uma porta de *Switch*.

Novamente através dos comandos SNMP podemos recuperar as informações da MIB do equipamento pesquisado de forma a localizar a porta física onde está conectado o endereço IP procurado.

A partir deste momento faremos uso da documentação da rede, do cabeamento estruturado, das plantas, para localizar geograficamente o ponto de rede onde se encontra o equipamento com o endereço IP procurado.

Mostramos abaixo um diagrama do método de pesquisa proposto.

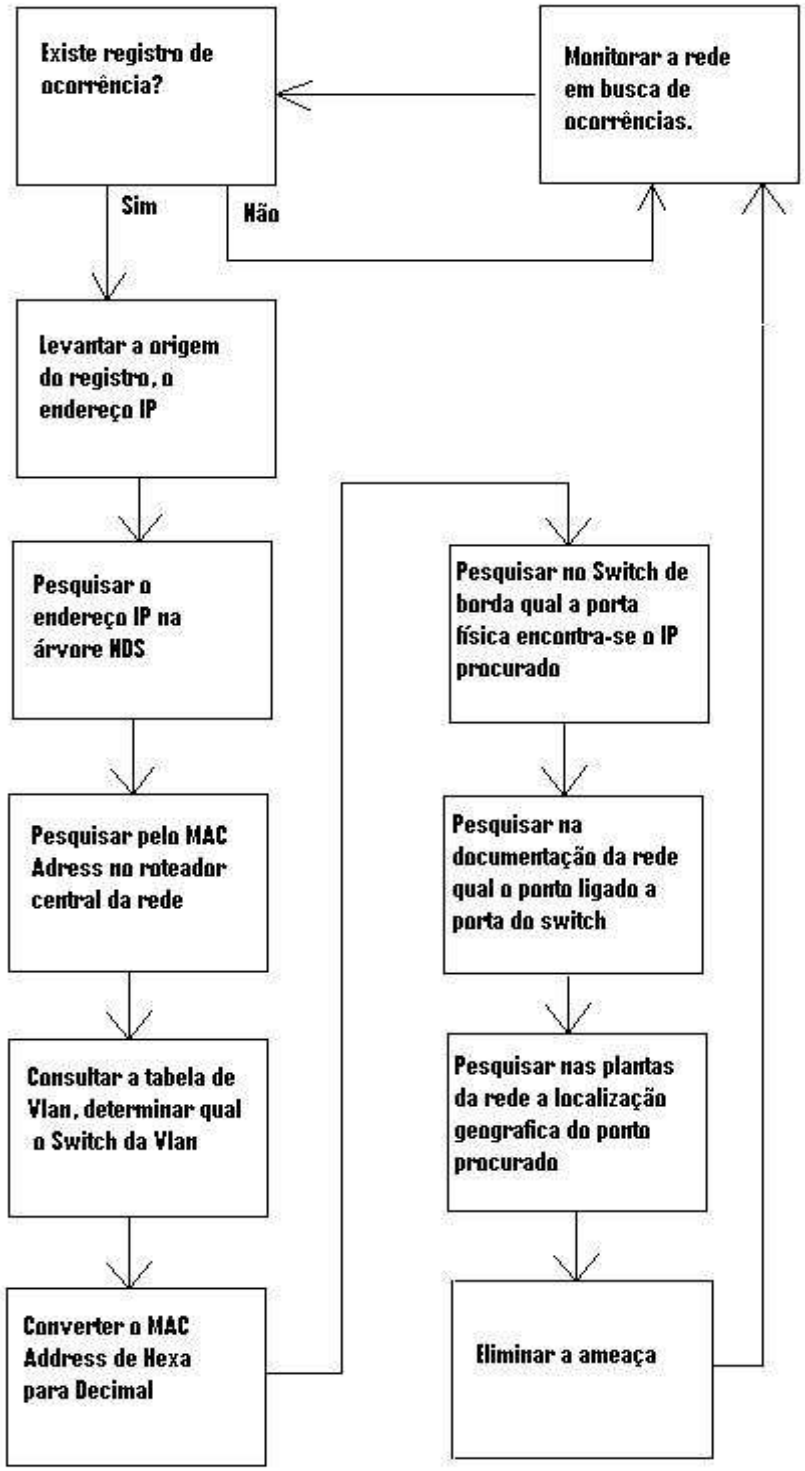

Figura 3 - Fluxograma da pesquisa na rede

3.3 Descrição do ambiente

A rede para demonstração da metodologia foi dividida em 6 *Vlan*s, sendo 1 *Vlan* por *Switch*. Temos um *Switch* Central, este *Switch* possui capacidade de roteamento TCP/IP, isto é, um *switch* nível 3, nele estão ligados os outros *Switchs* através de conexões por fibra ótica.

Os outros *Switchs* de borda, onde estão ligadas as estações, são em número de quatro.

Os endereços finais de cada *Vlan* são os endereços de *Gateway* de cada rede, e estes endereços são do módulo de roteamento do *Switch* Central, isto é, em cada rede o último endereço IP será o do roteador localizado no *Switch* central.

O gerenciamento dos *Switch* é efetuado através da *Vlan* 100 administrativa.

As estações conectadas nesta rede são Windows 9x e Windows XP, utilizam apenas o protocolo TCP/IP e cliente para Novell versão 4.90 SP2.

O Servidor da rede é Netware Novell 6.5 SP3.

Os *Switchs* estavam configurados com a comunidade de leitura igual a *public*.

O *Switch* central possui um módulo IDS (Intrusion Detection System) que registra atividades suspeitas repassando as ocorrências para um servidor Windows 2000.

Registramos abaixo a distribuição das *Vlan*s no ambiente:

Quadro 3 – Exemplo de quadro de distribuição de *Vlan*s

Vlan	Faixa de endereços IP	Nr. da *Vlan*	Gerência
Adm	10.0.1.0 a 10.0.1.253	100	Administrativa
Tec	10.0.2.0 a 10.0.2.253	110	Técnica
Lab	10.0.3.0 a 10.0.3.253	120	Laboratório

Obs.: O último endereço de cada rede (final 254) é o do módulo de roteamento do *Switch* central.

Quadro 4 – Exemplo de Quadro de Endereços de Gerenciamento de *Switch* que pertencem à *vlan* 100.

Switch 1	10.0.1.253
Switch 2	10.0.1.252
Switch 3	10.0.1.251
Switch 4	10.0.1.250

3.4 Política de cadastramento de máquinas

Para que a pesquisa na NDS seja mais elucidativa, mas descritiva, mais rica em detalhes, faz-se necessário à configuração no Windows do nome da máquina, colocando-se o setor, mais o número bem ou o número de série do equipamento, visto que a NDS captura este nome quando a máquina é conectada à rede. Desta forma, durante as pesquisas na NDS, pode-se localizar o equipamento, mesmo este estando desligado.

Ex.: Tec2313 (onde Tec é o setor técnico e o nr 2313 é o final do número de série).

3.5 Política de cadastramento de usuários

Outra boa política é cadastrar o ID de rede dos usuários de forma a identificá-lo e o seu respectivo setor, desta forma fica mais fácil de localizá-lo quando estiver conectado na rede.

Ex.: Jorge-tec (usuário Jorge, do setor técnico).

3.6 Mapeamento dos pontos – Ligações nos TCs

O correlacionamento dos pontos de rede, onde estão conectados as estações nos TCs, e os pontos nos TCs ligados aos switchs devem estar registrados em planilhas (MS-Excel), em banco de dados, ou mesmo em papel. Este mapeamento será usado nas pesquisas da localização física do equipamento, uma vez que as pesquisas nos Switchs indicam a porta física do Switch, sendo necessário localizar, através deste mapeamento, o equipamento.

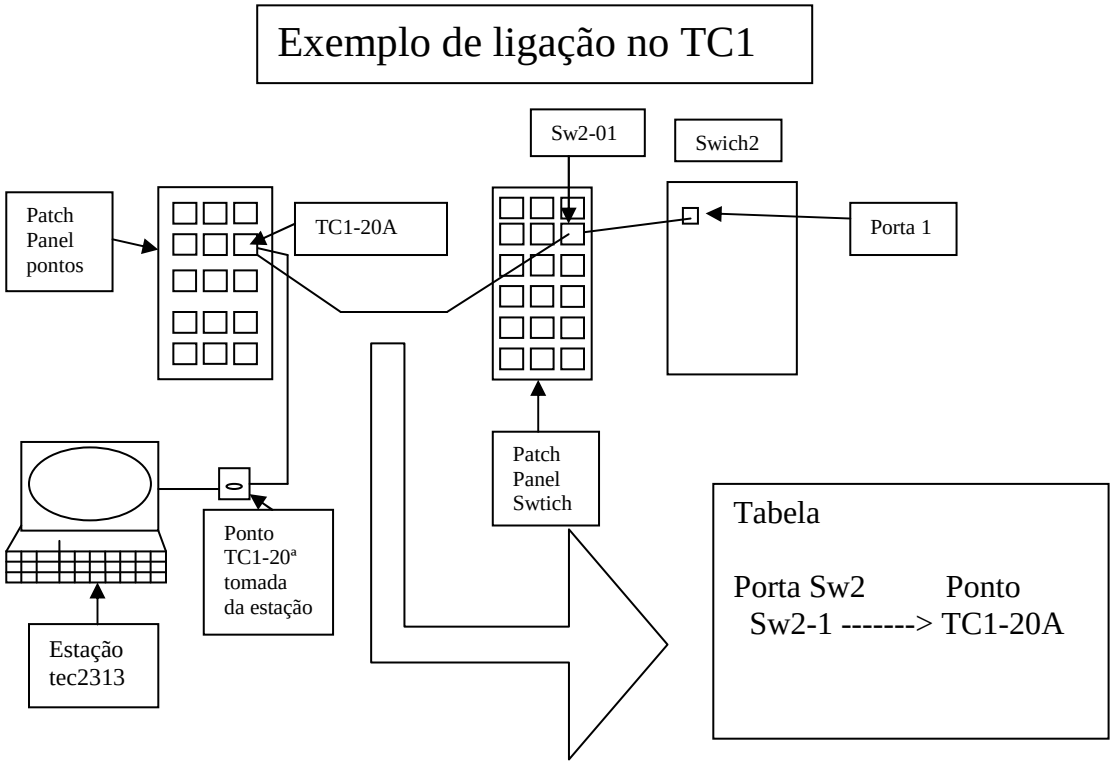

Figura 4 - Diagrama da ligação do ponto de rede, patch panel no TC e porta Switch.

3.7 FERRAMENTAS - Considerações Iniciais

Para a extração das informações da NDS e dos equipamentos ativos de rede, no processo de localização dos usuários conectados na rede, serão necessários os conhecimentos das ferramentas e técnicas para este levantamento. Neste capítulo serão apresentados estas ferramentas e métodos.

3.7.1 DOS

Usamos um equipamento com sistema operacional Windows XP conectado à rede Novell que foi pesquisada, executamos comandos e scripts DOS (Disk Operation System). A utilização de comandos DOS é mais simples e possibilita acesso a partir de qualquer tipo de estação Windows.

A utilização do DOS simplifica o uso dos comandos propostos, bem como facilita a sua automatização e a compreensão dos exemplos apresentados.

A abertura de uma janela DOS pode ser efetuada através do menu Iniciar do Windows XP, conforme mostrado na figura abaixo. Para termos acesso a comandos da rede e usamos os scripts deste trabalho, devemos primeiramente estar autenticados e conectados ao servidor da rede, e em seguida nos posicionar em uma unidade da rede para que estes funcionem adequadamente, digitando a letra da unidade de rede onde está localizado o volume SYS da árvore Novell. Normalmente este drive é mapeado como F: .

3.7.2 NLIST

Usamos a ferramenta NLIST da Novell. Trata-se de um comando bastante poderoso para listar objetos da NDS e seus atributos, esta ferramenta só funciona em ambiente DOS. É necessário também estar conectado e autenticado ao Servidor da rede, em nosso caso ao Servidor Novell Netware.

Existe também a necessidade do ambiente estar configurado com o caminho de procura onde se encontram os programas Novell, geralmente no volume SYS, o comando de inclusão do caminho de procura usado foi:

MAP INS S1:=”Nome do Servidor”/SYS:\PUBLIC

Mostramos abaixo as opções desta ferramenta:

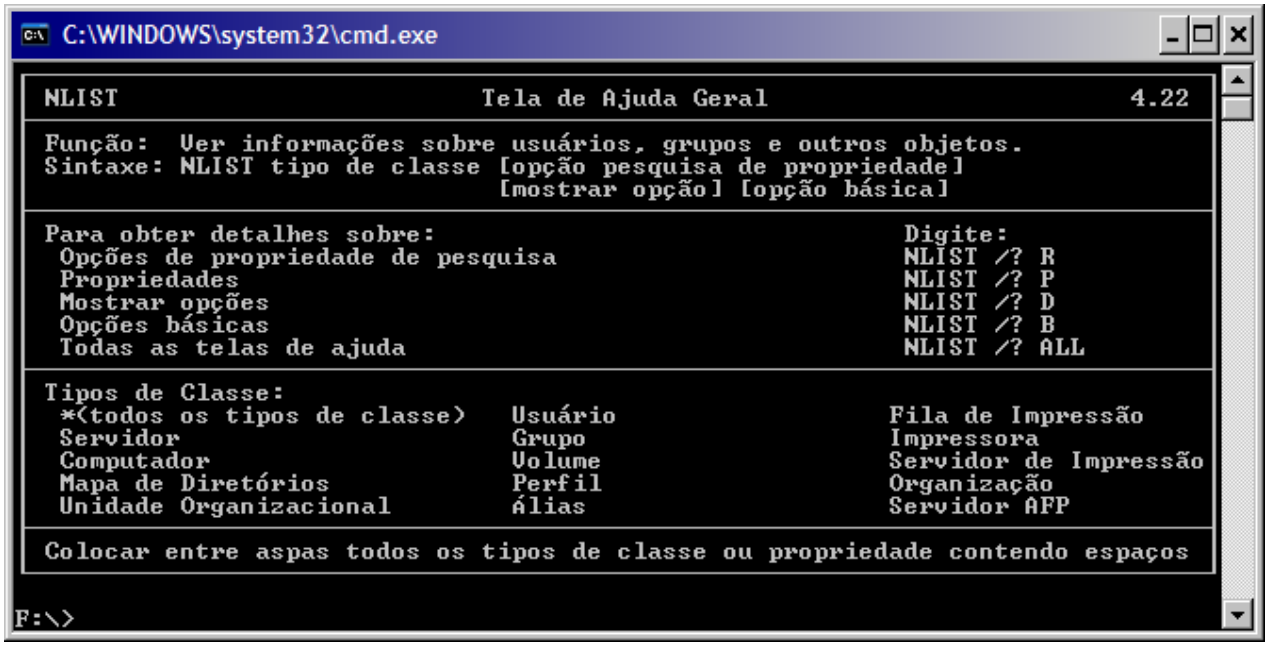

figura 4 – Comandos do Nlist

3.7.3 Programas SNMPGET e SNMPWALK

Os dois programas foram baixados do site

http://www.bradfordnetworks.com/support/utilities.html .

Estes programas fazem parte de um pacote chamado “SNMPwalk for Windows System”, onde se encontram compactados os programas, alem de um arquivo .dll (biblioteca para os sistemas operacionais MS Windows/DOS).

Com estes programas faremos pesquisas, via protocolo SNMP, na MIB dos equipamentos da rede, com o objetivo de recuperarmos as informações necessárias para a indicação da localização do endereço IP procurado.

3.7.4 Programa HEX2DEC

Este programa é necessário para a conversão do MAC Address de Hexa para decimal. Pois as consultas SNMP utilizam somente a notação decimal. Pode-se ainda usar a calculadora do Windows para a tarefa, mas o programa HEX2DEC é mais prático e pode ser baixado do seguinte site:

http://ftp.elf.stuba.sk/pub/pc/utilprog/hex2dec.zip

Mais adiante faremos uma demonstração do uso deste programa, que poderá inclusive fazer parte de uma rotina maior, automatizando assim o processo de descoberta da localização física de um determinado endereço IP.

3.7.5 SCRIPTS DOS

Usaremos dois scripts (arquivos de lote) DOS para facilitar a pesquisa. Estes dois scripts facilitam o processo de pesquisa, uma vez que automatizam parte do

processo de pesquisa na NDS e nos equipamentos ativos de rede. Estes scripts fazem parte do projeto seguinte, o projeto de construção de uma ferramenta única para todo o levantamento de localização física de usuários em rede.

O script primeiro faz pesquisa na NDS para saber qual o usuário esta usando determinado endereço IP.

Conteúdo do arquivo ListaIP.bat

Modo de execução: ListaIP "endereço IP"

```
@echo off        ( desliga o echo dos comandos )
if {%1} == { } @echo Sintaxe ListaIP 99.99.99.99 &goto :EOF
cls
echo .
echo Aguarde, consultando a NDS ....
nlist user /a /b /co . > resultado  ( lista todos os usuários a partir da raiz da NDS e direciona para o arquivo de nome resultado)
echo .
cls
echo .
echo
################################################################################
echo .
echo Con   Nome/ID do usuario          Endereco IP      No       Data/Hora Lo
gin
find /i "%1" resultado  ( procura no arquivo resultado o endereço IP digitado como parâmetro %1)
echo .
echo
################################################################################
echo .
echo Processo terminado.
del resultado ( remove o arquivo temporário )
```

O outro script será usado para conversão do endereço MAC de Hexa para decimal.

Conteúdo do arquivo converte.bat

```
@echo off
if {%1} == { } @echo Sintaxe Convert xx xx xx xx xx xx &goto :EOF
hex2dec.exe %1
hex2dec.exe %2
hex2dec.exe %3
hex2dec.exe %4
hex2dec.exe %5
hex2dec.exe %6
```

3.7.6 DOCUMENTAÇÃO DA REDE

Para elaborarmos a documentação da rede é necessário que todo o mapeamento entre os pontos de rede e as respectivas portas de *switch*, seja efetuado, de forma que quando chegarmos à identificação da porta de *switch*, onde se encontra o endereço IP procurado, possamos identificar qual é o respectivo ponto da rede.

Podemos elaborar tal documentação podemos usar planilhas eletrônicas, bancos de dados, etc.. Em nosso caso específico foram elaboradas duas planilhas eletrônicas Excel:

A - Uma constando da ligação entre os *patch panel*s, para verificação dos pontos;

B – A segunda da porta do *switch* e o ponto de rede.

Toda a documentação passa a não ter sentido caso não haja uma planta baixa do local, onde devem estar assinalados os pontos de rede. Tal planta baixa deve estar dividida em quadrantes, coordenadas, para facilitar a visualização e localização, os pontos também devem seguir uma padronização de nomenclatura para facilitar também a sua localização na planta.

Normalmente numa instalação de cabeamento estruturado por empresas competentes tal documentação é fornecida. O que não impede que, na sua falta, tal documentação seja elaborada pela equipe responsável pela rede.

4. ANALISE DE RESULTADOS

4.1 Pesquisa na NDS

Como a NDS é uma base de dados, efetuamos pesquisa na busca de um determinado endereço IP, para tentarmos localizar o usuário deste endereço. A pesquisa na NDS pode mostrar qualquer objeto, e seus atributos, mas nos concentraremos no endereço IP das conexões ativas, lembrando que esta informação só existe enquanto o usuário estiver conectado. Portando a procura por um endereço IP na NDS só mostrará alguma informação então enquanto o usuário estiver conectado. Para melhorar usaremos o script DOS ListaIP.bat descrito no capitulo 3.

A pesquisa na NDS foi efetuada, consultamos o endereço IP 10.0.2.6 e tivemos o seguinte resultado:

C:\>m:
F:\>ListaIP 10.0.2.6 (execução do comando passando como parâmetro o IP 10.0.2.6)
F:\>
##
###
.
Con Nome/ID do usuario Endereco IP No Data/Hora Login
-------- RESULTADO
2466 Fulano-tec [10.0.2.6][0] 08/26/05 09:40 am

##
###
Processo finalizado.
F:\>

Como podemos observar, o resultado da pesquisa trouxe um usuário Fulano que naquele instante da pesquisa estava usando o endereço IP 10.0.2.6. Neste

momento, através do telefone, podemos contatá-lo para perguntar que tipo de atividade ele esta fazendo na rede.

O *login* igual a Fulano-tec é um exemplo de como podemos cadastrar os usuários e identificá-los mais facilmente (nome do usuário ou chave de acesso + setor).

As outras informações mostradas são:

- Na primeira coluna o número da conexão de rede;

- Na segunda coluna o nome de *Login* do usuário;

- Na terceira coluna o endereço IP daquela conexão;

- Na quarta coluna o nó da estação, neste caso aparece como zero pois não há informação deste item;

- E no último campo a data (formato americano) e o horário de *login*.

A pesquisa na NDS foi positiva pois havia um usuário conectado usando o equipamento com IP 10.0.2.6. Apesar da pesquisa, ou mesmo não havendo um resultado satisfatório, resta agora saber a localização física do endereço IP.

4.2 Pesquisa no roteador da rede

O roteador central da rede estão todas as informações de *MAC Address* e endereço IP ativos, pois ele esta ligado a todas as *Vlan*s da rede. É através dele que chegamos ao *switch*/*Vlan* onde está ligado o endereço IP procurado.

A seguir mostramos uma pesquisa no roteador central da rede. Em nosso caso usamos equipamentos CISCO, de forma que a pesquisa foi ser executada seqüencialmente, uma vez que os equipamentos CISCO organizam as tabelas ARP separadas por *Vlan*.

A procura por um endereço IP deve ser através do seu endereço MAC, uma vez que o *Switch* comum só enxerga a camada de enlace. A pesquisa do MAC pelo endereço IP foi efetuada sabendo-se a qual *Vlan* este IP pertence, conforme o quadro 3.

Seguindo o exemplo anterior, a *Vlan* pesquisada foi a Tec, de número 110.

Internamente o *Switch* CISCO possui uma interface lógica associada a cada *Vlan*, então se executou o comando SNMP abaixo para levantamento da interface lógica do roteador da rede, o Switch_01 CISCO 6509:

C:\>snmpwalk 10.0.1.254 public .1.3.6.1.2.1.31.1.1.1.1

Onde:

10.0.1.254 – É o endereço do roteador da rede, no nosso caso o *Switch* 6509;

public – é a *community* para leitura SNMP;

.1.3.6.1.2.1.31.1.1.1.1 – e o OID da tabela onde consta a descrição das Interfaces do *Switch*, seus números e respectivas descrições.

O resultado do comando acima foi:

.iso.3.6.1.2.1.31.1.1.1.1.20 = "VI100"
.iso.3.6.1.2.1.31.1.1.1.1.21 = "Vl110"
.iso.3.6.1.2.1.31.1.1.1.1.22 = "Vl120"
.iso.3.6.1.2.1.31.1.1.1.1.23 = "Vl130"
.iso.3.6.1.2.1.31.1.1.1.1.24 = "Vl140"
.iso.3.6.1.2.1.31.1.1.1.1.30 = "VLAN-110"

Onde:

.iso.3.6.1.2.1.31.1.1.1.1 - é o OID da tabela;

21 – é o número da interface ligada à *Vlan* 110

VI110 – é a descrição da Interface ligada à *Vlan* 110

Obs.: não confundir a interface VI110 com a *VLAN*-110, a primeira é a interface do módulo de roteamento, e a segunda a interface *Vlan* do Switch_1.

Então passamos a seguinte à tabela:

Quadro 5 – Exemplo de Quadro de Interface/*Vlan*/número de *vlan*

Relação de nr interface e *Vlan* - *switch*_01

nome *vlan*	nr.interface	Nr.*vlan*	*Switch*	Range ip
Adm	20	100	01	10.0.1.1 a 10.0.1.253
Tec	21	110	02	10.0.2.1 a 10.0.2.253
Lab	22	120	03	10.0.3.1 a 10.0.3.253
Vago	23	130	04	10.0.4.1 a 10.0.4.253

4.3 Consulta a Tabela ARP do roteador da rede

Após saber-se qual é a interface lógica da *Vlan* Tec, passamos a consulta à tabela ARP existente no *Switch* central, Cisco Catalyst 6509. Procurou-se pelo MAC do IP 10.0.2.6, *Vlan* 110 e cuja interface era 21:

snmpget 10.0.1.254 public .1.3.6.1.2.1.4.22.1.2.21.10.0.2.6

Onde:

10.0.1.254 – endereço do *Switch* 1 da minha rede;

public – community de leitura SNMP

.1.3.6.1.2.1.4.22.1.2 – OID da tabela MAC do *switch*

.21 – OID da *Vlan* 110

.10.0.2.6 – Endereço IP procurado

O resultado da pesquisa anterior foi:

.iso.3.6.1.2.1.4.22.1.2.21.10.0.2.6 = Hex: 00 12 79 64 84 AB

onde o MAC Address associado ao IP 10.0.2.6 era 00-12-79-64-84-AB

4.4 Conversão MAC Address

O *MAC Address* é normalmente expressado em Hexa, no entanto a notação usada nos programas de consulta SNMP é a notação decimal, fazendo-se assim necessária à conversão de Hexa para decimal.

As consultas SNMP utilizam a notação decimal, então se faz necessário à conversão do *MAC Address* encontrado de Hexa para Decimal, novamente desenvolvemos um script DOS para conversão de uma só vez:

No exemplo anterior o MAC Address 00-12-79-64-84-AB convertido ficou assim:

0.18.121.100.132.171

4.5 Pesquisa da *Bridge* associada ao MAC Address

Nas estruturas dos *Switch* cada porta funciona como uma *bridge*, de modo que podem existir mais de um *MAC Address* por porta. No nosso caso temos apenas um *MAC Address* por porta, cada estação esta ligada diretamente a uma porta de *switch*. Desta forma teremos apenas uma correlação Porta/*MAC Address*.

Passamos então a consultar o *Switch* que deve estar conectado a estação procurada, uma vez que a rede estava dividida em *Vlan*s por *Switch*, chegamos ao *Switch* 2. Cada porta dos *Switchs* da rede possuem apenas uma estação conectada, sendo assim, cada porta possui uma única *Bridge* por endereço IP. Com os dados da consulta anterior pesquisamos a *Bridge* associada ao *MAC Address* no *Switch* da *Vlan* Tec, cujo endereço de gerenciamento era 10.0.1.252.

Usamos o resultado da conversão hexa para decimal na consulta. O comando SNMP ficou assim:

*snmpget 10.0.1.252 public@110 .1.3.6.1.2.1.17.4.3.1.2.**0.18.121.100.132.171***

Onde:

10.0.1.252 – endereço IP do *Switch* 2

public – community SNMP de leitura

110 – *Vlan* a ser pesquisada

.1.3.6.1.2.1.17.4.3.1.2 – OID da tabela pesquisada

.0.18.121.100.132.171 – MAC Address

O resultado foi o número da *Bridge* do *Switch* 2 associada ao MAC Address pesquisado.

.iso.3.6.1.2.1.17.4.3.1.2.0.18.121.100.132.171 = ***135***

4.6 Pesquisa a Porta do *Switch* associada a *Bridge*

Como descrito no item anterior, só temos uma porta associada a cada *Bridge*, pesquisamos então qual é a porta física associada a *Bridge* encontrada.

No exemplo abaixo, chegamos à porta física onde estava conectado o endereço IP procurado. O próximo comando executado foi:

snmpget 10.0.1.252 public@110 .1.3.6.1.2.1.17.1.4.1.2.135

Onde:

10.0.1.252 – endereço IP do *Switch* 2

public – community SNMP de leitura

110 – *Vlan* a ser pesquisada

.1.3.6.1.2.1.17.1.4.1.2 – OID da tabela pesquisada

.135 – Número da *bridge*

Obtivemos como resultado da porta associada à *bridge*:

.iso.3.6.1.2.1.17.1.4.1.2.135 = ***12***

4.7 Pesquisa Descrição da Porta

A porta física do *Switch* segue a lógica interna do hardware, dependendo da configuração. No nosso caso o *switch* possui módulos, e as portas tem a sua designação de acordo com a montagem do *Switch*. A porta externa visível corresponde a uma porta lógica.

Ex.: A porta 7 do módulo *Fastethernet* 3 é a porta lógica 12

Na pesquisa abaixo determinamos na estrutura física do *Switch* qual é a porta levantada na pesquisa anterior. Executamos o comando seguinte para pesquisar a descrição da porta 12 do *switch* 2:

snmpget 10.0.1.252 public@110 .1.3.6.1.2.1.31.1.1.1.1.12

Onde:

10.0.1.252 – endereço IP do *Switch* 2

public – community SNMP de leitura

110 – *Vlan* a ser pesquisada

.1.3.6.1.2.1.31.1.1.1.1 – OID da tabela pesquisada

Obtivemos como resultado a descrição da porta 12 do *Switch* 2 igual a Fa3/7, que corresponde a interface 7 Fast ethernet do módulo 3 do *Switch* 2, conforme abaixo:

iso.3.6.1.2.1.31.1.1.1.1.12 = "Fa3/7"

4.8 Consulta ao Ponto físico da Rede

Como descrito anteriormente, cada máquina esta ligada apenas uma porta de *Switch*, e na documentação cada porta de *Switch* corresponde a um ponto físico. Na planta da rede pesquisaremos a localização geográfica do ponto.

No exemplo anterior chegamos a porta Fa 3/7 do *Switch* 2. Consultamos então a tabela de pontos porta *Switch*/pontos da rede. Em nossa documentação constava que esta porta estava conectada ao ponto TC2-10A, quadrante C9. Chegamos ao ponto 10 do edifício A, ponto existente no TC2 , setor Técnico, quadrante C9 da planta baixa.

Concluindo, chegamos a posição física exata correspondente ao endereço IP 10.0.2.6.

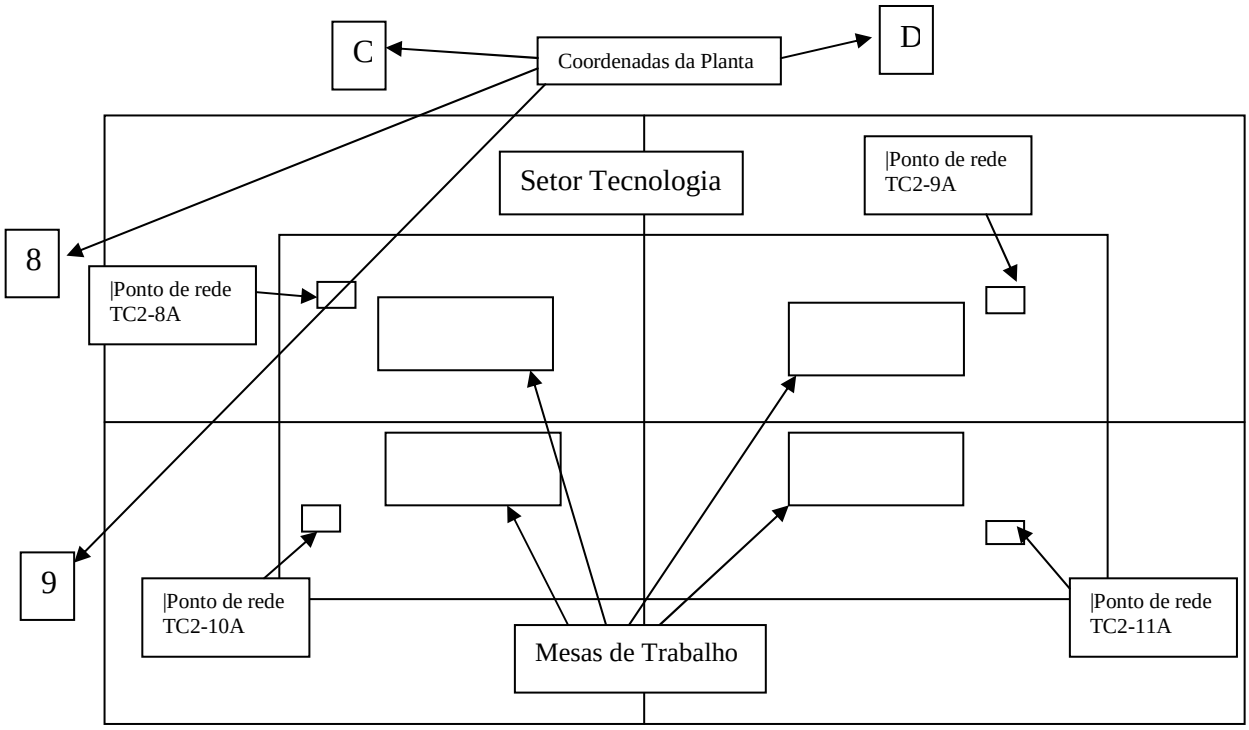

Figura 6 – Exemplo de planta baixa

5 CONCLUSÃO

5.1 Conclusão do trabalho

O modelo proposto mostrou-se eficaz no que diz respeito a extração e recuperação das informações nas várias fontes apresentadas. Com isso atende-se o objetivo proposto por este trabalho que é apresentar um estudo de detecção de ameaças internas na rede. Com o detalhamento das técnicas de extração de dados e apresentando um guia prático para aqueles que estão iniciando na área de administração de redes. Além disso, a apresentação de diversas ferramentas, juntamente com exemplos práticos, permite orientar o administrador de rede na escolha e manipulação de seus utilitários de análise.

Vale ressaltar neste ponto que as técnicas para extração das informações apresentadas neste trabalho não são de autoria do autor, e sim procedimentos pesquisados em documentos da CISCO e da NOVELL.

Sendo assim, este trabalho agrupou todos estes procedimentos para compor um processo de investigação ou um modelo de pesquisa de localização de usuário em rede.

Apesar das técnicas aqui descritas continua a pergunta “Quem esta conectado na rede?”. Será que a maioria dos administradores tem ciência das atividades e acessos na rede sob sua guarda? Com toda a certeza a resposta é não.

Diante de todas as novas tecnologias, do avanço e conhecimento dos Hackers e Crackers, muitas vezes disponível na Internet, e na extensa lista de responsabilidades impostas aos administradores de rede, com certeza o trabalho de elaboração de novas técnicas de detecção de quem está conectado na rede não se esgota aqui.

Existem vários programas comerciais para a detecção de intrusos (IDS) em uma rede, mas infelizmente nenhum deles consegue mostrar a localização física da ameaça, a maioria se atém a detectar o tipo de ataque e informar quais os endereços destino e origem, muitas vezes devido a diversidade das tecnologias de rede, da complexidade e especificidade da topologia. Na maior parte das vezes a pratica adotada é a defesa. Instalação de *Patch*s, *Firewall*, Bloqueios, constantes atualizações dos sistemas.

Infecções por vírus podem ser restringidas quando o foco destas é prontamente identificado. Ex.: log de tentativa de acesso de algumas estações diretamente para à Internet usando o serviço SMTP.

Fica a cargo do administrador fazer o seu “trabalho de casa”, montar o processo que mais lhe convier, e contra atacar, tentar localizar a origem do problema e, se possível, eliminá-lo.

5.2 Limitações da pesquisa

Para que seja efetiva a detecção, localização de usuários e/ou computadores em uma rede local, é necessário que a documentação e as configurações dos equipamentos estejam sempre atualizadas.

O trabalho de acompanhamento dos registros (*logs*) das ferramentas utilizados deve ser diário, e se preferível, pode-se usar programas e/ou scripts com execução periódica, para apontar algum desvio ou evento significativo.

Os exemplos descritos no presente trabalho podem ser adequados a outras redes com serviço de diretório, ou mesmo condensados em uma única ferramenta.

5.3 TRABALHOS FUTUROS

Existe a preocupação de automatizar o presente trabalho, entretanto não foi escolhida a linguagem adequada, uma vez que o desenvolvimento pode abranger uma gama variada de plataformas de sistemas operacionais.

O desenvolvimento de uma ferramenta única de pesquisa, que mostre inclusive a localização física, está planejada para uma próxima fase de estudos e graduação do autor.

REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, Andrew S. Redes de Computadores 4a. edição Rio de janeiro RJ: Editora Campus, 2003, 945 p.

SPURGEON, Charles E. Ethernet – O guia definitivo Rio de Janeiro RJ: Editora Campus, 2000, 477 p.

FRISCH, Aeleen Essential System Administrator Third Edition Sebastopol CA/USA: O'reilly, 2002, 1176 p.

HUNT, Craig TCP/IP Network Administration Third Edition Sebastopol CA/USA: O'reilly, 2002, 746 p.

GARFINEK, Simson; SPAFFORD, Gene; SCHWARTZ, Alan Pratical Unix & Internet Security Sebastopol CA/USA: O'reilly, 2003, 986 p.

NEMETH, Evi; SNYDER, Garth; SEEBASS, Scott; HEIN, Trent R. Manual de Administração do Sistema UNIX 3a. Edição São Paulo SP: Bookman, 2001, 896 p.

DERFLER, Frank J.; FREED Lês Tudo Sobre Cabeamento de Redes Rio de Janeiro: Editora Campus, 1996, 247 p.

COMER, Douglas E. Interligação em Redes com TCP/IP 2ª edição, 1998, Rio de Janeiro: Editora Campus, 700 p.

MAURO, Douglas R.; SCHMIDT, Kevin J. SNMP Essencial Rio de Janeiro RJ: Editora Campus, 2001, 316 p.

_____. How To Get Dynamic CAM Entries (CAM Table) for Catalyst Switchs Using SNMP Document ID: 13492 do site da CISCO, http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml, acessado em 28/08/2005.

NOVELL EDUCATION, Apostila do curso Administração do NetWare – Intranetware Curso 520 Orem Utah/USA, 1996, 423 p.

ANEXO 1

MIB SNMP dos equipamentos CISCO

.1.3.6.1.2.1.4.22
ipNetToMediaTable OBJECT-TYPE
-- FROM RFC1213-MIB
DESCRIPTION "The IP Address Translation table used for mapping from IP addresses to physical addresses."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) 22 }

.1.3.6.1.2.1.4.22.1.4
ipNetToMediaType OBJECT-TYPE
-- FROM RFC1213-MIB
SYNTAX Integer { other(1), invalid(2), dynamic(3), static(4) }
MAX-ACCESS read-create
STATUS Current
DESCRIPTION "The type of mapping.
Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) ipNetToMediaTable(22) ipNetToMediaEntry

.1.3.6.1.2.1.17.4.3.1.1
dot1dTpFdbAddress OBJECT-TYPE
-- FROM *BRIDGE*-MIB
-- TEXTUAL CONVENTION MacAddress
SYNTAX OCTET STRING (6)
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "A unicast MAC address for which the *bridge* has forwarding and/or filtering information."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) dot1d*Bridge*(17) dot1dTp(4) dot1dTpFdbTable(3) dot1dTpFdbEntry(1) 1 }

.1.3.6.1.2.1.17.4.3.1.2
dot1dTpFdbPort!OBJECT-TYPE
-- FROM *BRIDGE*-MIB
SYNTAX Integer
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "Either the value "0", or the port!number of the port!on which a frame having a source address equal to the value of the corresponding instance of dot1dTpFdbAddress has been seen. A value of "0" indicates that the port!number has not been learned, but that the *bridge* does have some forwarding/filtering information about this address (that is, in the StaticTable). Implementors are encouraged to assign the port!value to this object whenever it is learned, even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3)."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) dot1d*Bridge*(17) dot1dTp(4) dot1dTpFdbTable(3) dot1dTpFdbEntry(1) 2 }

.1.3.6.1.2.1.2.2.1.1
ifIndex OBJECT-TYPE
SYNTAX InterfaceIndex
MAX-ACCESS read-only
STATUS current
DESCRIPTION "A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."
::= { ifEntry 1 }

.1.3.6.1.2.1.17.1.4.1.2
dot1dBasePortIfIndex OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION "The value of the instance of the ifIndex object, defined in MIB-II, for the interface corresponding to this port."
::= { dot1dBasePortEntry 2 }

.1.3.6.1.2.1.31.1.1.1.1
ifName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The textual name of the interface. The value of this
object should be the name of the interface as assigned by
the local device and should be suitable for use in commands
entered at the device's `console'. This might be a text
name, such as `le0' or a simple port!number, such as `1',
depending on the interface naming syntax of the device. If
several entries in the ifTable together represent a single
interface as named by the device, then each will have the
same value of ifName. Note that for an agent which responds
to SNMP queries concerning an interface on some other
(proxied) device, then the value of ifName for such an
interface is the proxied device's local name for it.
If there is no local name, or this object is otherwise not
applicable, then this object contains a zero-length string."
::= { ifXEntry 1 }

Details of the MIB Variables--Includes Object Identifiers (OIDs)

vtp*Vlan*State OBJECT-TYPE
SYNTAX INTEGER { operational(1),
suspended(2),
mtuTooBigForDevice(3),
mtuTooBigForTrunk(4) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The state of this *VLAN*.

The state 'mtuTooBigForDevice' indicates that this device
cannot participate in this *VLAN* because the *VLAN*'s MTU is
larger than the device can support.

The state 'mtuTooBigForTrunk' indicates that while this
VLAN's MTU is supported by this device, it is too large for
one or more of the device's trunk ports."

::= { vtp*Vlan*Entry 2 }

.1.3.6.1.2.1.17.4.3.1.1
dot1dTpFdbAddress OBJECT-TYPE
-- FROM *BRIDGE*-MIB
-- TEXTUAL CONVENTION MacAddress
SYNTAX OCTET STRING (6)
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "A unicast MAC address for which the
bridge has forwarding and/or filtering information."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1)
dot1d*Bridge*(17) dot1dTp(4) dot1dTpFdbTable(3) dot1dTpFdbEntry(1) 1 }

.1.3.6.1.2.1.17.4.3

dot1dTpFdbTable OBJECT-TYPE
-- FROM *BRIDGE*-MIB
DESCRIPTION "A table that contains information about unicast entries for which the *bridge* has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) dot1d*Bridge*(17) dot1dTp(4) 3 }

.1.3.6.1.2.1.17.5.1
dot1dStaticTable OBJECT-TYPE
-- FROM *BRIDGE*-MIB
DESCRIPTION "A table containing filtering information configured into the *bridge* by (local or network) management specifying the set of ports to which frames received from specific ports and containing specific destination addresses are allowed to be forwarded. The value of zero in this table as the port!number from which frames with a specific destination address are received, is used to specify all ports for which there is no specific entry in this table for that particular destination address. Entries are valid for unicast and for group/broadcast addresses."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) dot1d*Bridge*(17) dot1dStatic(5) 1 }

.1.3.6.1.2.1.17.4.3.1.2
dot1dTpFdbPort!OBJECT-TYPE
-- FROM *BRIDGE*-MIB
SYNTAX Integer
MAX-ACCESS read-only
STATUS Mandatory
DESCRIPTION "Either the value "0", or the port!number of the port! on which a frame having a source address equal to the value of the corresponding instance of dot1dTpFdbAddress has been seen. A value of "0" indicates that the port!number has not been learned, but that the *bridge* does have some forwarding/filtering information about this address (that is, in the StaticTable).
Implementors are encouraged to assign the port!value to this object whenever it is learned, even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3)."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) dot1d*Bridge*(17) dot1dTp(4) dot1dTpFdbTable(3) dot1dTpFdbEntry(1) 2 }