Relatório de Estágio

Rex Antonio da Costa Medeiros

Relatório de Estágio submetido à coordenação de graduação do curso de Engenharia Elétrica da Universidade Federal da Paraíba – Campus II, como parte dos pré-requisitos para obtenção do grau de Engenheiro Eletricista.

Ênfase: Telecomunicações

Antônio Marcus Nogueira Lima
Professor orientador

Campina Grande, Paraíba, Brasil

© Rex Antonio da Costa Medeiros, Junho de 2002.

Biblioteca Setorial do CDSA. Fevereiro de 2021.

Sumé - PB

RENAULT

Este relatório apresenta as atividades desenvolvidas durante o estágio do aluno Rex Antonio da Costa Medeiros, do curso de Engenharia Elétrica da Universidade Federal da Paraíba – Campus II, realizado na Renault S.A., mais especificamente no *Centre Technique de Rueil*, situado à cidade de *Ruiel Malmaison*, França, no período de 15 de fevereiro a 30 de junho de 2001.

Sumário

1. APRESENTAÇÃO DA RENAULT S.A. 1

1.1. HISTÓRICO 1
1.2. ATIVIDADES DO GRUPO RENAULT 2
1.3. ORGANOGRAMA DA INSTITUIÇÃO 2

2. VISÃO GERAL DO ESTÁGIO 4

2.1. AS EQUIPES DE ADMINISTRAÇÃO E ASSISTÊNCIA TÉCNICA 5
2.2. RECURSOS DISPONÍVEIS NOS EQUIPAMENTOS CISCO INC. 5
2.2.1. Virtual LANs (VLANs) *6*
2.2.2. Domínio VTP *6*
2.2.3. Spanning Tree *7*
2.2.4. O agrupamento de portas *8*
2.3. ARQUITETURA DA REDE DO CTR 8
2.4. FERRAMENTAS DE GERENCIAMENTO E MONITORAÇÃO DA REDE 10
2.4.1. As estações de gerenciamento HP Openview *10*
2.4.2. O software TCRCatalyst *11*
2.4.3. Os scripts shell *11*
2.4.4. O portal web Dépannage Réseau CTR/CTL *13*

3. O SOFTWARE CISCOWORKS2000 15

3.1. CISCOWORKS2000 SERVER 16
3.1.1. O servidor ANI *16*
3.2. *RESOURCE MANAGER ESSENTIALS* 18
3.3. *CAMPUS MANAGER* 19
3.3.1. A aplicação User Tracking *21*
3.4. *DEVICE MANAGER* 22
3.5. AVALIAÇÃO DO CISCOWORKS2000 23
3.5.1. Análise da ferramenta User Tracking do CWSI *24*

4. O UTILITÁRIO CTR *USER TRACKING* 27

4.1. DESCRIÇÃO GERAL DO PROGRAMA 27
4.2. DIFICULDADES DE IMPLEMENTAÇÃO 28
4.3. FLUXOGRAMA DO PROGRAMA 29
4.4. AVALIAÇÃO, LIMITAÇÕES DO PROGRAMA E TRABALHOS FUTUROS 33

5. CONSIDERAÇÕES FINAIS 36

6. REFERÊNCIAS 37

1. Apresentação da Renault S.A.

Criada em 1899 a Billancourt (região parisiense) pelos irmãos Renault, a sociedade Renault S.A. é hoje o segundo maior grupo industrial francês. Dirigida por Louis SCHWEITZER, o grupo Renault possui um capital de 40,175 bilhões de euros, contando com um efetivo global de 161.114 pessoas.

1.1. Histórico

Em 1914, a Renault entra na história com os famosos táxis "*de la Marne*". Devido ao grande sucesso, 1200 unidades foram fabricadas para o transporte de soldados franceses durante a primeira guerra mundial. Depois da guerra, a empresa retoma a fabricação de veículos particulares.

Em 1922, a Sociedade Anônima das Fábricas Renault é criada. A sociedade reafirma sua posição no mercado participando de exposições de carros esportivos, como em 1926, batendo o recorde mundial de quilometragem alcançada em 24 horas por um veículo equipado com motor de 40 CV (4.167,78 km com média de 173,65 km/h). Tratava-se de um *Latécoère* 25 com motor Renault.

Em 1940, após a tomada da França pelos alemães, as fábricas da Renault passam a ser controladas pela Alemanha. Durante toda a segunda guerra mundial, a empresa fabrica automóveis militares, caminhões e motores de aviões, além de barcos e trens. Após libertação em 1945, o estado francês assume o controle total da empresa, que passa a ser chamada de Grupamento Nacional das Fábricas Renault (RNUR – *Régie Nationale des Usines Renault*).

Entre as décadas de 50 a 70, há uma explosão no mercado internacional de automóveis. Foram 20 anos de conquistas industriais e sociais. Em 1973, o Renault 5 e o Renault 12 são os automóveis franceses mais vendidos no mundo.

Em seguida, durante os anos 80, verificou-se uma redução importante no número de vendas e começou-se uma crise social. A partir de 1985, com a chegada de Georges BESSE à presidência, houve uma redução significativa no número de funcionários e uma política de qualidade rigorosa foi instaurada, permitindo o retorno do crescimento da empresa. Em 1986, BESSE, quinto presidente do Grupo Renault, é barbaramente assassinado.

Em 1990, a Renault se torna novamente uma sociedade anônima e, em seguida, assume o controle acionário da Volvo. Porém, em 1993 o projeto de fusão Renault-Volvo é abandonado. Em 1994 a Renault abre o seu capital à iniciativa privada e, durante o ano de 1996, a empresa é enfim privatizada e o acordo com a Volvo é refeito.

Em 1999 a Renault assume o controle de uma segunda marca, a Darcia (Romena). No mesmo período, ela adquire 37% do capital da japonesa Nissan, tornando-se então o quarto maior fabricante de automóveis do mundo. Em 2000, a Renault adquire 70% do capital da Samsung Motors.

1.2. Atividades do Grupo Renault

As atividades desenvolvidas pelo Grupo Renault são centradas no estudo (projeto), na produção e na comercialização de veículos particulares, utilitários e veículos industriais. O grupo é formado por três setores de atividades:

O setor automobilístico sempre foi a principal atividade da Renault. Este setor projeta, fabrica e comercializa automóveis de passeio e veículos utilitários, como também máquinas e implementos agrícolas. O setor detém certa de 78,4% do capital total do Grupo Renault. Em números, o setor automobilístico possui um efetivo de 131.261 funcionários espalhados pelo mundo, tendo vendido 1.872.631 veículos em 2000, movimentando certa de 31,5 bilhões de euros.

O setor de veículos industriais integra os grupos Renault V.I. e Mack Truck Inc. Eles projetam, fabricam e comercializam caminhões, veículos militares e veículos especiais. Em 2000, as vendas globais do grupo Renault V.I./Mack foram de 103.646 veículos contra 93.354 em 1999, com alta de 11%. Em termos de capital, o setor de veículos industriais representa 17,5% do capital do grupo Renault, ou seja, 7,033 bilhões de euros.

O setor financeiro engloba mais de quarenta sociedades de financiamento e dois bancos. Este setor funciona como um mecanismo de acompanhamento das atividades financeiras e comerciais do Grupo no mercado mundial. O setor responde por 4,1% do capital do Grupo.

1.3. Organograma da instituição

A estrutura organizacional simplificada do Grupo Renault, representada pelo seu organograma, é mostrada na Figura 1. O estágio foi realizado junto ao SAEL CTR/CTL, ligado ao Pólo de Infra-estrutura da Região Parisiense (PIRP – *Pole Infrastructure Région Parisienne*), que é subordinado a Direção das Entidades Operacionais Locais (DEOL – *Direction des Entités Opérationnelles Locales*) e a Direção de Tecnologias e Sistemas de Informação (DTSI – *Direction des Technologies et Systèmes d'Information*).

A PIRP tem como missão assegurar a disponibilidade e a qualidade dos serviços das redes de computadores (LANs e MANs), dos sistemas de telecomunicações (telefonia,

videoconferência, etc.) e o correto funcionamento dos terminais de computadores e telefônicos dos estabelecimentos Renault na região parisiense (*Île de France*). É função também da PIRP a implantação e o remanejamento dos serviços de telecomunicações e informática para funcionários que se deslocam fisicamente dentro da sua área de atuação.

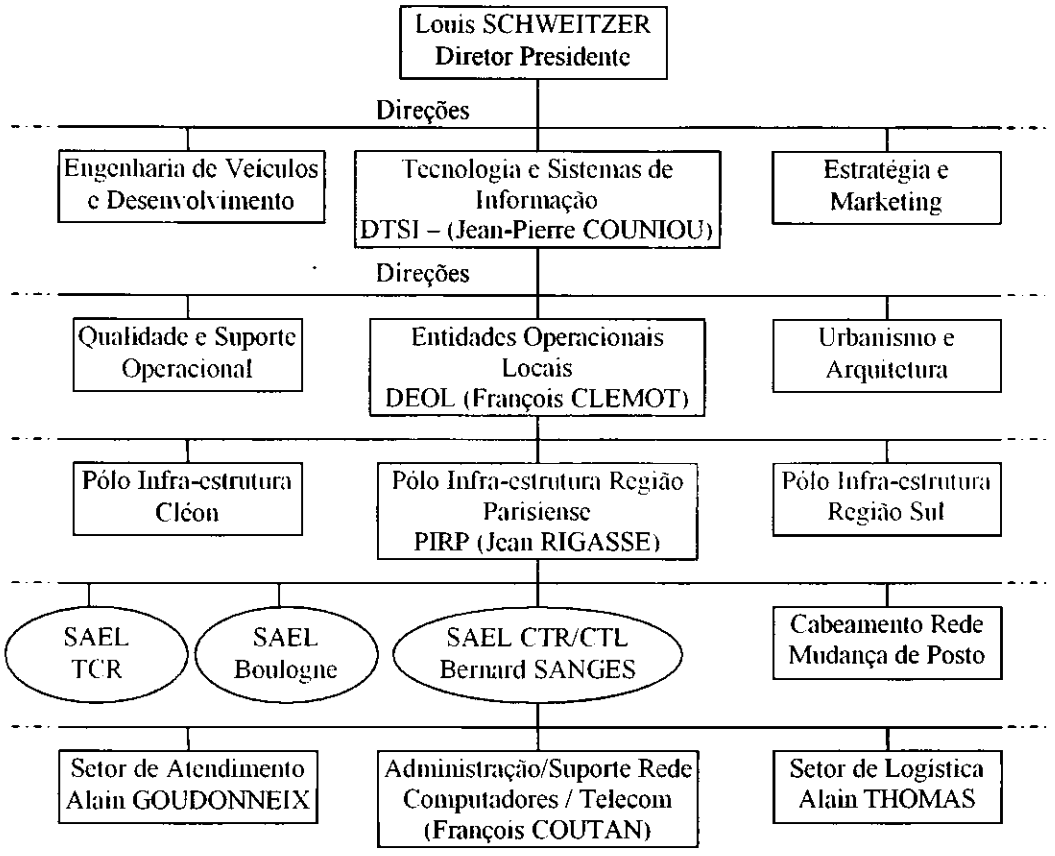


Figura 1: Organograma Renault.

Como pode ser visto pelo organograma, a PIRP é subdividida em três grupos de Suporte e Assistência Operacional Local SAELs (*Support Assistance Exploitation Locale*): o SAEL TCR, o SAEL Boulogne e o SAEL CTR/CTL; isto porque a Renault possui inúmeros centros de pesquisa distribuídos pela região parisiense. Assim, o SAEL TCR representa o PIRP no maior centro de pesquisa da Renault, o *Technocentre*, situado à cidade de Saint Quentin en Yvelines e centros de pesquisas adjacentes. O CTR Boulogne cobre as instalações da central administrativa do Grupo, localizado à cidade de Boulogne, sul de Paris. Já o SAEL CTR/CTL, atua no Centro Técnico de Rueil Malmaison e no Centro Técnico de Lardy. Outros centros menores, como o Centro Técnico de Marrolle e o Centro Técnico *"de la rue des epées"* possuem seus sistemas de comunicação administrados pela equipe do SAEL CTR/CTL.

2. Visão geral do estágio

Como mencionado, o presente estágio foi realizado no Centro Técnico de Rueil (CTR), localizado à cidade de Ruiel Malmaison. Mais precisamente, o estagiário atuou junto à equipe do SAEL CTR/CTL responsável pela administração da rede de computadores do Centro Técnico de Ruiel e do Centro Técnico de Lardy, além de centros menores nas adjacências, sob a tutoria do engenheiro François COUTAN.

Num ambiente com mais de 7000 usuários espalhados por uma área urbana e uma rede de computadores que possui cerca de 130 comutadores (*switches*) e dezenas de redes locais, é necessário dispor de ferramentas de diagnóstico e de administração remota dos elementos de rede. Além disso, elas devem ser fáceis de operar e devem possuir um alto grau de confiabilidade e níveis de segurança definidos, já que elas serão usadas por técnicos.

Neste contexto, os objetivos gerais do estágio foram:

- Fazer uma análise dos utilitários já existentes, mapeando suas funcionalidades;
- Analisar o software CiscoWorks2000 (CWSI) da Cisco Inc., recém adquirido pela PIRP;
- Comparar as suas funcionalidades do CWSI com as das ferramentas existentes;
- Disponibilizar os recursos do CWSI para a equipe técnica;
- Se necessário, desenvolver outras ferramentas, que possam auxiliar na administração da rede.

A Tabela abaixo ilustra o cronograma de realização do estagio.

Atividade \ Mês (2001)	**15 FEV**	**MAR**	**ABR**	**MAI**	**JUN**
Estudo da topologia da rede	X	X			
Análise das ferramentas de gerência		X	X		
Estudo do CWSI		X	X	X	
Comparação de suas funcionalidades com as dos utilitários existentes.		X	X	X	
Disponibilizar recursos do CWSI (caso seja viável)				X	X
Desenvolver novas ferramentas (se necessário)				X	X
Documentação		X	X	X	X

Para o total entendimento do trabalho realizado, é necessário o conhecimento da arquitetura da rede de computares do CTR, de alguns conceitos aplicados a redes locais modernas e terminologias de uso proprietário da Cisco Inc. Dada a natureza do estágio, é interessante apresentar a organização das equipes responsáveis pela supervisão e assistência técnica aos usuários.

2.1. As equipes de administração e assistência técnica

Quando um terminal de computador ou impressora conectados à rede dos centros de pesquisa da região parisiense deixa de funcionar, o usuário Renault dispõe de uma central de atendimento com cerca de 80 técnicos que recebem as ligações e tentam solucionar o problema remotamente ou, pelo menos, detectar a natureza do mesmo. Essa equipe é dita ser de grau 1.

Caso o problema persista, a central de atendimento repassa o pedido ao SAEL referente à área do usuário. Se o problema for na rede de computadores (porta do *switch* desabilitada, endereço ou máscara IP incorreta, etc), uma equipe mais especializada de aproximadamente 10 técnicos é acionada, devendo solucionar o problema em, no máximo, 2 horas. Essa equipe é dita ser de grau 2.

A equipe grau 2, no entanto, opera simples ferramentas de diagnóstico e gerenciamento de equipamentos de redes. Elas não possuem privilégios suficientes para alterar a configuração de rotas num roteador, por exemplo. Quando o problema exige uma intervenção mais séria, é acionada uma equipe de dois técnicos dita ser de grau 3, na ocasião formada por Daniel LECOUELLE e Tozé DIAS, e treinada pela própria Cisco. É essa equipe que configura novos comutadores e roteadores e somente eles, juntamente com seu responsável direto, possuem as senhas de acesso aos roteadores e comutadores. O estagiário trabalhou diretamente com o técnico Tozé DIAS.

2.2. Recursos disponíveis nos equipamentos Cisco Inc.

Para entender o funcionamento lógico da rede do CTR é necessário conhecer alguns conceitos suplementares sobre rede como: o que são VLANs (*Virtual LANs*), um domínio VTP (*Virtual Trunking Protocol)*, o que é *Spanning Tree* e o conceito de agrupamento de portas (*port channel*).

2.2.1. *Virtual LANs (VLANs)*

Uma VLAN é um grupo de entidades (computadores, impressoras, etc) interligados e compartilhando um conjunto comum de regras, independente da localização física. Uma VLAN se comporta da mesma forma que uma rede local, com a diferença de que é possível agrupar entidades mesmo se elas não estão localizadas no mesmo segmento de rede.

O uso de VLANs permite agrupar portas de um *switch* de tal forma a limitar o fluxo de dados gerados por difusões em *unicast, multicast* e *broadcast*. O tráfego gerado em uma determinada VLAN é somente repassado as portas dos *switches* que pertencem àquela VLAN.

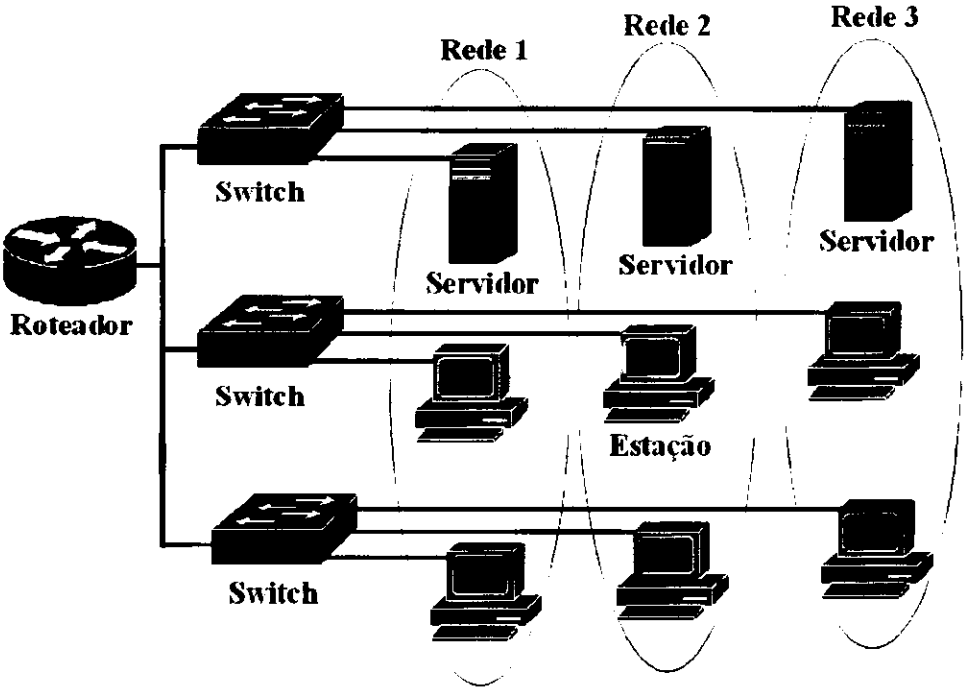


Figura 2: Exemplo de utilização de VLANs.

A Figura 2 mostra uma rede contendo três VLANs. Apesar de estarem conectadas a comutadores diferentes, as estações referentes à Rede 1, por exemplo, se comunicam sem a necessidade de roteamento, desde que estejam na mesma sub-rede física. O tráfego entre VLANs, ao contrário, deve sempre ser roteado.

O primeiro passo para a criação de uma VLAN é escolher um número, que para um *switch* Cisco *Catalyst* série 4000 pode ser entre 1 (*default*) e 1000. Outros parâmetros igualmente importantes são: tipo da VLAN (Ethernet, ATM, etc.), MTU (*Maximum transmission unit*), e nome da VLAN.

2.2.2. Domínio VTP

VTP (*Virtual Truking Protocol*) é um protocolo de mensagens nível 2 responsável por manter consistentes as configurações das VLANs, gerenciando a adição, remoção e edição de

seus parâmetros. Com o uso do VTP é possível centralizar as mudanças de configuração em um ou mais *switches*, de tal forma que as novas configurações sejam automaticamente aplicadas aos outros comutadores da rede.

Mais especificamente, o protocolo VTP é utilizado para gerir as configurações das VLANs quando, por um conjunto de *switches* interligados, fluem tráfego de diversas VLANs. Os enlaces físicos (*links*) que interligam esses *switches* são chamados de troncos (*trunks*) e as portas a eles associadas devem ser configuradas como tal. A Figura 3 ilustra uma situação onde o comutador A é usado para interligar dois outros comutadores A e B e o roteador. Em resumo, todo o tráfego de diferentes VLANs que entra ou sai de um *switch* deve ser escoado por um enlace *trunk*.

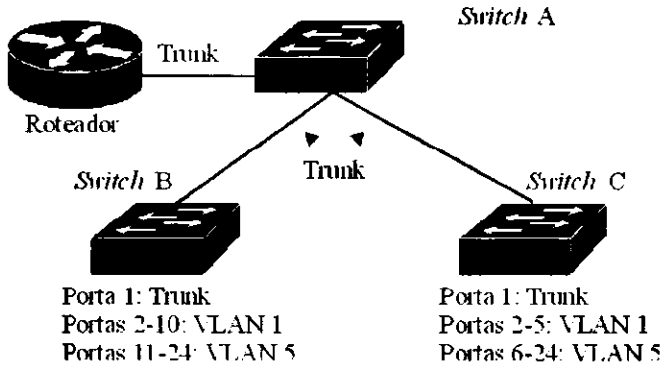


Figura 3: Domínios VTPs e enlaces *trunks*.

Um domínio VTP (também chamado de domínio de gerenciamento de VLANs) é formado por um ou mais *switches* interligados que compartilham o mesmo nome de domínio VTP. Um *switch* só pode ser configurado de forma a estar em apenas um domínio VTP. Os comutadores pertencentes a um domínio VTP podem ser configurados como sendo servidores VTP, clientes VTP ou modo transparente. Quando o *switch* é configurado como servidor VTP, todas as mudanças feitas nas configurações das VLANs são repassadas aos outros comutadores do domínio, por intermédio de mensagens VTP. Um *switch* cliente VTP não pode efetuar esse tipo de mudança de configuração.

2.2.3. *Spanning Tree*

Em redes que exigem um alto grau de confiabilidade, a utilização de redundâncias de seus elementos é quase uma obrigatoriedade. No entanto, em redes ethernet não é permitida a existência de dois ou mais caminhos entre duas estações. Para evitar a formação de laços quando redundâncias de enlaces físicos se fazem presente, são usados os protocolos de *spanning tree*, que gerenciam a ativação das portas dos comutadores, de acordo com

prioridades a elas atribuídas, de tal forma a manter a unicidade de caminho entre os as estações da rede. Nos equipamentos Cisco, esse gerenciamento é feito pelo protocolo proprietário MISTP (*Multi-Instance Spanning Tree Protocol*), que é baseado no protocolo IEEE 802.1D bSTP (*bridge Spanning Tree Protocol*).

2.2.4. O agrupamento de portas

Os equipamentos de comutação mais modernos da Cisco apresentam um recurso de agrupamento de portas, denominado de *port channel*, que permite utilizar duas portas de um comutador ou roteador para formar um só enlace lógico de transmissão. Esse recurso permite duplicar a capacidade de um *link* simples. É usado principalmente na conexão dos *switches* centrais com os roteadores (*backbone* da rede) e também em enlaces entre os *switches* do núcleo da rede e os servidores de arquivos.

2.3. Arquitetura da rede do CTR

A rede de computadores administrada pelo SAEL CTR/CTL possui certa de 130 comutadores (*switches*), totalizando mais de 8000 pontos de rede, sendo aproximadamente 6500 pontos no CTR e os restantes distribuídos no CTL e adjacências. Um diagrama da rede do CTR é mostrado na Figura 4.

A rede física é divida logicamente em três domínios VTP: o domínio VTP CTRA2A3, compreendendo os comutadores da parte superior da Figura 4, o domínio VTP abc, composto pelos comutadores da parte inferior e o domínio VTP SERVCENTRCTR, que compreende ao conjunto de comutadores que interligam os servidores, vistos do lado esquerdo do diagrama.

Ao centro, se encontram os dois roteadores ctr_rvl01 e ctr_rvl02, que são os roteadores de VLANs, sendo o primeiro configurado para rotear tráfegos originários de VLANs pares e o segundo tráfegos de VLANs ímpares. No entanto, em caso de falha de algum deles, o protocolo de *spanning tree* atuará de tal forma a redirecionar o tráfego para o outro roteador. O roteamento do tráfego de entrada / saída do CTR é feito pelos roteadores ctr_r01, ctr_r02, ctr_r03 e ctr_r04.

Acima e abaixo dos roteadores de VLANs, são usados três níveis de comutadores. O primeiro, que integra o *backbone* da rede, é formado pelos comutadores nomeados de LTP01 a LTP04. O segundo nível é formado pelos comutadores LTB01 a LBT12, que interligam os comutadores do núcleo e os comutadores aos quais as estações de trabalho estão conectadas,

nomeados de LTSxxx, onde *xxx* designa o byte final do endereço IP de cada comutador LTS, agrupados em uma VLAN de administração.

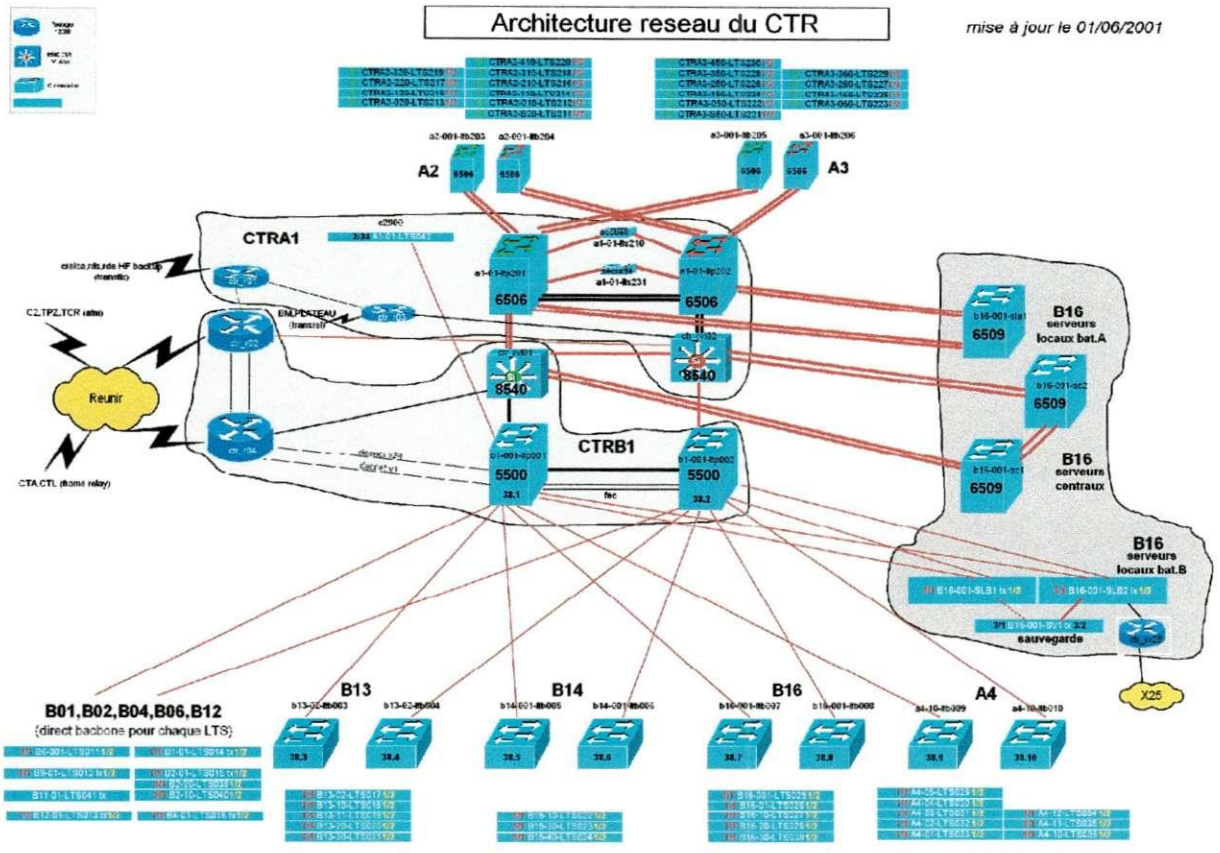


Figura 4: Arquitetura da rede do CTR.

Os enlaces físicos entre os equipamentos do *backbone* da rede são de fibra óptica com taxas de transmissão variando de 200 Mbps (2 fibras a 100 Mbits – *fast ethernet*) a 2 Gbps (2 fibras a 1Gbps – *gigabit ethernet*). O enlace de saída do CTR é ATM, com taxa de transmissão de 655 Mbps (ver roteadores ctr_r01 e ctr_r02).

A supervisão da rede deve ser tal que qualquer falha registrada em algum comutador, roteador ou enlaces entre eles deve ser automaticamente identificada, de forma a permitir uma rápida intervenção por parte da equipe de suporte. Neste nível de administração, é utilizado o software de gerenciamento HP *Openview*, baseado no protocolo SNMP (*Simple Network Management Protocol*). A outra opção de gerenciamento é o software CiscoWorks2000, alvo de estudo neste estágio.

Vale salientar que concentradores (*hubs*) não estão presentes na rede, ou seja, todas as estações de trabalho são conectadas diretamente a portas dos *switches*. Isto permite uma gerência nível 2 (MAC) aplicada a todos os elementos ativos da rede.

2.4. Ferramentas de gerenciamento e monitoração da rede

Paralelamente ao estudo da topologia e do funcionamento lógico da rede, foi feito um levantamento das ferramentas de supervisão, controle e configuração da rede SAEL CTR/CTL.

2.4.1. As estações de gerenciamento HP *Openview*

Apesar dos três SAELs gerenciarem redes diferentes em diversos centros de pesquisa Renault espalhados pela região parisiense, há uma interação muito forte entre as equipes, de forma que elas compartilham praticamente o mesmo conjunto de ferramentas.

A supervisão nível 3 da rede é feita através de três estações risc HP *Openview*, rodando sistema operacional HP-UX. Cada SAEL possui sua estação de gerenciamento e, apesar de estarem fisicamente separadas, elas estão sempre sincronizadas com relação às ferramentas que disponibilizam.

O HP *openview* é um software de supervisão de rede que opera na camada 3 da arquitetura ethernet. Isto significa que ele não consegue distinguir a maneira com que os comutadores LTP, LTB e LTS estão conectados na Figura 4. Para o HP *Openview*, todos os *switches* estão conectados em um só barramento e este conectado aos roteadores de VLANs. Aliás, a existência de VLANs é ignorada para o HP *Openview*, já que elas só existem para os protocolos da camada 2 (MAC).

O *openview* opera em tempo real e é baseado no protocolo SNMP. As versões mais atuais do software dispõem de ambientes gráficos, chamados de mapas, onde os equipamentos de redes são representados por ícones, e os enlaces por linhas interligando-os. Os equipamentos devem ter seus agentes SNMP configurados de tal forma a enviarem suas mensagens (*traps*) SNMP as estações de gerenciamento. Mensagens SNMP são geradas pelos equipamentos de rede quando ocorrem alterações nas suas configurações, quando o módulo supervisor detecta falha em algum subsistema, quando a falha é corrigida, etc. Assim, a simples conexão de uma estação ao comutador gera uma mensagem SNMP confirmando que a porta do comutador foi ativada.

As mensagens SNMP possuem níveis de prioridades e estas devem ser configuradas junto aos agentes SNMP dos equipamentos. Por exemplo, em um *switch*, mensagens SNMP originárias da inserção de uma simples estação de trabalho ao barramento devem ter baixa prioridade. Já quando um servidor central de arquivos for ligado a uma porta do comutador, o monitoramento do estado da porta se torna crítico, e qualquer alteração deve ser

imediatamente identificada. Logo, a mensagem SNMP com relação àquela porta, deve possuir uma prioridade alta.

Traps SNMP que chegam as estações *openview* são analisados em tempo real e, dependendo de seu conteúdo, alertas são gerados na forma de janelas *pop-up* e, caso algum equipamento pare de funcionar, a cor do ícone corresponde muda, geralmente de verde para amarelo, azul, vermelho, dependendo da gravidade da situação (e da versão do software!).

2.4.2. O software TCRCatalyst

O software TCRCatalyst foi desenvolvido pela equipe SAEL do TCR (*Technocentre*) e tem como principal função fazer o mapeamento entre os endereços IPs de máquinas conectadas as portas dos comutadores Cisco e números atribuídos a cada ponto de rede.

Basicamente o que é feito é associar o identificador do ponto de rede a porta do comutador ao qual ele se conecta. Este é o trabalho manual que o software exige. A partir desse ponto, o software agenda horário para interrogar, via SNMP, os comutadores da rede, com o objetivo de descobrir quais são os endereços MAC conectados a cada porta. Os dados são armazenados em um banco de dados. Em seguida, as tabelas ARP dos roteadores de VLANs são recuperadas, as quais relacionam o endereço MAC de uma máquina com o seu endereço IP. De posse das informações, o software associa o número do ponto de rede ao endereço IP da máquina.

Além de fazer esta equivalência, o TCRCatalyst avalia o estado de cada porta dos comutadores e gera um relatório das portas que se encontram em *shutdown*. Quando é ativada a segurança numa porta de um *switch* Cisco, ele armazena o endereço MAC da primeira máquina a se conectar após a ativação. O endereço permanece armazenado mesmo que a estação seja desligada. Assim, se outra interface de rede se conectar a porta segura, automaticamente ela é desabilitada (entra no estado *shutdown*) e o novo endereço é armazenado.

Essa ferramenta seria bastante útil se a tabela onde são armazenadas as informações de equivalência ponto de rede / porta do comutador fosse confiável. No entanto, os técnicos responsáveis pela instalação das estações de trabalho não tomam o cuidado aferir essas informações. O TCRCatalyst é de uso da equipe técnica de grau 2.

2.4.3. Os scripts *shell*

Durante mais de seis anos, um técnico lotado ao SAEL TCR chamado Gerard CAIE, especialista em redes cisco, sistema operacional Unix, HP *openview* e programação *shell*,

desenvolveu (e continua desenvolvendo) uma série de scripts *shell* que, combinados ao HP *openview* e ao TCRCatalyst, formam um poderoso conjunto de ferramentas de gerenciamento e supervisão. Os scripts são alojados nas três estações de gerenciamento da HP, cabendo ao mesmo técnico a sincronização das estações, descrita em 2.4.1. Alguns scripts são desenvolvidos em linguagem Perl.

A execução dos scripts é feita, quase em sua totalidade, de forma automática, através da programação de horários. Serão descritas aqui as tarefas administrativas mais importantes realizadas pelo conjunto de scripts.

A primeira delas é a cópia de segurança (*back-up*) dos arquivos de configuração de todos os equipamentos de rede, tais como *switches* e roteadores. A cada 24 horas é feita uma cópia desses arquivos e são mantidas arquivadas as configurações dos últimos três dias. Esses arquivos, principalmente os oriundos dos roteadores, são fontes de informações importantíssimas e alvo de análise de vários outros scripts. Um deles, por exemplo, analisa as configurações dos roteadores de VLANs com o objetivo de extrair informações sobre as sub-redes associadas, presentes no centro de pesquisa. Elas são identificadas com a VLAN correspondente e as informações, sempre atuais, são armazenadas em arquivos texto das mesmas estações.

Outros grupos de scripts mantêm atualizada uma série de arquivos texto que contém informações sobre os equipamentos da rede. Isto é feito analisando os arquivos de configuração e executando comandos remotos[1] (através do comando Unix rsh – *remote shell*) nos equipamentos de tal forma a obter, por exemplo:

- Informações sobre cada equipamento: endereço IP, nome do equipamento, domínio VTP, número de série; número de módulos instalados; seriais dos módulos; memória instalada no supervisor; versão do sistema operacional instado no supervisor; etc.
- Informações sobre portas dos módulos: número de portas de cada módulo; nome das portas, capacidades; VLANs associadas,
- Arquivos com as tabelas ARP dos roteadores. Além de associar o endereço IP com o endereço MAC, o arquivo ainda indica a rede, a VLAN e a porta canal (*port channel*) associada ao endereço.

Essas e outras informações são dispostas numa árvore de diretório que começa pelo domínio de gerência dos SAELs, ou seja, pelos diretório TCR (*Technocentre*), CTR e TPZ

[1] Executar comandos remotos é mais rápido e prático do que interrogar o equipamento via SNMP.

(*Trapèze* – como é conhecido a central administrativa de Boulogne) e seguem dependendo do tipo de informação contida nos arquivos texto.

Um grupo de scripts de fundamental importância são aqueles utilizados para a atualização automática dos softwares dos *switches* e roteadores. Imagine uma rede com mais de 130 *switches* cujos softwares necessitem de uma atualização. Os scripts testam versão e compatibilidade dos novos softwares antes de efetuar a atualização.

Scripts que podem colher informações em tempo real também foram desenvolvidos. É possível, por exemplo, traçar o caminho nível 2 entre duas estações quaisquer da rede, desde que elas estejam ligadas. O script totalmente em linguagem *shell*, encontra primeiro o comutador e a porta a qual está conectada a estação de origem. Em seguida, é feita uma análise para determinar a VLAN e por qual enlace tronco os pacotes são encaminhados. Esse processo é feito até que se chegue ao comutador destino, no caso das duas estações estarem na mesma sub-rede, ou no roteador, caso contrário. Neste caso, é possível identificar por qual enlace o roteador envia o pacote e o próximo *switch* é identificado. O processo continua até que o comutador de destino seja descoberto. É possível saber a porta a qual a estação de destino está conectada, bastando listar os endereços MAC presentes em cada porta do *switch* de destino.

Esta foi uma pequena amostra de um trabalho sério em busca de mecanismos de gerenciamento eficazes para as redes locais Renault da região parisiense. Um novo trabalho que vem sendo feito, e que está em fase bem adiantada, é de transformar esses scripts *shell* em scripts CGI (usando a mesma linguagem) e com isso disponibilizar todas essas informações através de um portal Web, tornando-os acessíveis de qualquer máquina que possua um navegador Web, como o Netscape.

2.4.4. O portal web *Dépannage Réseau CTR/CTL*

A equipe de suporte grau 2 é responsável pela resolução da maioria dos problemas relacionados à rede. Mas eles não possuem permissão para alterar a configuração dos *switches* ou roteadores diretamente por *shell* remoto ou telnet. Como ferramentas de identificação / diagnóstico, os técnicos de grau 2 possuem o HP *openview* (em modo leitura), o TCRCatalyst, e uma exportação do bancos de dados *User Tracking*, que será descrito na seção 3.3.1. Para visualizar as configurações dos equipamentos de rede e efetuar alterações simples nas configurações, eles utilizam um conjunto de scripts CGI, desenvolvidos por Daniel LECOUELLE em linguagem *shell*, organizados em um portal web chamado de *Dépannage*

Réseau CTR/CTL, organizado em duas partes: uma de diagnóstico e outra de alteração de configuração.

Na parte de diagnóstico, o portal oferece a possibilidade de efetuar comandos remotos pré-determinados de leitura de configurações nos *switches*. Para isso, um formulário com campos para entrada do nome *switch* e outras informações é disponibilizado. Os principais comandos são: *show port*, que retorna o estado de cada porta do comutador; *show conf*, que mostra a configuração geral do *switch*, *show vtp domain*, que retorna o domínio VTP do comutador e *show VLAN*, que retorna a VLAN associada a cada porta do comutador.

A parte de alteração de configuração permite a mudança de alguns parâmetros associados às portas dos *switches*, tais como:

- VLAN associada à porta;
- Nome da porta;
- Velocidade da porta (10/100 Mbps).
- Estado da porta para ativado, quando a mesma estivesse no modo *shutdown* (ver seção 2.4.2).

Com esses recursos, os técnicos grau 2 resolvem quase a totalidade dos problemas que chegam até eles, de maneira simples, rápida e segura.

3. O software CiscoWorks2000.

CiscoWorks2000 (CWSI) é um conjunto de utilitários de gerenciamento de equipamentos de rede Cisco. Os utilitários são desenvolvidos utilizando linguagem Java. A interface com o usuário, no entanto, é feita através de um navegador web, como o Netscape ou o Internet Explorer. A Figura 5 ilustra o ambiente de trabalho do CiscoWorks2000.

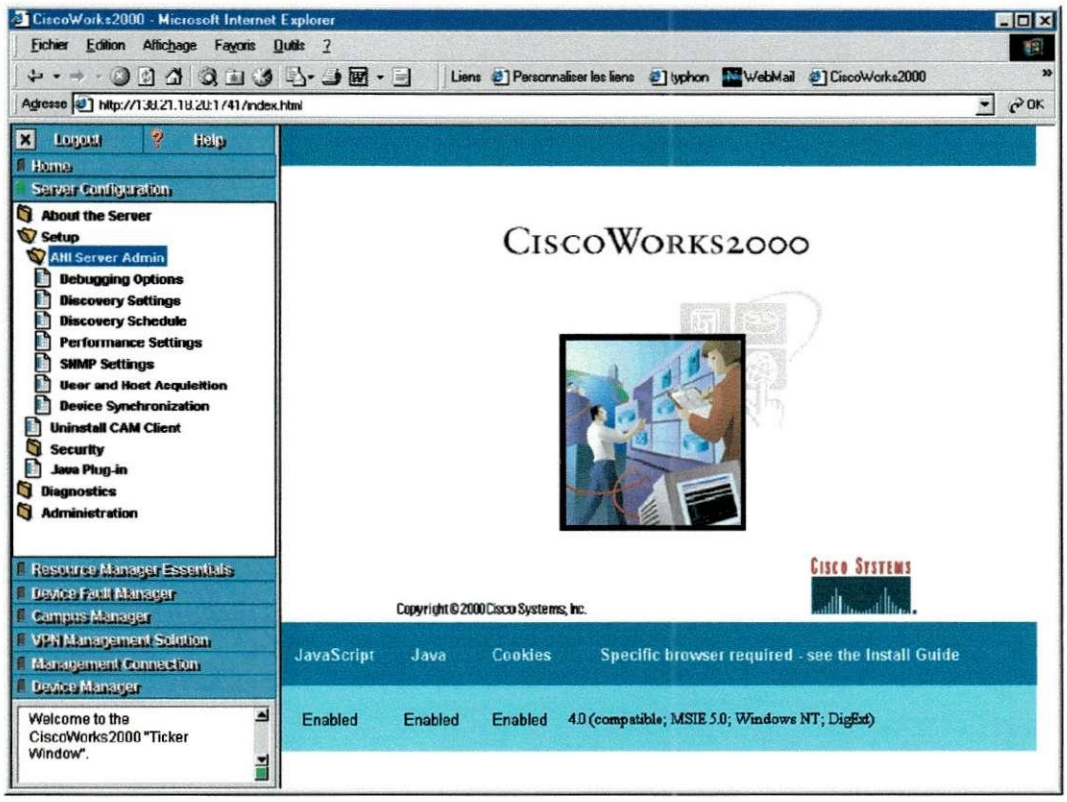


Figura 5: Interface CiscoWorks2000.

Os utilitários de gerenciamento do CWSI estão divididos em quatro módulos, de acordo com a suas funcionalidades:

- CiscoWorks2000 *Server;*
- *Resource Manager Essentials;*
- *Campus Manager;*
- *Device Manager.*

Uma descrição detalhada de cada módulo, destacando suas funcionalidades, é apresentada nas seções que se seguem. A seção 3.5 apresenta a avaliação feita pelo estagiário acerca do produto, destacando principalmente seu desempenho e uma possível utilização do software pela equipe de supervisão do CTR.

3.1. CiscoWorks2000 Server

O módulo servidor do CiscoWorks2000 é uma coleção de serviços que são compartilhados com os outros utilitários de gerenciamento de rede. Todos os módulos do CWSI dependem do módulo servidor para funcionarem corretamente. Suas principais funções são:

- Criação de contas de usuários, definição de permissões e autenticação;
- Configuração e administração do produto;
- Diagnóstico e detecção de problemas de funcionamento dos módulos

3.1.1. O servidor ANI

Além da criação e gerenciamento de contas de usuários, o CiscoWorks2000 Server é responsável pela configuração e inicialização do servidor ANI (*Asynchronous Network Interface*), que é uma aplicação responsável por rastrear todos os equipamentos cisco presentes na rede, recuperando toda e qualquer informação que eles possam disponibilizar e armazená-las em banco de dados proprietários. Algumas dessas informações são listadas abaixo:

- Conjunto de comutadores e roteadores da rede e como eles estão conectados: capacidade e taxa de utilização dos equipamentos; portas que os interligam; capacidade e características físicas dos enlaces; informações de *spanning tree*; etc.
- Informações sobre cada equipamento: endereço IP, nome do equipamento, domínio VTP, número de série; número de módulos instalados; seriais dos módulos; memória instalada no supervisor; versão do sistema operacional instado no supervisor; etc.
- Informações sobre portas dos módulos: número de portas de cada módulo; nome das portas, capacidades; VLANs associadas, status da porta – conectada, desconectada, bloqueada, desativada. Caso a porta esteja conectada, informa o endereço MAC do equipamento conectado e, a partir do resultado, interage com outras entidades de rede (roteadores, servidores wins, servidores de autenticação, etc) e verifica o endereço IP, a sub-rede e o nome DNS / wins do equipamento conectado à porta, etc.

Como pode ser visto, o funcionamento do servidor ANI é essencial para o conjunto de aplicações CiscoWorks2000. A forma com que algumas dessas informações são obtidas não é

bem clara, como, por exemplo, a obtenção dos nomes wins das máquinas Windows conectadas. Algumas considerações são feitas na seção 3.5.

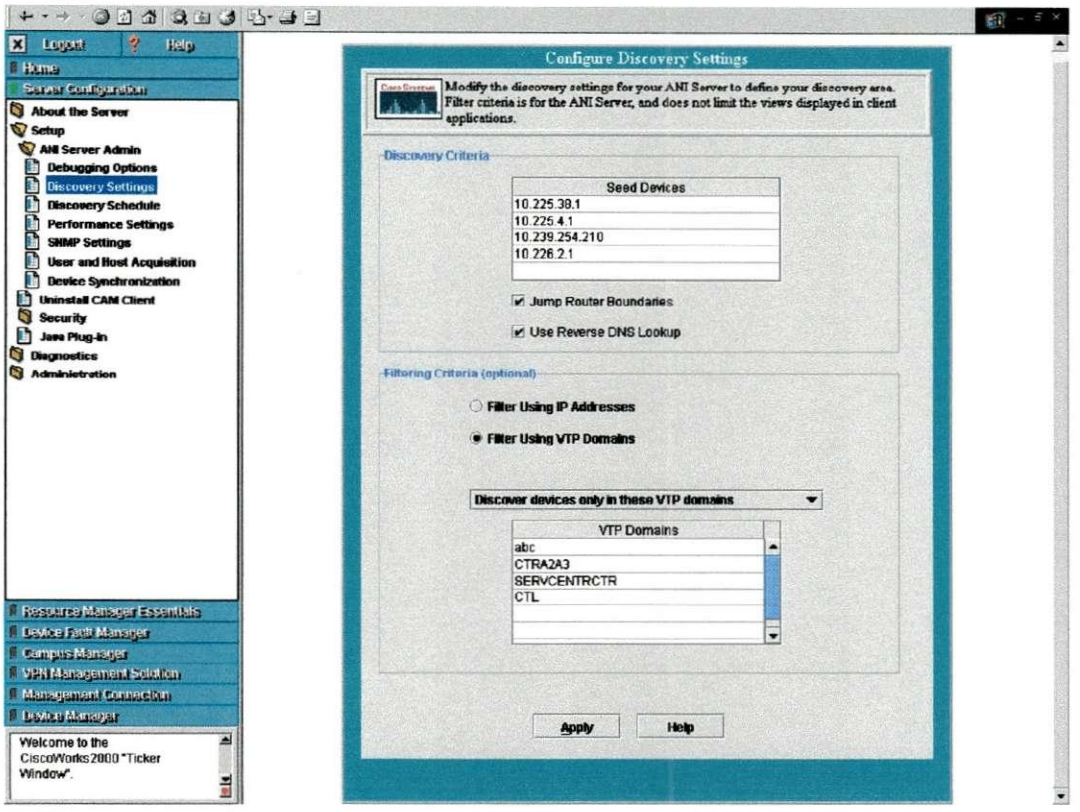


Figura 6: Interface de configuração do Servidor ANI.

Os parâmetros mais importantes na configuração do servidor ANI são mostrados na Figura 6. O ANI realiza a descoberta dos equipamentos de acordo com o domínio VTP. Ele inicia pelos comutadores do *backbone* que são configurados como servidores de domínio VTP (ver seção 2.2.2), cujos endereços IPs são devem ser indicados na mesma seqüência dos nomes de domínio VTP. Além dos domínios VTP do CTR, está incluso o domínio VTP CTL, referente ao Centro Técnico de Lardy, também supervisionado pelo SAEL CTR/CTL.

A outra interface de configuração é usada para a sincronização entre os dados do rastreamento do servidor ANI e o módulo *Resource Manager Essentials* (RME), que utiliza as informações coletadas para fornecer relatórios acerca das configurações e funcionamento dos equipamentos. O RME será estudado em mais detalhes na seção 3.2.

Outros parâmetros não menos importantes são as senhas SNMP dos equipamentos, que permite ao servidor ANI interrogar os comutadores e a programação dos horários em que o servidor ANI realiza a descoberta dos equipamentos. Normalmente, o servidor ANI é programado para realizar rastreamentos diários, às 08:00 hs e às 13:00 hs.

3.2. *Resource Manager Essentials*

O *Resource Manager Essentials* (RME) é um módulo do CiscoWorks2000 que integra um conjunto de aplicações que coletam de informações sobre falhas e estado de operação dos equipamentos da rede, descobertos pelo servidor ANI. O módulo RME também possui aplicações que permitem atualizar imagens dos sistemas operacionais de roteadores e *switches*, além de visualizar facilmente suas configurações. A Tabela 1 relaciona o conjunto de aplicações do módulo RME a suas principais funções.

Nome da Aplicação	Descrição
Availability	• Monitora o funcionamento e o tempo de resposta de um equipamento selecionado • Coleta dados de falhas e desempenho de roteadores e *switches*.
Change Audit	• Contém um log de todas as mudanças de configurações feitas nos equipamentos • Converte essas mudanças em mensagens SNMP (*traps*) e as envia para qualquer sistema de gerenciamento.
Configuration Management	• Mantém cópias atualizadas da configuração dos equipamentos • Edita arquivos de configuração e os envia para os respectivos equipamentos • Cria arquivos *templates* para mudanças de configuração.
Devices Views	• Seleciona um equipamento e exibe um conjunto de informações, tais como status de portas, etc.
Inventory	• Adiciona equipamentos manualmente para o gerenciamento • Gera relatórios e gráficos com informações sobre desempenho do *hardware* dos equipamentos gerenciados • Muda automaticamente as configurações SNMP dos equipamentos gerenciáveis • Instala suporte para novos equipamentos.
Software Management	• Analisa a necessidade de atualização dos softwares dos equipamentos • Programa, baixa, e monitora atualizações de softwares

	• Valida as imagens antes de enviá-las aos equipamentos.
Syslog Analysis	• Analisa e indica as possíveis causas de falhas nos equipamentos • Configura ações a serem realizadas automaticamente de acordo com mensagens de erro recebidas.

Tabela 1: Aplicações do módulo RME.

3.3. *Campus Manager*

O módulo *Campus Manager* (CM) é o mais interessante para a Renault em termos de aplicações na supervisão da rede. Ele traz consigo três aplicações:

- *Topology Services*
- *User Tracking*
- *Path Analysis*

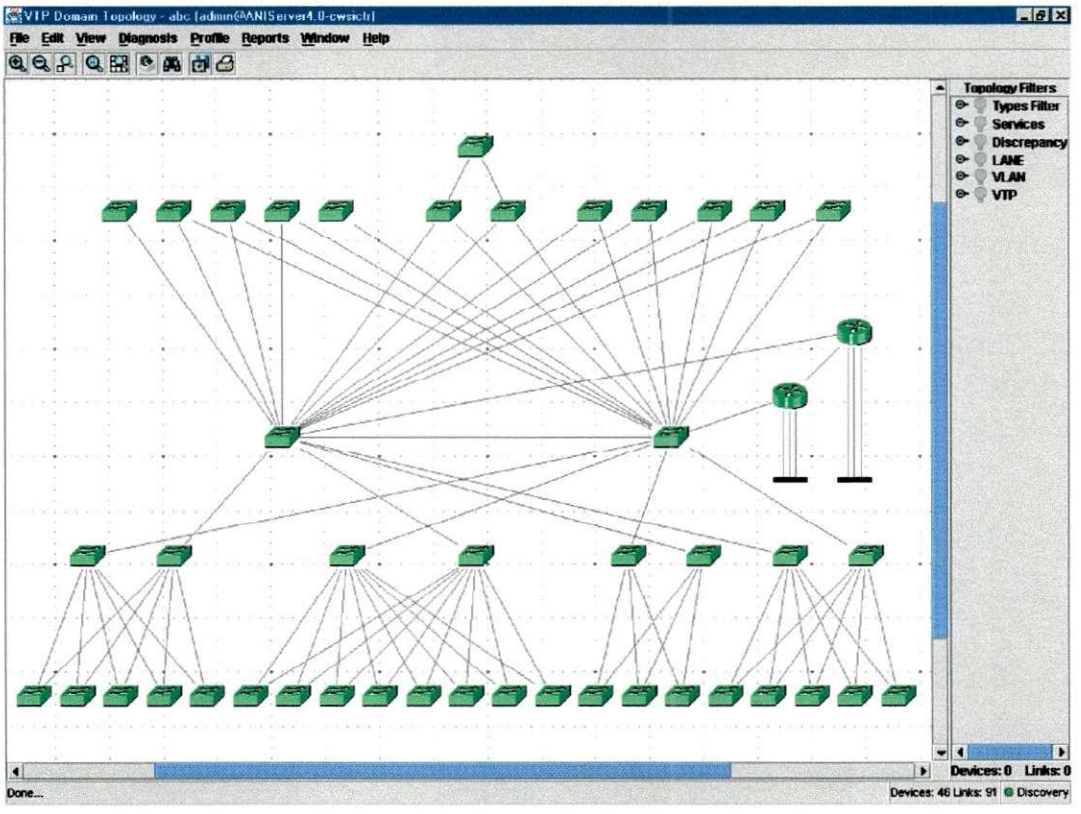


Figura 7: Topologia do domínio VTP abc gerada por *Topology Services*.

Topology Services utiliza as informações coletadas pelo servidor ANI para traçar a topologia nível 2 da rede, ilustrando através de gráficos os enlaces que interligam os *switches* entre si, como também as ligações entre os *switches* e roteadores. O *topology services* traça os

diagramas de rede por domínio VTP. É possível visualizar todos os domínios VTP juntos e como eles se relacionam. A Figura 7 ilustra os comutadores pertencentes ao domínio VTP abc (compare com a parte inferior da Figura 4).

O diagrama também pode indicar os nomes dos comutadores, bem como as portas a que os enlaces troncos (*trunk links*) estão conectados em cada comutador. O barramento logo abaixo dos roteadores de VLANs indica que outros domínios VTP estão conectados aos roteadores. Vale salientar que VLAN é um conceito associado ao nível 2 (MAC), enquanto que o roteamento IP é nível 3. Logo os roteadores não "entendem" o significado de VLANs.

Path Analysis é outra ferramenta gráfica, que traça os caminhos nível 2 e 3 entre dois elementos da rede. É o equivalente gráfico nível 2, do comando *traceroute* no Unix, o qual informa pelo console o caminho nível 3 entre a estação de origem e a de destino. A Figura 8 ilustra dois exemplos onde são traçadas rotas níveis 2 e 3 entre duas máquinas que, na Figura 8(a) estão na mesma sub-rede (uma sub-rede com 1024 endereços), enquanto que na Figura 8(b) as máquinas estão em sub-redes diferentes.

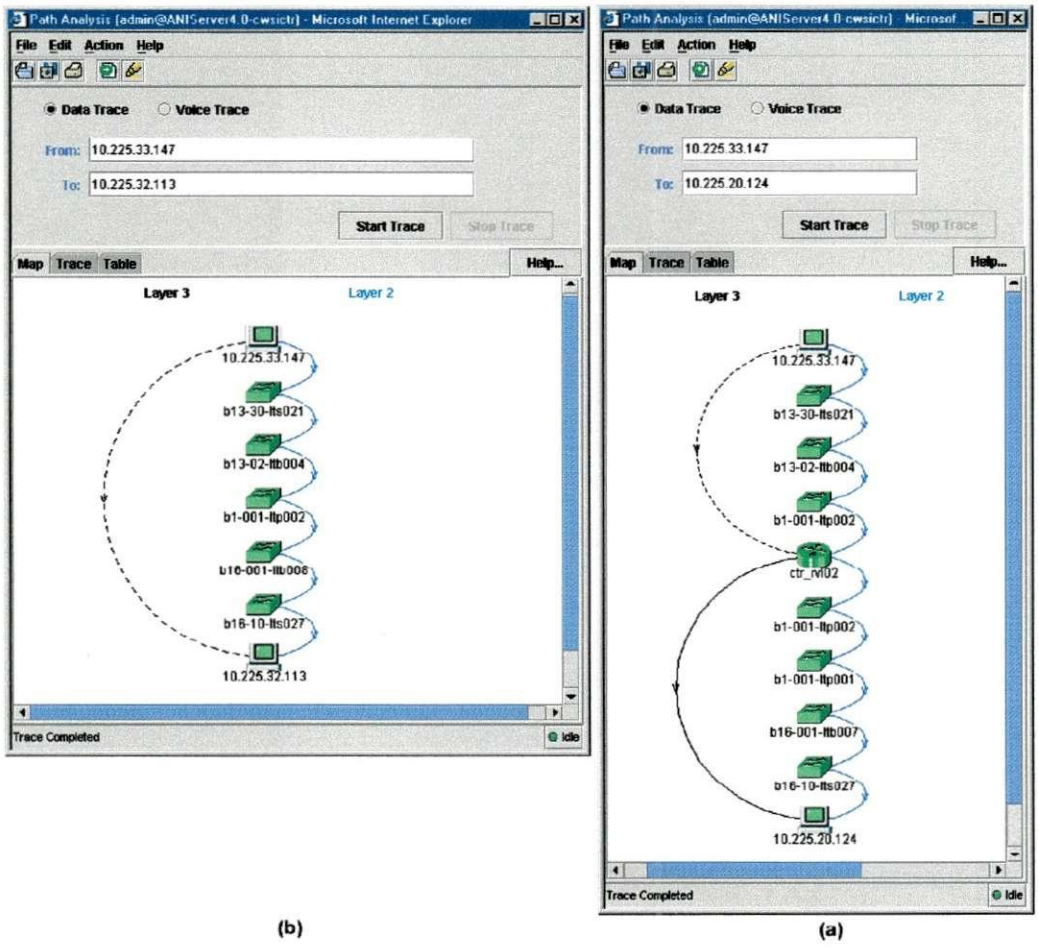


Figura 8: Caminhos nível 2 e 3 entre duas estações (a) na mesma sub-rede (b) em sub-redes diferentes.

A segunda aplicação *User Tracking* foi objeto de um estudo mais aprofundado e será descrita em seção à parte.

3.3.1. A aplicação *User Tracking*

A ferramenta *User Tracking* é utilizada para localizar usuários na rede. A partir das informações coletadas pelo servidor ANI e repassadas ao *Campus Manager*, é possível criar uma tabela com informações precisas da localização de cada máquina na rede. A aplicação *User Tracking* disponibiliza as seguintes informações:

- Endereço MAC do equipamento conectado a porta do comutador;
- O nome DNS / wins do equipamento, se disponível;
- O endereço IP;
- O nome do comutador ao qual a máquina está conectada;
- O endereço IP do comutador;
- O número da porta;
- O nome da porta;
- O domínio VTP ao qual o comutador pertence;
- A VLAN a qual a porta está associada;
- A última vez em que a máquina foi detectada pelo servidor ANI.

A Figura 9 ilustra a interface da aplicação. Note que, no exemplo, não foi possível detectar o endereço IP das máquinas. Isto porque elas podem está usando um outro protocolo para redes locais.

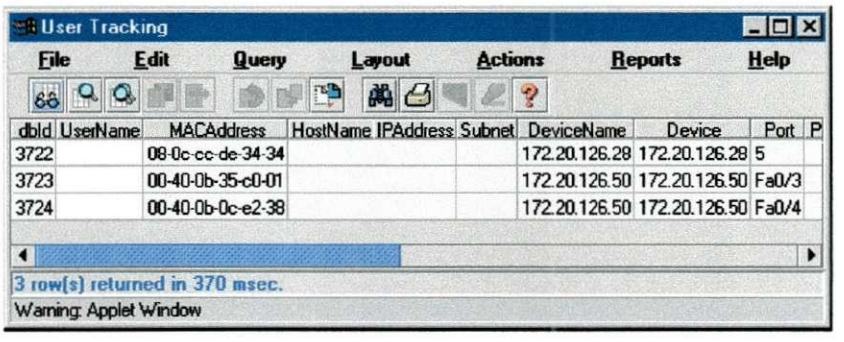


Figura 9: Interface da aplicação *User Tracking*.

Uma aplicação como essa representa um ganho de produtividade altíssimo para a equipe de suporte quando a rede a ser gerenciada possui em torno de 7000 máquinas. Se um usuário telefona informando que não consegue acessar a rede, simplesmente o técnico lhe pergunta o endereço IP da máquina. De posse do endereço o técnico descobre a qual comutador o usuário

está conectado e, utilizando outras ferramentas, verifica se a porta está ativada ou mesmo se há algum problema com o comutador.

A ferramenta *user tracking* é, sem dúvida, o que de melhor o conjunto de aplicações CiscoWorks2000 pode oferecer a equipe de suporte de rede do SAEL CTR/CTL, que complementa a estação de gerência HP *openview* e os inúmeros scripts *shell* desenvolvidos na própria Renault e descritos na seção 2.4.

3.4. *Device Manager*

O *Device Manager* (DM) é composto por uma única aplicação, *Cisco View*, que é uma ferramenta gráfica para a visualização e modificação de configuração em um determinado dispositivo. A Figura 10 ilustra o funcionamento de Cisco *View* para um *switch* catalyst 4006.

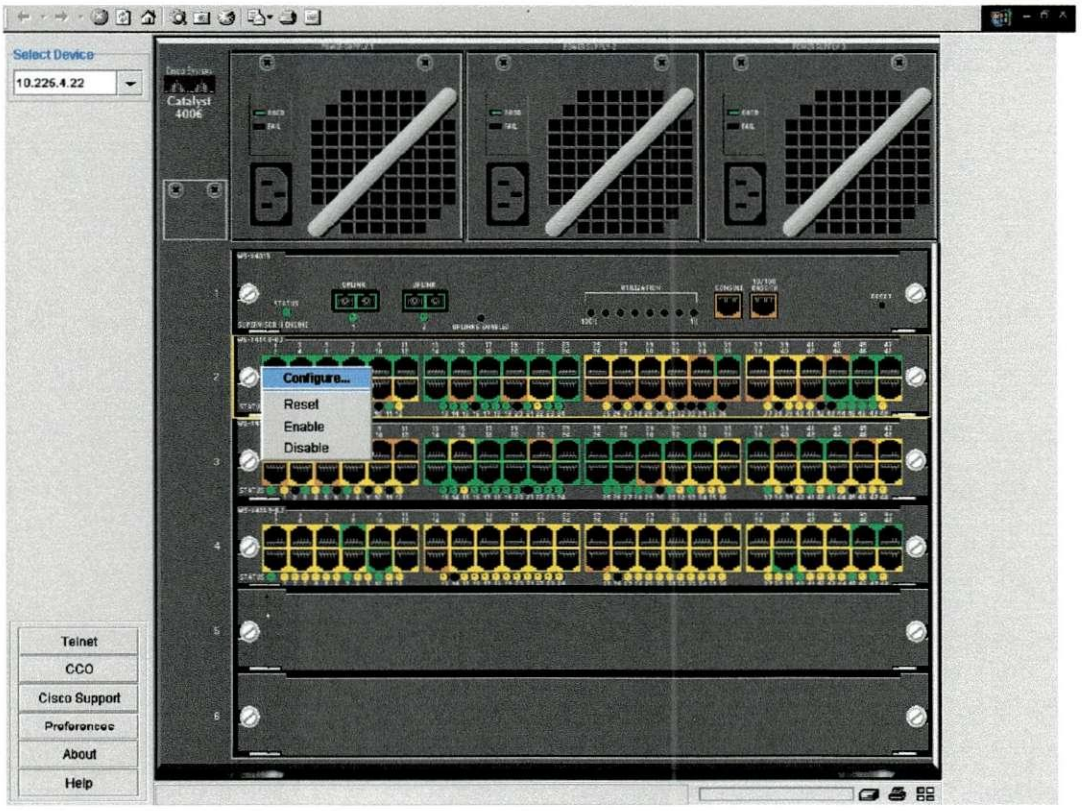


Figura 10: Cisco *View*.

Ao indicar o endereço ou nome do equipamento, cisco *view* inicia uma séria de chamadas SNMP para obter as informações sobre a configuração atual do equipamento. Entre as informações solicitadas estão o tipo, modelo e série do equipamento; o número de módulos que o equipamento possui (no catalyst da figura são quatro módulos); o status de cada porta de cada módulo e o status das fontes de alimentação do chassi. Para cada porta, um *link* na cor

verde indica que ela está conectada. Na cor amarela indica que a porta não está conectada e, na cor vermelha, que ela está desabilitada ou bloqueada.

Para configurar uma determinada porta para mudança de VLAN, por exemplo, basta apontar o mouse sobre a porta desejada e clicar com o botão direito, fazendo aparecer um menu semelhante ao da Figura. Então é só escolher a opção e realizar a configuração.

Além das portas, outros parâmetros podem ser configurados. Se o mouse estiver sobre o chassi em si e o botão direito for pressionado, uma janela se abrirá permitindo configurar parâmetros tais como mudança de endereço IP do chassi, de nome, de domínio VTP, de senhas SNMP, entre outras. Um menu no canto inferior esquerdo também é disponibilizado, onde é possível fazer um telnet para o chassi ou mesmo acionar o suporte Cisco.

Note que a interface utilizada pelo Cisco *view* é tão somente um navegador web. Os scripts que permitem interrogar os chassis, bem como desenhar suas interfaces, são feitos usando linguagem Java.

3.5. Avaliação do CiscoWorks2000

Esta seção apresenta um resumo da análise feita pelo estagiário sobre o produto CiscoWorks2000. Um relatório técnico detalhado foi elaborado e entregue a equipe SAEL CTR/CTL da Renault.

A utilização do CWSI como ferramenta de supervisão e administração de redes para uso nos SAELs foi desaconselhada, principalmente devido ao seu baixo desempenho e a falta de confiabilidade nos dados apresentados. Além disso, a maior parte dos recursos oferecidos pelo CiscoWorks2000 já tinha sido implementa pelas equipes dos SAELs (compare as seções 2.4 e 3) e as informações eram disponibilizadas de maneira simples, rápida e confiável.

O baixo desempenho (tempo de acesso muito altos, travamentos de janelas do navegador) do CiscoWorks2000 se deve ao fato da aplicação ser muito grande e complexa, projetada para "funcionar bem" em qualquer topologia de rede. Além disso, como essas aplicações foram quase totalmente programadas em Java, elas exigem um esforço computacional relativamente alto e um alto grau de alocação dos recursos do sistema.

As recomendações de hardware para a instalação do conjunto de aplicações CiscoWorks2000 são:

- Processador Pentium III 450 MHz ou superior;
- 512 MB de memória RAM;
- 8 GB de espaço em disco.

No entanto, o software foi instalado no SAEL CTR/CTL em uma estação DELL *Precision* com dois processadores Pentium III 600 MHz, 1 GB de memória RAM e HD SCSI de 20 GB. Mesmo assim, o software se apresentava lento principalmente ao ser acessado por clientes web a partir de outras máquinas.

A ferramenta apresentava também diversos erros de programação. Como exemplo, tome a ferramenta *Path Analysis*, do módulo *Campus Manager*. Devido a um erro de programação, a ferramenta não traçava o caminho nível 2 entre duas máquinas se, em algum dos enlaces tronco de interligação entre os comutadores, existisse um agrupamento de portas (*port channel* – ver 2.2.4). Isto impossibilitava a obtenção do caminho nível 2 entre máquinas dos domínios VTP CTRA2A3 e abc, pois a interligação dos roteadores de VLANs com os comutadores do núcleo da rede pertencentes ao domínio CTRA2A3, é feita usando 14 enlaces de 1 Gbps agrupados dois a dois (veja Figura 4).

As ferramentas do módulo RME já tinham sido quase totalmente implementas em scripts *shell*, que disponibiliza sempre informações atualizadas e confiáveis sobre os equipamentos. O Cisco *view* poderia ser uma de configuração interessante, devido a sua interface amigável. O problema é o tempo necessário para obter a imagem do comutador (em média 20 segundos, dependendo do computador) e, o mais importante, não é possível limitar os parâmetros que podem ser modificados. Logo seu uso não é recomendado às equipes níveis 1 e 2.

A única aplicação que o CiscoWorks2000 disponibilizava que ainda não tinha sido implementada pelas equipes SAEL CTR/CTL era a ferramenta *User Tracking*, do módulo *Campus Manager*. Que foi alvo de um estudo mais aprofundado.

3.5.1. Análise da ferramenta *User Tracking do CWSI.*

Não foi difícil perceber que a ferramenta *User Tracking*, descrita na seção 3.3.1, era de fundamental importância para as equipes de suporte. Quando a equipe de suporte recebe uma solicitação de conserto é porque, logicamente, a conexão do usuário não funciona. Assim, ferramentas em tempo real não podem ser usadas para localizar o comutador ao qual a estação está conectada.

Porém, eram muitas as reclamações que chegavam ao chefe do setor, e tutor no presente estágio, com relação a tal ferramenta do CiscoWorks2000. Dentre os problemas mais comuns estavam duplicatas de endereços IP, de endereços MAC, de porta dos comutadores e, em alguns casos, falta de correlação em todas as informações repassadas. Em observações feitas pelo estagiário, na base de dados *user tracking* que continha cerca de 8.500 entradas, existiam

por volta de 2000 linhas com informações incorretas. Isto representa quase 27% do total de dados. Situações descritas no exemplo que se segue são fáceis de encontrar.

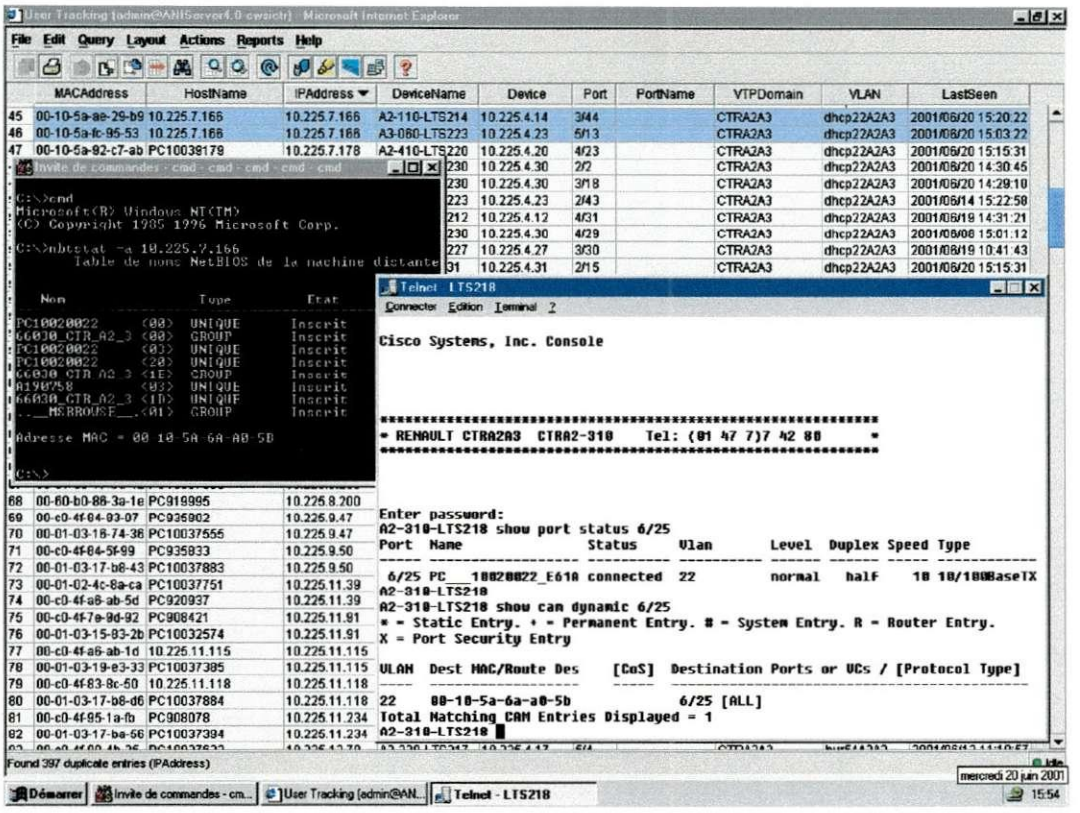


Figura 11: Avaliação da ferramenta *user tracking*.

A Figura 11 é uma impressão da tela da estação de gerenciamento CiscoWorks2000 rodando a aplicação *user tracking*. As entradas da tabela foram obtidas através de uma triagem por duplicatas de endereços IP. Como pode ser visto na barra de status da janela, foram encontrados 397 entradas com endereços IPs duplicatos. Tomemos as duas primeiras linhas em destaque na tabela. A primeira falha é a própria duplicação de endereços IPs.

Uma situação foi analisada um pouco mais a fundo. De posse do endereço IP em questão, 10.225.7.166, o comando *nbtstat –a 10.225.7.166* foi usado em uma janela DOS para obtermos as informações netbios na máquina em questão. Para máquinas rodando Windows, o comando *nbtstat* retorna informações tais como: nome wins da máquina, nome do usuário atual da máquina, servidor de autenticação ao qual o usuário está conectado, se a máquina é *master browser* da rede e, o mais importante aqui, o endereço MAC da interface de rede da máquina. Para a surpresa, o endereço MAC da interface de rede da estação de trabalho em questão é 00-10-5A-6A-A0-5B, que difere dos dois outros relacionados na aplicação *user tracking* para o endereço IP em questão.

Um telnet sobre o *switch* A2-310-LTS218 mostra, através do comando *show port status 6/25*, que o a interface que possui endereço MAC correspondente ao IP 10.225.7.166 está conectada sobre a porta 25 do módulo 6 desse comutador e não sobre a porta 3/44 do A2-110-LTS214 nem tal pouco sobre a porta 5/13 do comutador A2-060-LTS223, como são mostradas nas duas linhas corresponde ao endereço IP em questão.

As informações repassadas pela ferramenta, nesse e em muitos outros casos, atrapalham e tomam tempo dos técnicos do grau 2, que nesses casos recorrem aos dois técnicos de grau 3 (e aos estagiários!) e esses tentam encontrar a porta a qual está ou estava conectada a máquina entre mais de 8000 possíveis.

A situação era mais grave para máquinas (na maioria, *notebooks*) que estavam em duas sub-redes de 1024 endereços cada, as quais possuíam IPs dinâmicos distribuídos por servidores DHCP. Por amostragem ao longo de uma semana, se verificou algum **erro** em 48% por cento nas linhas das tabelas referentes a essas sub-redes (somente 62% de entradas corretas).

Num primeiro momento se pensou que isto era devido a erros de configuração no software, o que não se verificou. Sucessivas ligações foram feitas ao suporte da Cisco, que repassava a ligação à equipe que desenvolveu o produto. Esta se limitava a perguntar qual a versão do Internet Explorer que estava instalada na máquina e a aconselhar sua reinstalação.

Em seguida, foi sugerido o desenvolvimento de um programa que interagisse diretamente no banco de dados onde o CiscoWorks2000 armazenava as informações da referida aplicação para tentar corrigir erros. O problema foi que não se encontravam critérios que levassem a eliminação dos diversos tipos de duplicatas, nem tão pouco critérios que possibilitasses a correção dos dados, já que não se tinha certeza de quais dados estavam corretos ou não.

A solução proposta pelo estagiário, discutida e aceita pelos integrantes da equipe de suporte de rede do SAEL CTR/CTL, foi a criação de um software batizado de *CTR User Tracking* e que tivesse as mesmas características do CiscoWorks2000 *user tracking*, mas com um desempenho melhor.

4. O utilitário CTR *User Tracking*

Nesta parte do relatório será descrito o algoritmo utilizado no desenvolvimento da ferramenta CTR *user tracking*, proposta pelo estagiário como uma alternativa à aplicação *user tracking*, pertencente ao módulo *campus manager* do CiscoWorks2000.

4.1. Descrição geral do programa

O programa foi desenvolvido em linguagem PERL. Ela foi escolhida pela facilidade com que manipula arquivos texto e seqüências de caracteres (*strings*). O programa utiliza diversos recursos da rede para a coleta de informações que agrupadas, trazem as seguintes informações sobre cada uma das estações de trabalho conectadas aos *switches* da rede:

- O endereço MAC da interface;
- O endereço IP da máquina;
- O número da VLAN associada à porta do comutador;
- O número e o nome da porta;
- O endereço IP, nome e domínio VTP do chassi;
- A data e hora que a máquina foi "vista" conectada ao comutador.

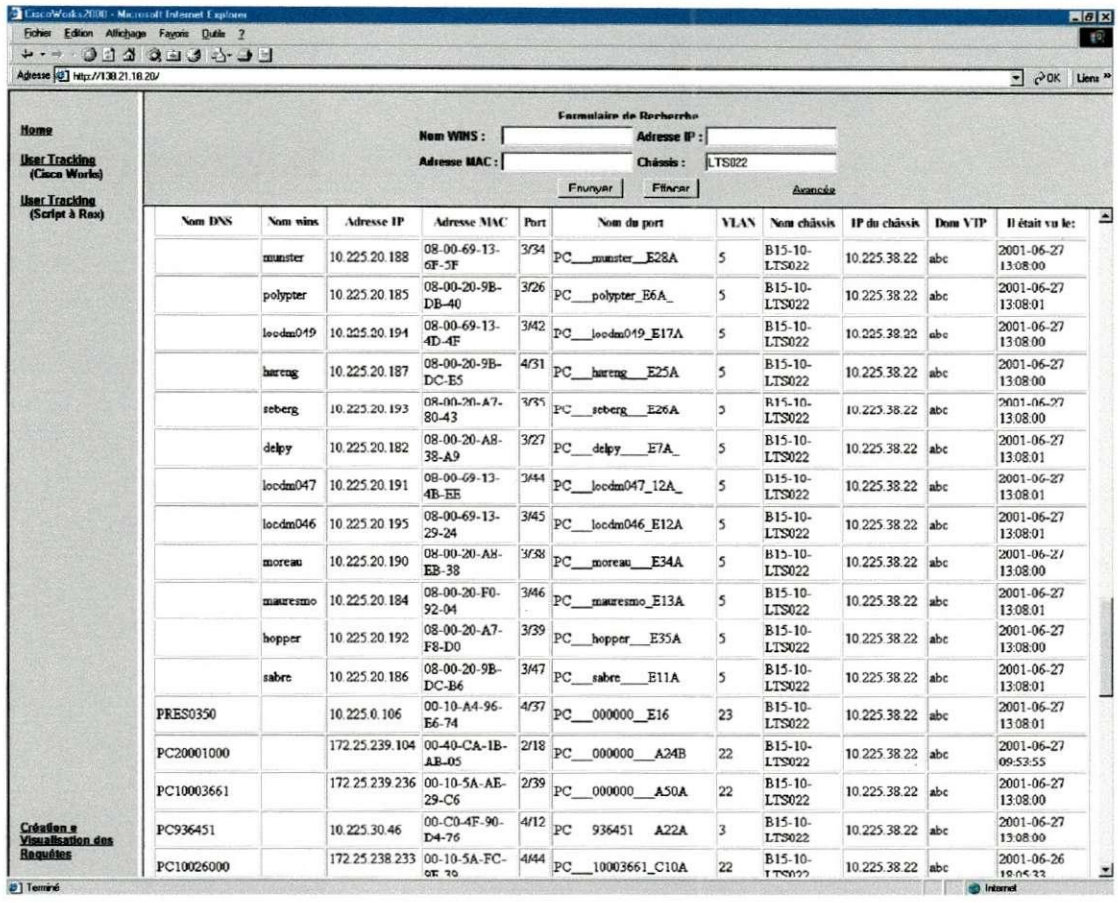
Essas informações eram inseridas numa tabela chamada *ctrusertracking,* de um banco de dados MySQL chamado de *CTRExploitation.* Além dessa tabela, foram criadas mais duas tabelas: *tablearp* e *chassis*. A tabela *tablearp* armazena pares de endereços IP/MAC com os correspondentes nomes DNS e/ou wins, oriundos das tabelas ARP dos roteadores de VLAN e dos servidores DNS e wins. A tabela *chassis* contém a lista de todos os *switches* que devem ser interrogados, bem como o modelo de cada um.

A pesquisa aos dados era realizada por intermédio de um navegador *web* qualquer. Para isso, foram desenvolvidos também scripts PHP, usados para acessar o banco de dados via um *driver* ODBC. A Figura 12 ilustra a interface *web* do programa. Neste caso, foi feita uma pesquisa das máquinas conectadas ao *switch* B15-10-LTS022. Serão discutidos aqui somente os programas em Perl.

Para obter os dados, o programa realiza o conjunto de ações descritas abaixo e analisadas com mais detalhes mais adiantes:

- Interroga o servidor Wins e DNS da rede;
- Emite mensagens *ping* a todas as máquinas da rede;
- Interroga cada um dos roteadores para obter as tabelas ARP;
- Atualiza a tabela *tablearp*;

- Interroga cada um dos *switches* presentes na tabela *chassis:*
  - Emite mensagens *ping* enquanto interroga os comutadores;
  - Atualiza a tabela *ctrusertracking;*
- Retira inconsistências presentes na tabela *ctrusertracking*



Nom DNS	Nom wins	Adresse IP	Adresse MAC	Port	Nom du port	VLAN	Nom châssis	IP du châssis	Dom VTP	Il était vu le:
	munster	10.225.20.188	08-00-69-13-6F-5F	3/34	PC___munster__E28A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	polypter	10.225.20.185	08-00-20-9B-DB-40	3/26	PC___polypter_E6A_	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
	locdm049	10.225.20.194	08-00-69-13-4D-4F	3/42	PC___locdm049_E17A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	hareng	10.225.20.187	08-00-20-9B-DC-E5	4/31	PC___hareng___E25A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	seberg	10.225.20.193	08-00-20-A7-80-43	3/35	PC___seberg___E26A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	delpy	10.225.20.182	08-00-20-A8-38-A9	3/27	PC___delpy___E7A_	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
	locdm047	10.225.20.191	08-00-69-13-4B-EE	3/44	PC___locdm047_12A_	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
	locdm046	10.225.20.195	08-00-69-13-29-24	3/45	PC___locdm046_E12A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
	moreau	10.225.20.190	08-00-20-A8-EB-38	3/58	PC___moreau___E34A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	mauresmo	10.225.20.184	08-00-20-F0-92-04	3/46	PC___mauresmo_E13A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
	hopper	10.225.20.192	08-00-20-A7-F8-D0	3/39	PC___hopper___E35A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
	sabre	10.225.20.186	08-00-20-9B-DC-B6	3/47	PC___sabre___E11A	5	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
PRES0350		10.225.0.106	00-10-A4-96-E6-74	4/37	PC___000000__E16	23	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:01
PC20001000		172.25.239.104	00-40-CA-1B-AB-05	2/18	PC___000000___A24B	22	B15-10-LTS022	10.225.38.22	abc	2001-06-27 09:53:55
PC10003661		172.25.239.236	00-10-5A-AE-29-C6	2/39	PC___000000___A50A	22	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
PC936451		10.225.30.46	00-C0-4F-90-D4-76	4/12	PC 936451 A22A	3	B15-10-LTS022	10.225.38.22	abc	2001-06-27 13:08:00
PC10026000		172.25.238.233	00-10-5A-FC-9E-39	4/44	PC___10003661_C10A	22	B15-10-LTS022	10.225.38.22	abc	2001-06-26 18:05:33

Figura 12: Interface para consulta do CTR *user tracking*.

4.2. Dificuldades de implementação

Antes de descrever detalhadamente cada ação do programa, é interessante ressaltar alguns fatores que afetaram o projeto do programa.

O primeiro foi o tempo necessário para interrogar um *switch* utilizando SNMP. Cada chamada SNMP demora entre 3 e 15 segundos, dependendo da quantidade de dados retornada pelo comutador. Para cada comutador, eram necessárias, no mínimo 8 requisições SNMP (esse número varia de acordo com a quantidade de VLANs atribuídas as portas do *switch*). Considerando que uma média de 10 segundos por requisição e 80 comutadores, teríamos que o programa necessitaria de, no mínimo, 1h46mim para realizar a tarefa, sem contar tempo de processamento. Esse tempo é muito alto, considerando que o servidor ANI realiza sua detecção, em média, em 1h30mim.

A solução encontrada para esse problema foi o uso de *threads*, permitindo que se interrogassem vários *switches* ao mesmo tempo. Testes mostraram que o desempenho do sistema era máximo quando 10 *switches* eram interrogados simultaneamente. Esse recurso permitiu diminuir para 13 minutos o tempo de execução do programa. Em contrapartida, foi necessário programar rotinas para controle de processos filhos lançados, como será visto mais adiante.

Outro problema encontrado foi com relação aos endereços físicos (MAC) das máquinas, que eram obtidos a partir dos *switches*. Um dos parâmetros gerais na configuração dos mesmos é o tempo de vida do endereço MAC, que se pode configurar entre 1 e 5 minutos. Isto significa que se a estação não enviar ou receber nenhum pacote no intervalo referente ao tempo de vida do endereço, simplesmente o comutador apaga da memória o endereço MAC da interface de rede conectada. Após isso, para o comutador, tudo se passa como se não existisse nenhuma interface de rede conectada àquela porta. Como o período de realização das requisições SNMP durava cerca de 15 minutos, era necessário assegurar que os comutadores teriam o endereço MAC das estações a eles conectadas. Para se ter essa garantia, um processo filho é lançado juntamente com o programa principal. Esse processo ler os endereços IPs contidos na tabela *tablearp* e, para cada endereço, envia um mensagem *ping* sem confirmação, com apenas um pacote de 32 bytes. A meta era emitir cerca de 9.000 mensagens *ping* em intervalos menores que 5 minutos (uma mensagem a cada 30 ms), o que foi conseguido graças a um controle de processos que permitia o envio simultâneo de 30 mensagens.

Outro fator que exigiu cuidados especiais foi à obtenção dos dados das tabelas ARP dos roteadores de VLANS. Por incrível que pareça, havia duplicatas de endereços IP e MAC na tabela. A solução encontrada para isso era a obtenção de outro parâmetro fornecido pelo roteador, que é a idade (*age*) de cada entrada da tabela. Esse era o tempo, em minutos, que o último pacote tinha sido roteado para o endereço físico correspondente. Logo uma análise na idade das entradas sempre definia qual era e correta.

4.3. Fluxograma do programa

O fluxograma do programa é mostrado em detalhes na Figura 13. O programa começa por interrogar os servidores DNS e wins da rede, onde são usados os comandos externos *nslookup* e *winsdump*, respectivamente. O resultado são dois arquivos texto que possuem linhas como as mostradas abaixo:

Para os dados DNS:

```
> Default Server:  hop.ctr.renault.fr
Address:  138.21.5.242
> [hop.ctr.renault.fr]
renault.fr.                    NS      server = kitten.pdj.renault.fr
kitten.pdj                     A       138.21.10.172
renault.fr.                    NS      server = denys.ctr.renault.fr
denys.ctr                      A       10.225.16.1
cra                            NS      server = kitten.pdj.renault.fr
...
```

Para os dados do servidor Wins:

```
138.21.40.130,"PC10002906□",3,17,0,0,8727191,0,994234165,1,10.226.18.30,
138.21.40.130,"PC10002906",0,17,0,0,8727192,0,994234165,1,10.226.18.30,
138.21.40.130,"PC10002906",20,17,0,0,8727193,0,994234165,1,10.226.18.30,
138.21.40.130,"PC923013",3,17,0,0,8728274,0,994234165,1,172.25.50.189,
138.21.40.130,"PC923013",0,17,0,0,8728275,0,994234165,1,172.25.50.189,
...
```

Desses arquivos eram extraídos os nomes DNS e Wins das máquinas, associados com os respectivos endereços IP.

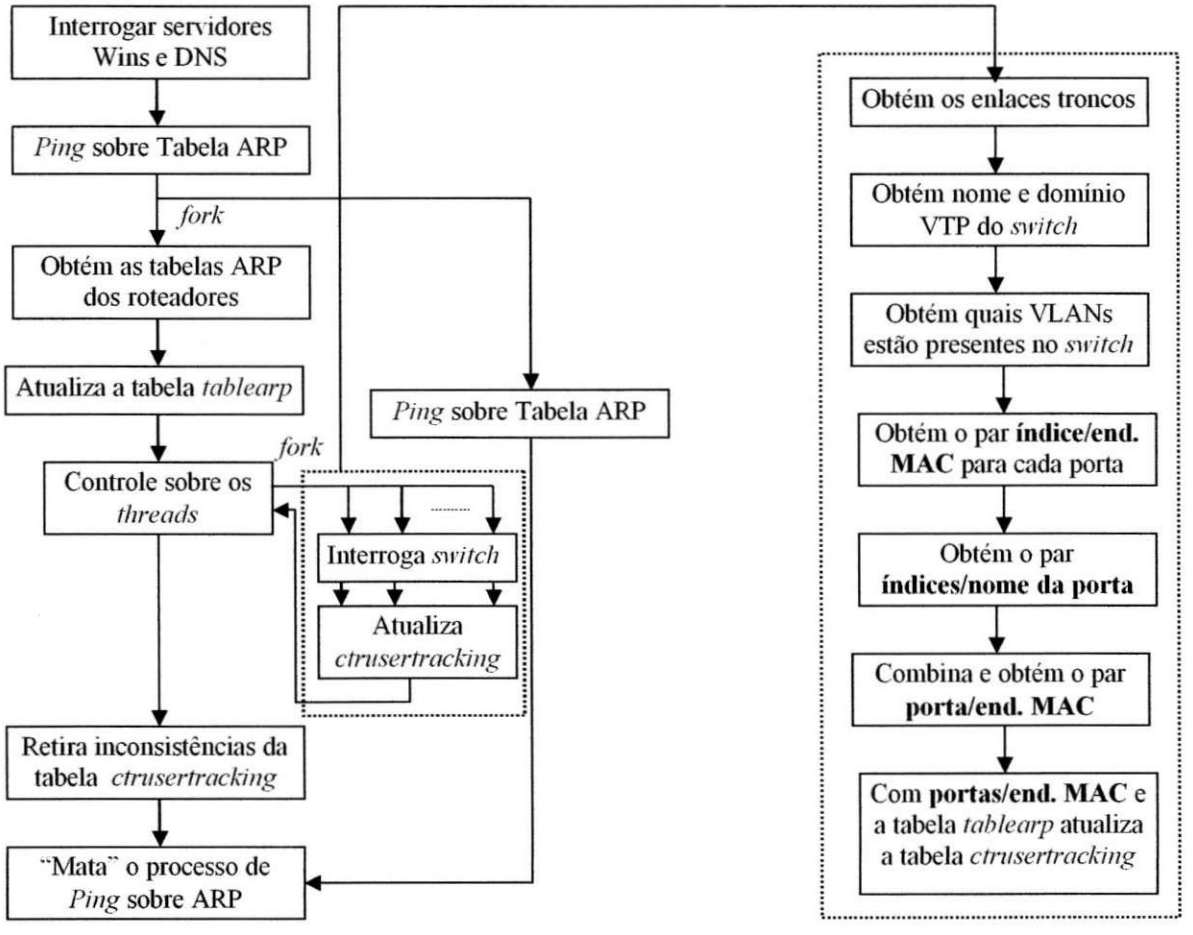


Figura 13: Fluxograma do programa CTR *user tracking*.

Em seguida, é aberta uma conexão com a tabela *tablearp* e, para cada endereço IP contido na tabela, é feito um *ping* sem confirmação de recebimento. Isto é feito antes de recuperar a tabela ARP dos roteadores, para se obter melhor consistência dos dados.

Um *shell* remoto é então enviado para todos os roteadores de VLANS. O resultado novamente é um conjunto de arquivos texto, com o formato mostrado abaixo:

```
Protocol     Address     Age (min)  Hardware Addr   Type     Interface
Internet  10.226.24.240      1       0050.04df.dbb9  ARPA   Port-channel2.98
Internet  138.21.189.34      2       0800.8611.da3b  ARPA   Port-channel2.98
Internet  10.226.8.224       5       0001.030f.75af  ARPA   Port-channel2.98
Internet  172.26.185.15      7       0010.8301.d0b6  ARPA   Port-channel2.98
...
```

Desses arquivos são extraídos o endereço IP, o endereço MAC e o tempo de vida de cada entrada. O próximo passo é atualizar as informações DNS, wins e os arquivos coletados dos roteadores para atualizar a tabele *tablearp*, que possui os seguintes argumentos:

Tabela *tablearp*	
Argumento (coluna)	**Descrição**
Id	Identificador único
IP	Endereço IP da máquina
MAC	O endereço físico (MAC) correspondente
DNS	O nome DNS correspondente ao endereço IP
Wins	O nome wins para máquinas Windows.
Vu	Data e hora da última atualização

Atualizada a tabela *tablearp*, as equivalências IP/MAC/nome DNS/nome wins, são conhecidas. O próximo passo é encontrar as correspondências endereço MAC/porta/VLAN, para todos os *switches* da rede. Paralelamente, é lançado um processo filho para enviar mensagens *ping* a todos os endereços IP presentes na tabela *tablearp*, por razões descritas em na seção 4.2. Ele deverá ser repetido continuamente até que o final do programa.

Como explicado na seção 4.2, o uso de *threads* é necessário no momento de interrogar via SNMP os comutadores. Assim, um controle é feito de forma a manter sempre 10 *switches* sendo interrogados de forma simultânea. Para começar a lançar os *threads*, o programa acessa o banco de dados e procura pela tabela *chassis*, que possui a seguinte estrutura:

Tabela *chassis*	
Argumento (coluna)	**Descrição**
Chassis	Endereço IP do *switch*
Modele	Modelo do *switch* (4000, 5000, ...)

e para cada *switch* são realizados os procedimentos descritos abaixo.

A primeira requisição SNMP é para saber quais são as portas configuradas como enlaces troncos (*trunks*). Essa informação é fundamental, pois o tráfego de todo o *switch* é escoado por essas portas. Isto faz com que elas tenham inúmeros endereços MAC associados. As chamadas SNMP são feitas usando comandos externos (*shell*), e possuem um formato semelhante ao mostrado abaixo:

```
snmpwalk -M arquivo_mibs endereço_do_switch senha_SNMP oid_mib
```

onde o parâmetro *"oid_mib"* representa o "endereço" onde as informações de encontram no banco de dados SNMP (MIB) dos equipamentos. No caso de informações sobre os enlaces troncos, o *oid* da MIB é .1.3.6.1.4.1.9.5.1.9.3.1.8. O resultado agora é um seqüência de linhas que indicam que indicam as portas configuradas como *trunk*, com o seguinte formato:

```
enterprises.9.5.1.9.3.1.8.1.1 = 1
enterprises.9.5.1.9.3.1.8.1.2 = 1
enterprises.9.5.1.9.3.1.8.2.1 = 2
enterprises.9.5.1.9.3.1.8.2.2 = 2
enterprises.9.5.1.9.3.1.8.2.3 = 2
enterprises.9.5.1.9.3.1.8.2.4 = 2
...
```

Os números em negrito representam as portas do *switch* em questão, onde **x.y** quer dizer porta **y** do módulo **x**. Somente as portas que possuem 1 como valor são enlaces *trunk*. Esses dados são for formatados e colocados em variáveis do tipo matriz.

Segue-se então uma série de chamadas SNMP e tratamento dos dados recebidos, conforme descrito na parte direita do algoritmo da Figura 13. Ao final, seguintes informações são obtidas para cada um das portas do comutador em questão:

- A matriz associativa $portas_mac{número_da_porta_} = endereço_MAC
- A matriz associativa $nome_portas {número_da_porta_} = nome_da_porta
- A matriz associativa $vlan_portas{número_da_porta_} = número_da_vlan
- Duas outras variáveis, $nome_do_switch e $dominio_vtp

Para cada valor da matriz associativa @portas_mac (ou seja, o endereço MAC da interface conectada a porta indicada pelo índice da variável), é feita uma consulta na tabela *tablearp*.

De posse desses dados é feita, finalmente, a atualização/inserção na tabela *ctrusertracking*, que possui a seguinte estrutura:

Tabela *ctrusertracking*	
Argumento (coluna)	**Descrição**
Id	Identificador único
AdresseIP	Endereço IP da máquina
AdresseMAC	Endereço físico (MAC) correspondente
NomWINS	Nome wins (para máquinas Windows)
NomDNS	Nome DNS
Port	Número da porta onde a interface está conectada
PortNom	Nome da porta
Vlan	VLAN assoada a porta
ChassisNom	Nome do *switch*
DomaineVTP	Domínio VTP do *switch*
ChassisIP	Endereço IP do *switch*
Vu	Data e hora da inserção/atualização.

Esta operação se repete para todos os *switch* presentes na tabela *chassis*. A etapa seguinte é eliminar possíveis incoerências existentes na recém atualizada tabela *ctrusertracking*. É fácil notar que o programa não gera duplicatas de endereços MAC, pois no momento da atualização/inserção descrita acima, se faz uma busca pelo Endereço MAC. Caso ele já exista os dados são atualizados, caso uma nova interface é encontrada um novo registro é criado. As duplicatas de Endereços IP podem existir, mas elas são facilmente eliminadas simplesmente excluindo da tabela o registro que for mais antigo. A última tarefa a ser realização é a destruição do processo filho responsável pelo envio das mensagens *ping*.

Teoricamente, os dados contidos na tabela *ctrusertracking* são totalmente coerentes com a realidade atual e passada da rede. Porém, devido a pequenos detalhes, algumas falhas também foram identificadas no programa, as quais descritas na próxima seção.

4.4. Avaliação, limitações do programa e trabalhos futuros

O desenvolvimento do programa teve fim quando restavam somente duas semanas para o término do estágio. Contudo, a interface *web* do programa CTR *user tracking* foi prontamente disponibilizada às equipes de suporte SAEL CTR/CTL e o que se seguiu foi um processo de

avaliação, onde os técnicos eram instruídos a compararem a consistência dos dados fornecidos pelas duas ferramentas. O resultado não poderia ser diferente: enquanto que o utilitário *user tracking* do CiscoWorks2000 apresentava duplicatas de endereços e mesmo dados totalmente descorrelacionados, o programa CTR *user tracking* trazia, em 98,5% dos acessos, a informação correta. O erro de 1,5% é atribuído à máquinas que estavam se uma sub-rede e, no intervalo entre as detecções, é conectado a outra sub-rede ou, no caso de máquinas DHCP, recebem outro endereço IP.

Um percentual parecido com esse (98%) foi obtido pelo estagiário por amostragem. Quando são consideradas somente as portas dos comutadores associadas a VLANs DHCP o percentual baixou para 95,4%. Esses números são consideravelmente melhores do que os obtidos pelo CiscoWorks2000 (ver seção 3.5.1). Duas limitações foram observadas durante as semanas de avaliação.

A primeira ocorre quando **uma** máquina possui **duas** interfaces de rede com o **mesmo** endereço MAC. Logicamente, as interfaces não estão na mesma sub-rede. Isto é possível em estações SUN que utilizam uma das interfaces para prover serviços e a outra somente para administração. Dessa forma é possível limitar as conexões pela interface que provê o serviço, enquanto que outra interface, de gerenciamento, faz parte de uma sub-rede de gerenciamento que pode não possuir rotas de entrada nos roteadores (por questões de segurança). A solução para esse caso é retirar da tabela da tabela de rotas do roteador a relação de sub-redes e suas máscaras associadas a cada endereço IP da tabela ARP. Com isso, é possível identificar o endereço IP que está associado ao endereço MAC presente na sub-rede e assim evitar sobreposição de endereço IP.

A outra limitação é com respeito a *switches* que não utilizam portas configuradas como troco (*trunk*) para escoar seu tráfego. Isso acontece, por exemplo, quando todas as portas do *switch* pertencem a uma mesma VLAN. Dessa forma, qualquer porta do *switch* pode ser usada para escoar seu tráfego, desde que a porta do outro esteja na mesma VLAN. O que acontece é que como nenhum tronco é encontrado, o programa procura por endereços MAC em todas as portas do *switch*. Quando chega a vez da porta de interligação, o script vê uma infinidade de endereço MAC de máquinas que já se comunicaram com estações conectadas ao *switch* em questão. A solução mais fácil para isso é aumentar um pouco o volume do tráfego no enlace e configurar a porta *trunk* (o volume de tráfego aumenta, pois o *switch* insere um cabeçalho em cada pacote trafega num enlace *trunk*, para identificar o domínio VTP e a VLAN a qual o pacote pertence). A utilização de concentradores (*hubs*) ligados a portas de *switches* produz o mesmo efeito, só que em proporções menores.

Por fim, futuras modificações na estrutura do programa foram sugeridas pelo estagiário a fim de fazer com que o mesmo se torne independente do modelo do *switch* ou mesmo do fabricante. Isto é possível, pois as informações essenciais para o programa são extraídas dos *switches* via SNMP. Algumas MIBs SNMP dos equipamentos fornecem as informações de forma padronizada, de forma que uma mesma informação é localizada pelo mesmo *oid* em equipamentos de diferentes fabricantes.

Uma motivação para tal projeto surge quando as fábricas Renault espalhadas pela Europa são consideradas. Nelas, os equipamentos de redes predominantes são fabricados pela Lucent Technology.

5. Considerações finais

O estágio realizado no Centro Técnico Renault de Ruiel Mailmaison foi considerado pelo estagiário como de fundamental importância para a sua formação pessoal e principalmente profissional.

Pessoal porque ele teve a oportunidade de se relacionar com pessoas de culturas diferentes e, na medida do possível, absorver para si alguns desses elementos.

Profissional porque as tarefas exigiram uma gama de conhecimentos sobre arquiteturas e serviços de rede de computadores, permitiu ao estagiário se familiarizar com a topologia de redes coorporativas de grande porte e ainda desenvolver uma ferramenta de gerência de redes baseada em SNMP, que exigia interações com diversas entidades de rede, como servidores DNS e wins, roteadores e *switches*. Além disso, se teve a oportunidade de conhecer a estrutura e métodos de trabalho de uma grande empresa líder de mercado nos setores que atua.

Os conhecimentos adquiridos ao longo do curso foram de fundamental importância para o acompanhamento das tarefas, sobretudo a principal característica inerente à formação de engenheiros: a capacidade de identificar, e resolver problemas.

Contribuíram para o sucesso na realização das tarefas, os técnicos altamente qualificados Tozé DIAS e Daniel LECOUELLE e, fundamentalmente, o tutor do estágio, François COUTAN, que apresentava um alto nível de conhecimento sobre os assuntos relacionados ao estágio e estava sempre a disposição para discussões e esclarecimentos de dúvidas do estagiário.

6. Referências

[1] LEINWAND, Allan. *Cisco Router Configuration*. 2nd edition. Cisco Press. 2000.

[2] MAURO, Dougas; SCHMIDT, Kevin. *Essential SNMP*. 1st edition. Sebastopol: O'Reilly & Associates, Inc. 1999.

[3] SCHWART, R.L. *Learning Perl*. 2nd edition. New York: O'Reilly & Associates, Inc. 1997.

[4] Anônimo. *Configuring SNMP*. Cisco Systems. 1999.

[5] Anônimo. *Configuring Spanning Tree*. Cisco Systems. 2000.

[6] Anônimo. *Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports.* Cisco Systems. 2000.

[7] Anônimo. *Getting Start with CiscoWorks2000 Server.* Cisco Systems. 2000.

[8] Anônimo. *MySQL Reference Manual.* MySQL.org, 2000.

[9] Anônimo. *PHP Manual*. PHP.org. *2001.*

[10] Anônimo. *Understanding and Configuring VLANs.* Cisco Systems. 2000.

[11] Anônimo. *Using Campus Manager*. Cisco Systems. 2000.

[12] Anônimo. *Using Cisco View 5.1*. Cisco Systems. 2000.

[13] Anônimo. *Using Resource Manager Essentials*. Cisco Systems. 2000.