Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Rodrigo Zuolo Carvalho

Análise comparativa de métodos de descoberta de equipamentos de rede

São Paulo
Março de 2007

Rodrigo Zuolo Carvalho

Análise comparativa de métodos de descoberta de equipamentos de rede

Dissertação apresentada ao Instituto de pesquisas Tecnológicas de São Paulo para obtenção do título de mestre em engenharia de computação. Área de concentração: Redes de computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo
2007

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

C331a **Carvalho, Rodrigo Zuolo**

Análise comparativa de métodos de descoberta de equipamentos de rede. / Rodrigo Zuolo Carvalho. São Paulo, 2006.

103p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

1. Rede de área local 2. Topologia de redes de computadores 3. Mapeamento de redes de computadores 4. Ethernet 5. SNMP 6. TCP/IP 7. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Coordenadoria de Ensino Tecnológico II.Título

07-86 CDU 004.732(043)

Rodrigo Zuolo Carvalho

Análise comparativa de métodos de descoberta de equipamentos de rede

Agradecimentos

Agradeço primeiramente ao prof. Dr. Volnys Borges Bernal que me orientou neste trabalho.
Fico grato com toda minha família que me apoiou durante todas as fases de meus estudos. Em especial agradeço à Cláudia Reis Sordi, Roberto Chust Carvalho e Maria Regina Zuolo Carvalho.
Agradeço a toda equipe do NuCC-Internet e a equipe da APT, ambas da PUC-SP. Em especial agradeço ao prof. Victor Emmanuel J. S. Vicente, Marcio Jorge dos Santos e ao Cláudio Seiki Arashiro que me apoiaram e principalmente estiveram presentes nos momentos de desenvolvimento da dissertação.

Resumo

Uma das áreas funcionais do gerenciamento OSI de redes é o gerenciamento de configuração. Em redes baseadas na pilha TCP/IP uma das atividades importantes nesta área de gerenciamento é a descoberta da topologia física e de rede.

Existem configurações de ambientes no qual esta descoberta de topologia e dos mapeamentos de endereços físicos em endereços de rede é mais prejudicada.

Este trabalho realiza o estudo de alguns métodos de descoberta de topologia e propõe a composição de alguns métodos existentes de forma a possibilitar melhora no resultado da descoberta de topologia física mesmo quando os elementos de roteamento destas redes não são gerenciáveis.

Para esta situação, juntamente com o método de descoberta tradicional, é utilizado um método de comunicação induzida.

Através de experimentos que comparam o método proposto com o método tradicional foi possível observar a melhora de resultados obtidos em algumas situações nos processos de descoberta de topologia física e de endereços.

Abstract

One of the functional areas in the OSI network management is the configuration and name management. In the TCP/IP networks this management area has a relevant issue that is the mapping topology and physical discover for network address and devices´ interfaces (layer 2 and 3).

There are some environments configurations that do not allow the network discover topology to works correctly with usual techniques.

This dissertation studies network topology discover methods considering some composition of these on trying and intending to get better results in physical topology discover in despite of the nonexistence of management router or gateways.

In this way the traditional methods are used together with the induced communication method.

The comparative experiments that face the proposed method and a commercial application observed the improvement of results in the network topology discover processes.

I – Sumário

II - Lista de figuras

III - Lista de tabelas

IV – Lista de Abreviaturas

ARP Address Resolution Protocol

DHCP Dynamic Host Configuration Protocol

TCP Transmission Control Protocol

ICMP Internet Control Message Protocol

IEEE Institute of Eletrical and Eletronics Engineers

IETF Internet Engineering Task Force

IP Internet Protocol

MAC Mediaum Access Control

MIB Managemetn Information Base

OSI Open Systyems Interconnect

RFC Request for Coments

RMON Remote Monitoring

SNMP Simple Network Management Protocol

SRT Source Routing Transparent

VLAN Virtual Local Araea Network

1 - Introdução

A pilha do TCP/IP é o padrão de fato utilizado para a transmissão de dados em ambientes corporativos. Em redes locais, a camada mais baixa da pilha (camada "intra-rede"), comumente utiliza-se da família de protocolos derivada do Ethernet : IEEE 802.2, IEEE 802.3u (Spurgeon, 2000), IEEE 802.3ab, entre outros.

Um problema já vastamente estudado é o gerenciamento de redes, incluindo a área funcional do gerenciamento de configuração como descrito no modelo de gerenciamento OSI (Stallings, 1999). Existem várias boas práticas e estudos bem fundamentados que podem simplificar o gerenciamento de redes locais baseadas na pilha TCP/IP; em especial estudos que visam executar técnicas de descobrimento de topologia como em Lowekamp (2000); Gkantsidis (1999); e Manjunath et all (2002).

Através dos estudos supracitados são apresentadas técnicas que permitem realizar a construção topológica da rede e do mapeamento de endereços físicos em endereços de rede, bem como as respectivas portas dos dispositivos em uma rede local.

O modelo de gerenciamento adotado na Internet é baseado no protocolo SNMP. Neste modelo existem entidades chamadas agentes de gerenciamento, executados nos equipamentos, que tem responsabilidade de manipular os "objetos gerenciados" que são definidos em bases de informações denominadas de MIB.

Neste âmbito é necessário lembrar que existem milhares de informações gerenciais disponíveis relacionadas às interfaces de comunicação presentes nos equipamentos (roteadores, pontes, estações de trabalho, etc).

O interesse na determinação e correlação destes objetos gerenciáveis e informações sobre os nós folhas reside no fato de ser possível identificar fisicamente equipamentos a partir dos endereços IP em uma rede local. Ainda, pode-se afirmar que os gerenciamentos de configuração e de desempenho utilizam o conhecimento da topologia para construir considerações e conclusões mais verossímeis. Exemplo disso é visto no diagnóstico de

conflitos de endereço IP ou na busca de equipamentos invasores. Vale citar também que as operações de manutenção, controle e atualização dos dados que constituem a topologia de redes locais se tornam lentas quando não se dispõe de processos automatizados para esta descoberta.

1. 1 - Objetivo

O objetivo deste trabalho é propor a utilização de técnicas adicionais para melhorar a qualidade da descoberta dos "nós folhas" ativos, num dado momento, dentro de uma rede local, baseando-se em métodos de descoberta de topologias já existentes.

Deseja-se, com isso, uma aplicação que levante de forma automática as configurações de IP, MAC e as portas dos equipamentos de uma rede na qual seja possível ter permissão de leitura de informações gerenciais SNMP V1 (Case et al, 1990).

Na comparação dos métodos serão consideradas questões ligadas à descoberta de topologia, tentando ainda contornar eventuais faltas de informações gerenciais decorrentes da existência de equipamentos de interconexão não gerenciáveis ou, ainda, decorrente de outras características das redes que impeçam a aquisição das informações necessárias.

Para realizar a análise comparativa será desenvolvido um sistema para prova de conceito do método proposto. Assim, será possível comparar os resultados do método tradicional com o método proposto.

1.2 – Escopo

Como o estudo em questão trata da geração da topologia da rede incluindo a identificação dos endereços IP associados às portas dos equipamentos em um ambiente gerenciado de redes locais, então todas as considerações e investigações estão relacionadas à camada "intra-rede" (enlace) e a camada de rede da pilha do TCP/IP.

Na teoria do gerenciamento de redes, o estudo se encaixa na área do gerenciamento de configuração, sendo somente realizados acessos de leitura a objetos gerenciados SNMP definidos nas MIB (Stallings, 1999) dos equipamentos da rede.

Quanto à classificação do tipo de rede, esta pesquisa destina-se ao estudo de conjuntos de redes locais, baseadas em ethernet-TCP/IP interligadas por pontes, roteadores ou repetidores que tenham a capacidade de gerenciamento. Já para a realização dos testes reais, foram dimensionados ambientes de redes locais dentro de um campus universitário ou até mesmo um conjunto de campi, que por assim dizer é um conjunto de redes locais.

No referente às aplicações, faz-se necessário limitar o uso de consultas somente para leitura via SNMP através da chave de comunidade pública dos equipamentos gerenciáveis. As dificuldades presentes na dinamicidade da configuração IP dos equipamentos devido à existência de servidores DHCP e VLANs são consideradas neste estudo quando forem pertinentes, entretanto não fazem parte do foco principal de observação.

O desenvolvimento da ferramenta de comprovação utilizou linguagem perl, linguagem C, bibliotecas de interface net-snmp, uucd-snmp e também suporte de ferramentas elementares como ping (Gkantsidis, 1999), ping forjado (Gkantsidis, 1999), entre outras.

1.3 – Justificativa

A linha de estudo adotada faz referência às discussões dedicadas a algoritmos e métodos de descoberta de topologia como os vistos em Breitbart et all (2000) e Lowekamp et all (2001). Todavia, nestes estudos não são abrangidos todos os aspectos do levantamento das configurações de rede. Exemplos disso são situações em que roteadores não possuem gerenciamento SNMP ou ainda quando existem VLANs definidas por endereço de rede.

A solução da busca dos nós folhas é pouco explicitada ou encontrada em ferramentas de código livre. Ocorre que na maioria das vezes os softwares de gerenciamento comumente referenciados, não apenas identificam as interfaces e endereços, mas também compõem uma gama de serviços tão grande que se tornam superficiais para a finalidade aqui desejada.

Deve-se deixar claro que isto não incorre em crítica aos softwares de gerenciamento, mas em uma tentativa de construir uma ferramenta mais especialista ou complementar e que tenha uma visão pontual do problema.

Ao fim destas considerações, deve-se destacar a justificativa do estudo como forma de comparação na determinação espacial dos endereços IP dentro de redes ethernet, através de uma visão auxiliar aos métodos existentes. Fechando as argumentações, vale lembrar que outro aspecto importante é a contribuição deste processo na melhoria da monitoração da topologia da rede.

1.4 – Estrutura do trabalho

Esta seção tem como finalidade apresentar a estruturação do texto que segue,

deixando mais clara a compreensão e delineação da conduta da pesquisa.

O capítulo dois trata acerca de modelos de dados e representações para redes de computadores e suas informações. O objetivo deste não é detalhar o funcionamento das redes, mas construir uma linguagem representativa que melhor expresse o cenário envolvido no estudo.

No capítulo três são apresentados os conceitos de gerenciamento de redes e também são descritos os conceitos e fundamentos elementares do funcionamento das redes. Esta seção é de grande importância, pois a partir desta podem ser apresentadas padronizações a serem utilizadas ao longo de todo o texto.

O quarto capítulo tem o foco direto em técnicas já utilizadas para a descoberta de topologia de redes. Neste trecho do texto há discussão das técnicas e teorias sobre os mecanismos de obtenção de topologia física. Este capítulo aborda de maneira rápida as dificuldades para obtenção das informações, que também são trazidas para o plano principal neste capítulo. Por fim nesta parte do texto é mostrado um panorama geral de como efetivamente deve-se conduzir uma descoberta de topologia física conhecendo estas eventuais dificuldades.

O capítulo cinco trata diretamente do estudo de caso de uma ferramenta que serve de alicerce e inspiração para a construção das propostas de descoberta de topologia e também serve para descrever o funcionamento de um software com tais finalidades.

O sexto capítulo descreve resumidamente a proposta de técnica para solução de descoberta de nós folhas. Nele são apresentadas as técnicas de comunicação induzida utilizando como molde o sistema apresentado no capítulo 5 e também as considerações teóricas do capítulo 4.

Mais à frente, no capítulo 7; são relatados os testes realizados com a ferramenta que prova o conceito, já descrita no capítulo 6. Neste mesmo capítulo, é feita uma análise sucinta e uma apresentação dos resultados dos testes. Com base nestes valores apresentados nesta seção é que são realizadas comparações quantitativas.

O capítulo de número 8 vem discutir, com base nas comparações do capítulo 7, os resultados obtidos para a descoberta de nó folha. As conclusões e considerações são feitas com base nas justificativas perante resultados provenientes do capítulo 7. Finalmente neste mesmo capítulo são descritos os trabalhos futuros e estudos relacionados a este interesse.

Finalizando, no nono capítulo estão as referências bibliográficas e em seqüência estão os anexos que constituem os principais códigos fonte utilizados no sistema de descoberta da topologia.

2 - Modelos para configuração de ambientes de redes

2.1 – Modelo para objetos e configurações

A fim de organizar uma conduta ou formalizar a referência das informações estudadas, adotou-se um modelo de configuração do ambiente de rede assim como o reproduzido em Bernal (1999). Neste documento são definidas as representações das informações topológicas da rede em diversos níveis. Em termos gerais, estas formalizações adotadas ajudam na descrição e documentação dos objetos da topologia.

O nível de maior interesse para esta dissertação considera as informações de equipamentos, de elemento de rede e de domínio de sub-rede; e para melhor entender estas definições, algumas representações serão explicadas e dispostas a seguir.

2.1.1 - Nível de equipamentos

O nível de equipamentos define as conexões físicas entre os diversos equipamentos da rede. Neste nível existem as identificações dos equipamentos e as portas de comunicação.

O ponto relevante aqui é saber como representar as portas de um equipamento. Um exemplo para isso pode ser visto a seguir:

Porta 0 <-> interface eth0 <-> 001122334455

Porta 1<-> interface eth1<->554433bb4455

Donde, nesses relacionamentos tem-se representados as portas de um equipamento e as respectivas interfaces de estações com seus endereços MAC.

2.1.2 - Nível de Elemento de rede

Neste nível a topologia é descrita em função de elementos de rede interconectados entre si. Se um equipamento executa mais de uma função do ponto de vista do sistema, então é possível afirmar que este equipamento é composto por mais de um elemento de rede. Elementos de rede podem ser: roteador, ponte ou bridge, hub, computador ou modem.

As relações de interesse, nestes casos, são apresentadas a seguir com alguns exemplos:

a) Relação Equipamento – Elemento de Rede

Eq1 = {ElementoRede2,ElementoRede3}

Neste caso o equipamento 1 assume papel de dois elementos de rede.

b) Relação Elemento de Rede – Portas

ElementoRede1 = {porta1,porta2}

O elemento de rede 1 possui 2 portas físicas: porta 1 e 2.

c) Relação Porta – MAC

MAC1 = {porta1.Er1}

MAC3 = {porta3.Er2,porta3.Er1,porta5.Er2}

Nesta situação o endereço MAC 1 está associado à porta 1 do elemento de rede 1. Já o endereço MAC 3 está associado às portas 3 e 5 do elemento 2 e à porta 3 do elemento 1.

d) Conexão ponto a ponto entre equipamentos

conexao0 = <ER1.porta2,ER2.porta1>

Neste exemplo, há uma conexão entre dois elementos de rede. O elemento de rede 1 se conecta através de sua porta 2 até a porta 1 do elemento de rede 2.

e) Tabela de encaminhamento das portas

Para cada porta presente em uma ponte ou switch é associada uma tabela de encaminhamento. Esta tabela de encaminhamento consiste no conjunto de endereços de hardware mapeados por cada porta de uma ponte. Seja esta porta denominada de n, então para todos os valores de MAC aprendidos para a porta n de uma ponte A serão representados como F_A^n.

2.1.3 - Nível de sub-rede

No nível de sub-rede são manipuladas as informações relacionadas à camada 3 (camada de rede). As informações relevantes para este nível são: endereço IP, endereço de rede, endereço de broadcast e tabelas de roteamento. Para a descoberta de topologia em nível de sub-rede é comum utilizar as relações exemplificadas adiante:

a) Relação Sub-rede e IPs

Sub-rede1 = {IP1, IP2, IP3,...}

Nesta descrição são mostrados endereços IP da sub-rede 1.

b)Relação IP e MAC

MAC = {IP1,IP2,...}

Nesta relação são atrelados os endereços IP para os endereços MAC dos equipamentos. Em geral esta relação é de um MAC para um endereço, mas nada impede de que exista um único MAC relacionado a vários endereços IP.

2.1.4 – Nó Folha

O nó folha é uma definição que possibilita referenciar da melhor maneira os objetos existentes nas bordas ou elementos da topologia de uma rede. Do ponto de vista da descoberta da topologia de uma rede, na grande maioria, os nós folhas são estações de trabalho, telefones IP, leitores de cartão, etc. Estes equipamentos são aqueles que não agem ativamente nos encaminhamentos das camadas 2 e 3 da rede.

De maneira prática, as informações que modelam o nó folha são conjuntos de dados que identificam um equipamento final. Um nó folha é identificado através do endereço físico (MAC) e lógico (IP) associados à porta de um elemento ao qual este equipamento final está conectado.

2.2 - Classificação das redes abordadas

As redes de computadores a serem utilizadas nos testes e análises podem ser classificadas de diferentes maneiras. Neste nível de modelo são apresentados parâmetros (variáveis) de interesse deste estudo que interferem nesta classificação das redes utilizadas. Existem dois principais parâmetros que são importantes para este nível de modelo: alcance de informação gerenciável via SNMP e alcance de comunicação sem roteamento devido ao domínio de *broadcast* IP.

A seguir são exibidas as classes de redes utilizadas para os testes conforme os dois parâmetros principais previamente citados.

2.2.1 - Classificação dos elementos de roteamento

De fato, não apenas os elementos de roteamento podem influenciar na descoberta de nós folhas e descoberta de topologia, mas também qualquer elemento de rede no qual seja executado um agente SNMP.

Por fatores de facilidade e agilidade, os elementos de roteamento são tidos como principais elementos fornecedores das informações SNMP. De fato o são, pois estes além de conterem as rotas para as redes vizinhas, também podem conter as traduções das relações MAC-IP.

Como a grande maioria das ferramentas de descoberta recorre às informações SNMP contidas nos roteadores, então fica conveniente classificar as redes quanto aos seus elementos de rotemanento. Isto é, indicando se estes elementos possuem ou não a capacidade de responder satisfatoriamente às requisições SNMP.

2.2.2 - Classificação das sub-redes IP quanto à segregação do acesso aos equipamentos gerenciáveis

Por motivos de restrição de acesso administrativo aos equipamentos de rede, várias sub-redes IP podem ser mapeadas sobre uma mesma rede ethernet. Por exemplo, caso a interface administrativa de uma ponte tenha endereço IP na mesma sub-rede que um determinado equipamento (estação); então neste caso a rede pode ser denominada como uma rede não segregada entre pontes e estações.

Por sua vez, redes segregadas são aquelas em que as interfaces administrativas (endereço IP utilizado para o gerenciamento do elemento) de suas pontes não podem

estabelecer comunicações diretamente com uma estação destino. Nestas situações, devem existir roteadores intermediando a comunicação IP entre uma estação e uma ponte.

Uma situação comumente vista na prática é quando uma rede possui pontes com interfaces IP em uma rede 10.1.1.0 enquanto que as estações estão em uma rede não privada qualquer, neste caso 200.144.178.0. Para estas redes, fica definida a nomenclatura de rede com dispositivos (equipamentos, elementos e nós folhas) segregados em nível IP.

Todas estas nomenclaturas e definições serão utilizadas no decorrer do texto e são importantes para familiarizar e delimitar os ambientes que são casos de estudo de descoberta de topologia.

3 – Fundamentos e técnicas do gerenciamento de redes

A dificuldade em se gerenciar redes reside no fato da heterogeneidade de seus componentes. Por isso, modelos e padrões foram adotados na tentativa de minimizar estes problemas. Historicamente, pode-se afirmar a existência de dois modelos principais de gerenciamento: o modelo OSI e o SNMP. Entretanto, o protocolo SNMP foi definido para atender as necessidades do gerenciamento sobre redes TCP/IP e, devido a sua simplicidade, este modelo de gerenciamento tornou-se um padrão de fato.

Apesar de seu funcionamento ser simples, o SNMP pode ser detalhado em pormenores, haja vista as referências em Stallings (1993), Rose e McCloghrie (1995). Para efeitos práticos serão apresentados somente os principais conceitos e principais funcionalidades deste gerenciamento. Além disso, as sessões seguintes apresentam também o funcionamento básico de redes locais para que sejam denominados termos e consensos gerais importantes para o progresso do estudo.

3.1 – Áreas funcionais do gerenciamento

As cinco áreas funcionais desse gerenciamento já muito citadas em várias literaturas como em Stallings (1999) são: gerenciamento de falhas, gerenciamento de contabilização, gerenciamento de configuração, gerenciamento de desempenho e por fim gerenciamento de

segurança. Por sua vez, este trabalho aborda questões relacionadas ao gerenciamento de configuração.

A descrição do gerenciamento de configuração, como em Stallings (1999), assinala a esta área a incumbência de identificar os componentes físicos e lógicos participantes da rede, bem como efetuar ou monitorar a configuração destes. É da alçada deste gerenciamento também manter ou criar relações e componentes dentre os elementos lógicos e físicos através da atribuição, adição ou atualização de valores de configurações.

3.2 - O modelo SNMP

No gerenciamento SNMP, a comunicação se baseia em um modelo cliente-servidor utilizando tipicamente o protocolo UDP da camada de transporte.

Quando um administrador necessita obter informações de um hardware ou equipamento específico, este deve executar uma aplicação chamada de gerente. Do outro lado da comunicação está o agente de gerenciamento, sendo executado no equipamento a ser gerenciado. A figura 1 ilustra melhor esta idéia.

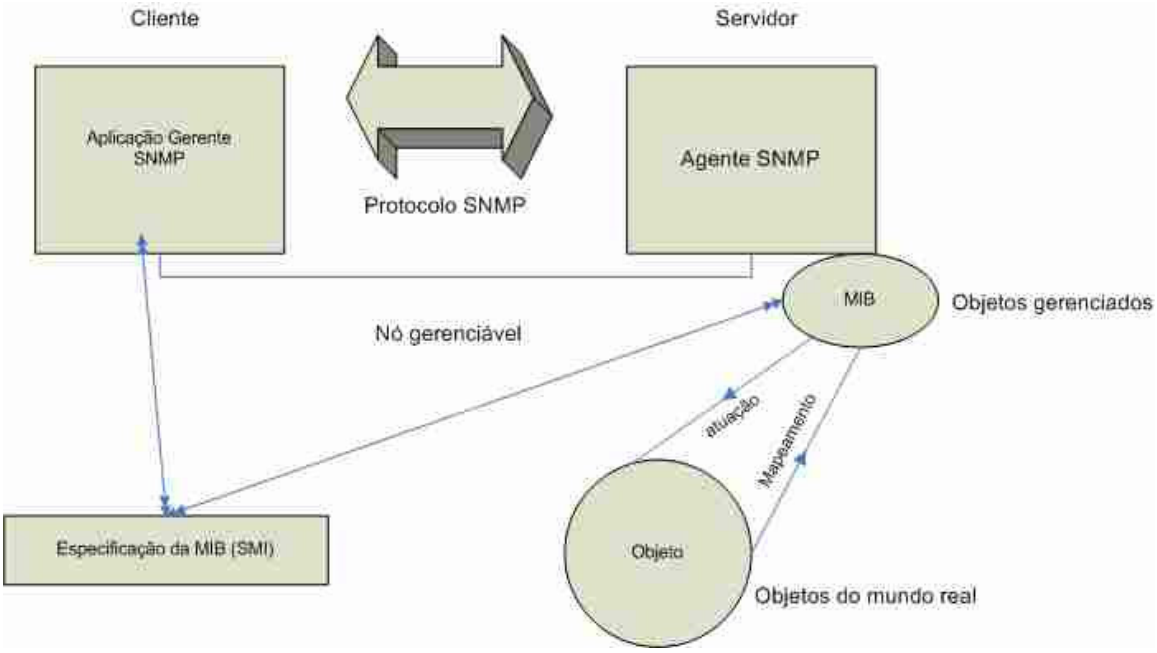


Figura 1 : Gerenciamento SNMP.

Na figura 1 pode-se ver que o modelo de gerenciamento SNMP consiste de quatro componentes principais: agentes, gerentes, objetos gerenciados definidos nas MIB e o protocolo de gerenciamento SNMP.

3.2.2 - O paradigma da comunicação no SNMP

O protocolo SNMP não define uma quantidade extensa de primitivas de protocolo, mas primitivas básicas para monitoração e controle (leitura e escrita).

Neste modelo, o gerente observa ou determina a alteração dos estados dos objetos gerenciados. Por sua vez, o agente é responsável em refletir o estado do objeto gerenciado no objeto real.

Segundo Comer (1999) o paradigma do protocolo SNMP representa uma interação de

carga e armazenamento. “Um gerente carrega ou consulta valores de objetos para determinar certo estado do equipamento; as operações que controlam o equipamento são definidas como efeitos colaterais dos valores armazenados nos objetos”.

De maneira sucinta, os agentes mantém “variáveis” que descrevem os estados dos objetos reais gerenciados. Como cita Tanenbaum (1996), a literatura SNMP refere-se a estas “variáveis” como objetos apesar destes não seguirem exatamente as definições de sistemas orientados a objetos.

Estes objetos gerenciados são descritos através de bases de informações, chamadas de MIBs. As MIBs constituem a essência do modelo SNMP, pois elas definem as informações disponíveis nos agentes.

Para observar ou alterar os valores dos objetos gerenciados nas MIBs, existem operações de leitura e escrita através do protocolo SNMP. Para cada operação deve-se informar o objeto correto a ser manipulado. Uma maneira alternativa de comunicação pode acontecer quando eventos assíncronos ocorrem em um agente e este deve alertar ou notificar imediatamente um gerente para os mais diversos propósitos. Esta comunicação ocorre em forma de traps, que são mensagens SNMP automáticas geradas pelos agentes em direção aos gerentes com o intuito geral de informar o acontecimento de um fato ou condição alarmante.

3.2.3 - Bases para o SNMP

A ASN.1 (Abstract syntax notation 1) é uma linguagem formal padronizada pela OSI e tem como ponto forte a capacidade de abstrair a arquitetura de hardware e demais características subjacentes do equipamento proprietário. Dessa forma, a comunicação entre dois equipamentos de fabricantes diferentes pode ser realizada de maneira transparente e independente de arquitetura adotada.

A ASN.1 serve como base para a formulação da linguagem utilizada no protocolo SNMP e dos objetos gerenciáveis. Mais propriamente dizendo, a SMI (RFC1155) (Structure of Management Information), que é um conjunto de definições baseadas em ASN.1, define

como devem ser os objetos e as primitivas de protocolo utilizados no SNMP.

A SMI (RFC1155) define as macros e os parâmetros utilizados nas MIB, nas quais são permitidos vetores e tipos de dados definidos pelo usuário. A tabela a seguir, retirada de Tanenbaum (1996), exibe os tipos básicos de dados para os objetos SNMP gerenciados.

Tabela 1: Tipos de dados usados para variáveis SNMP monitoradas

Nome	Tipo	Bytes	Significado
INTEGER	Numeric	4	Inteiro (32 bits)
Counter32	Numeric	4	Contador de 32 bits que zera em determinado limite (crescente)
Gauge32	Numeric	4	Valor unsigned que não zera (crescente)
Integer32	Numeric	4	32 bits, mesmo em CPU 64 bit
UInteger32	Numeric	4	Contador inteiro de 32 bit unsigned.
Counter64	Numeric	8	Contador de 64 bits
TimeTicks	Numeric	4	Centésimos de segundo desde uma data estipulada
BIT STRING	String	4	Mapa de bits de 1 a 32
OCTECT STRING	String	≥0	String com tamanho de um byte
Opaque	String	≥0	Obsoleto
OB JECT IDENTIFIER	String	>0	Uma lista de inteiros
IpAddress	String	4	Endereço de internet
NsapAddress	String	<22	Endereço NSAP OSI

As primitivas do protocolo SNMP geralmente são encapsuladas sobre o protocolo UDP, definidas na tabela que segue (Tanenbaum 1996).

Tabela 2: Tipos de mensagens SNMP V1

Mensagem	Descrição
Get-request	Requisita o valor de um ou mais objetos
Get-next-request	Requisita o valor do objeto seguinte
Set-request	Atualiza um ou mais objetos
Inform-request	Mensagem ente gerentes para descrever a MIB local
Get-response	Resposta para uma requisição
Get-bulk-request	Leitura de tabelas grandes

Outra característica importante herdada da ASN.1 é a capacidade de identificação dos objetos gerenciados por meio de OIDs. A identificação baseada em OIDs é estruturada em uma árvore já padronizada, permitindo a identificação dos objetos gerenciados difundidos nas MIB. A raiz desta árvore tem como ponto de origem a organização ISO, donde todos demais objetos são filhos. Com isso, é possível identificar precisamente um objeto através de números presentes no caminho da raiz até os níveis em que este objeto se encontra na árvore. Ou seja, o objeto identificador do grupo system da MIB II pode ser designado através do valor 1.3.6.1.2.1.1 como se vê no esquema de árvore da figura 3.

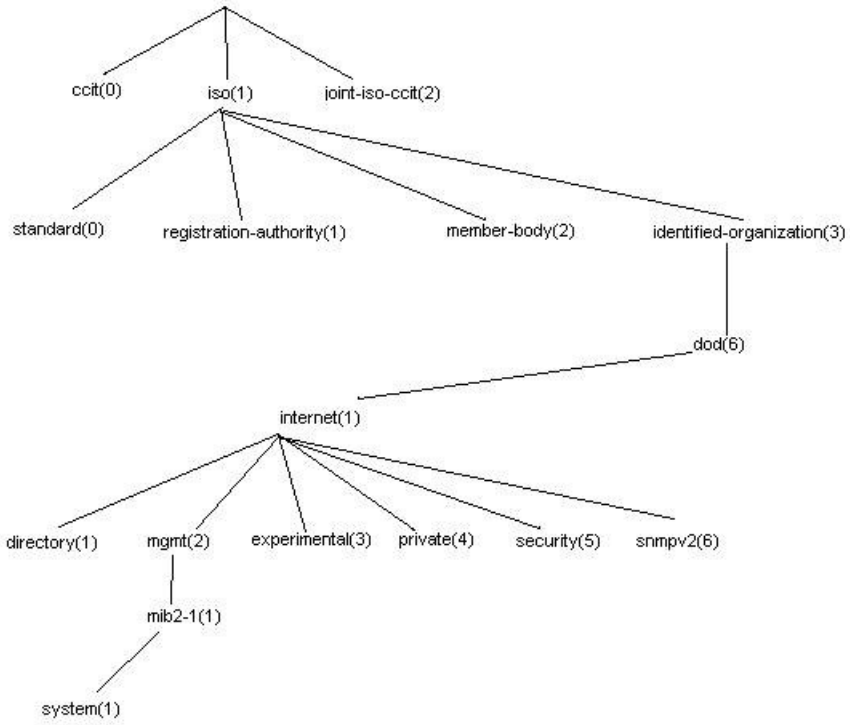


Figura 2: Árvore identificando os ID de objetos

As MIBs podem conter tanto objetos escalares quanto vetores que, na verdade, são listas de objetos ou ainda tabelas. Como a ASN.1 não prevê operação de indexação, isto faz com que o acesso às tabelas seja feito através de referências indexadas implícitas. Com isso, para se consultar um objeto deve-se conhecer o nome da tabela e a referência de indexação a fim de obtê-lo.

3.3 - Pontes Ethernet

O entendimento a respeito dos switches ou pontes ethernet são primordiais para que sejam esclarecidas as razões dos métodos escolhidos e como melhor orientar o desenvolvimento destes métodos. Não convém que os algoritmos e detalhes sejam

pormenorizados, mas sim os conceitos básicos de como os quadros ethernet são encaminhados e quais são as informações disponíveis e ainda como acessá-los. Todos esses aspectos devem ser relacionados sempre visando à solução do problema central.

3.4 - Encaminhamento de pacotes

Uma switch ethernet é a denominação atual do mercado para equipamentos do tipo ponte operando geralmente no modo *transparent bridge.* Para efeito prático, são descritos a manipulação das informações e o funcionamento básico do encaminhamento dos quadros entre as interfaces físicas destas pontes.

Suponha que seja A uma das interfaces ethernet de uma ponte. Assim, quando um quadro com o endereço de origem X chega até a interface A, a ponte faz com que uma nova entrada seja criada em sua tabela de encaminhamento, relacionando o endereço X com a interface A. Em um dado momento posterior; suponha que um quadro com endereço destino X tenha sido recebido na interface B. Nesta ocasião a ponte (*Source Routing Transparent*) deve então encaminhar este quadro originário na interface B para a interface A.

De maneira superficial, este é o funcionamento de encaminhamento de quadros em pontes SRT. As informações manipuladas são relativas às interfaces ethernet e aos endereços MAC.

3.5 - Informações gerenciáveis

Atualmente, grande parcela das pontes contém agentes de gerenciamento. Os endereços MAC, conforme comentado anteriormente, são adicionados um a um em tabelas de encaminhamento com a finalidade de promover o encaminhamento transparente entre os diversos pontos da rede local.

Ao se conectar uma estação a uma ponte, o primeiro quadro ethernet enviado por esta estação faz com que, automaticamente, seja registrado na respectiva entrada da tabela de encaminhamento desta ponte, o respectivo endereço MAC da estação (equipamento final).

Estas tabelas de encaminhamento são mapeadas em objetos gerenciáveis segundo formatos padronizados na MIB bridges, vide RFC 1493 (Decker et al, 1993).

A MIB para bridges RFC 1493 (Decker et. all; 1993) tem um identificador mib-2.17. Por sua vez, o grupo de interesse para observação dos valores desta tabela de bridge é o dot1dTp. Este grupo modela os objetos de pontes transparentes. Desta forma, a tabela dot1dTpPortTable presente neste grupo é de grande interesse para este estudo, pois representa a tabela de encaminhamento. Esta entrada Dot1dTpFdbEntry é uma seqüência de Dot1dTpFdbSAddress, Dot1dTpFdbPort e Dot1dTpFdbStatus. O primeiro objeto tem identificação 1.3.6.1.2.1.4.3.1.1 e retrata o valor para um endereço MAC ao qual a ponte está encaminhando ou filtrando. O objeto Dot1dTpFdbPort tem identificação 1.3.6.1.2.1.4.3.1.2 e indica a porta para o qual um endereço MAC de origem tenha sido encontrado. O objeto Dot1dTpFdbStatus indica o estado desta entrada na tabela Dot1dTp, sendo eles: outro (1), inválido (2), aprendido (3), self (4) e mgmt (5).

Em poucas palavras, da MIB bridge deve-se aproveitar a tabela Dot1dTpFdbEntry para o estudo corrente. Mais especificamente os objetos 1.3.6.1.2.1.4.3.1.1 (Dot1dTpFdbSAddress) para MAC e os objetos 1.3.6.1.2.1.4.3.1.2 (Dot1dTpFdbPort) para portas.

Existe ainda outra tabela de grande interesse para a descoberta dos nós folhas e que pode ser encontrada tanto em switches quanto em roteadores ou em qualquer elemento de rede

gerenciável, pois mantém a tradução de valores de endereço IP em respectivos endereços MAC. Esta tabela pertencente ao grupo IP da MIB II leva o nome de ipNetToMediaTable (OID 1.3.6.1.3.1.4.22). Cada entrada é formada pelos objetos ipNetToMediaIfindex, ipNetToMediaPhysAddress, ipNetToMediaNetAddress e ipNetToMediaType. Dentre estes todos, o objeto de importância é o ipNetToMediaPhysAddress (OID 1.3.6.1.2.1.4.22.1.2), cujo próprio nome (IP para endereço físico) já indica sua finalidade.

Em roteadores as informações destes objetos são de grande valor, pois em geral contém o mapeamento de todos os endereços ativos das redes diretamente conectadas a este roteador, principalmente quando a rede não contém sub-redes ou proxy. Porém estas tabelas nas pontes de camada 2 puras não apresentam valores, pois como naturalmente se espera das pontes, nada é tratado em camada 3 (nível IP). Grosso modo, ocorre que se uma ponte não se comunica via IP com uma estação, então informações que relacionam MAC em IP não são adicionadas nas tabelas da MIB.

O uso de repetidores gerenciáveis também pode ser utilizado na busca dos nós folhas. Para isso, pode-se utilizar a MIB repeater. A RFC 2108 (D., McMaster et. al, 1997) define a existência da tabela rptrAddrSearchTable que possibilita identificar endereços MAC associados a cada porta de um repetidor gerenciável da rede. Cada entrada da tabela possui o endereço MAC de origem do último quadro recebido pela porta do repetidor naquele momento. A porta é identificada pelo o objeto rptrAddrSearchPort (OID 1.3.6.1.2.1.22.3.1.1.6) e rptrAddrSearchAddress (OID 1.3.6.1.2.1.22.3.1.1.3) identificando o quadro com endereço de origem e a porta de origem.

4 - Descoberta de topologia e equipamentos de rede

Com a finalidade de entender o funcionamento do mecanismo da descoberta de topologia, apresentam-se, de maneira sucinta, estudos anteriores acerca deste assunto neste capítulo.

São discutidos os métodos de descoberta de nós folhas, donde se é desejável formular técnicas adjacentes às já existentes nos processos de descoberta de topologia física.

Analisando somente o mérito da descoberta de topologia física, tem-se que o mapeamento das conexões e posicionamento dos elementos em uma topologia física é fundamental na determinação e identificação de aplicações da rede (Lowekamp; 2000) e estabelece um suporte na tomada de decisões para aplicações cujos recursos incluem a rede (Lowekamp et. al, 2001).

4.1 – Introdução ao mapeamento da rede

Para se fazer um mapa da rede é necessário utilizar um conjunto de métodos e técnicas já que não há um método único ou protocolo que forneça a solução desejada.

A elegância e versatilidade do encaminhamento de quadros ethernet são importantes para facilitarem a comunicação, embora tornem o processo da identificação da topologia e descoberta de endereços menos favoráveis.

A descoberta do endereço IP associado a uma interface ethernet (porta) de um equipamento conectado à rede deve ser obtida através de consultas SNMP junto ao grupo

interface da MIB II. Porém, a consulta diretamente ao equipamento "folha" esbarra em diversos problemas. O principal deles está relacionado à possível ausência de gerenciamento SNMP nestes equipamentos.

A determinação da conexão entre a porta de um elemento em nível 2 (ponte ou repetidor) ao equipamento (endereço MAC) pode ser obtida ao se consultar diferentes informações gerenciais nestes elementos. No caso das pontes, a determinação é realizada com base em sua tabela de encaminhamento. Já no caso dos repetidores esta determinação é feita com base na sua tabela de repetição. Ambas as consultas utilizam o protocolo SNMP anteriormente citado.

Assim, vários algoritmos baseados no conhecimento do funcionamento da tecnologia ethernet e no SNMP podem ser empregados para esboçarem o resultado da descoberta de topologia.

Dentro destas considerações, conforme a prática e estudos de diversos ambientes como em Manjunath et al(2002) e Gkantsidis(1999), pode-se afirmar que existem fatores capazes de definirem o grau de dificuldade para que um monitor descubra a topologia da rede. Eis que as situações críticas na determinação de topologia são:

- Existência de uma ponte ou repetidor não gerenciável ou não acessível;
- Existência de repetidores interligando duas pontes ou mesmo uma ponte não gerenciável interligando outras duas pontes;
- Computadores que não respondam comunicações ICMP (tipo echo request) ou computadores que não tenham suas interfaces listadas nas tabelas de encaminhamento das pontes pelo motivo de ainda não terem estabelecido comunicação com as mesmas;
- Dificuldade na aquisição da tabela de encaminhamento completa de algumas pontes;
- Interface administrativa dos equipamentos em segmentos IP não pertencentes ao segmento da estação de gerenciamento (monitor);

À medida que estes problemas dificultam a determinação da topologia, se faz necessário criar técnicas ou medidas de contorno para eliminá-los ou minimizá-los.

4.2 – Descoberta da topologia da camada de rede

O processo de descoberta de topologia geralmente se inicia pela descoberta de topologia de rede, identificando as sub-redes do ambiente.

Para isto, a estação de gerenciamento consulta sua tabela de rotas. Através desta tabela de rotas é possível identificar as sub-redes nas quais o equipamento está conectado e também identificar eventuais roteadores existentes. Neste caso, no mínimo um roteador é identificado: o *default gateway*.

Para cada roteador identificado é realizada a consulta à tabela de roteamento (através de requisição SNMP) e realizando novamente o procedimento anterior.

Ao final do processo são identificados os roteadores do ambiente e as sub-redes existentes. O próximo passo é realizar a descoberta de equipamentos existentes em cada sub-rede.

Os resultados desta etapa apresentam conjuntos como Sub-rede1={IP1, IP2, IP3,...}, Sub-rede2 ={IP4, IP5, IP6, ...} e assim sucessivamente. Em geral as ferramentas de descoberta fazem uso de pacotes ICMP *echo request* que podem ser enviados para endereços IP *broadcasts* tanto quanto endereços *unicast* de maneira seqüencial. As respostas a estes pacotes formam então o conjunto de endereços IP que estão ativos nesta sub-rede.

4.3 – Descoberta de topologia a nível físico

A construção de topologia consiste na identificação de como os equipamentos

(computadores e elementos de rede) estão conectados fisicamente entre si. Portanto nesta fase são determinadas as ligações entre as portas dos equipamentos. Estas ligações, como vão ser discutidas mais à frente, são classificadas ou divididas em:

- Conexão entre roteadores, pontes e repetidores.
- Conexão de nós folhas com pontes, repetidores ou roteadores.

4.3.1 - Métodos para descoberta de conexões entre pontes

A seguir são apresentados métodos que definem o reconhecimento das interconexões entre as pontes em uma rede local. As conexões entre pontes podem ser vistas como de forma direta quando uma esta conectada diretamente a outra ou então através de segmentos em comum, porém indefinidos.

4.3.1.1 – Teorema da conexão Direta

Este método estabelece uma prova formal de como identificar se uma ponte está conectada diretamente até uma outra ponte (Lowekamp, 2000). Aqui segue uma sucinta explanação deste método.

A figura 3 ilustra um exemplo a ser aplicado por este método:

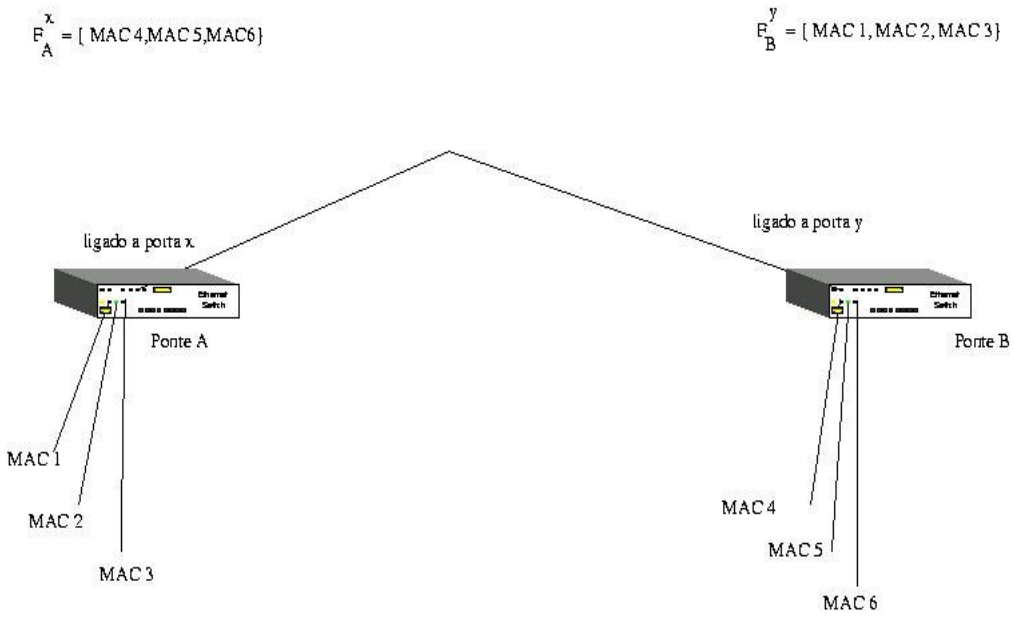


Figura 3 : Duas pontes Conectadas Diretamente

Os elementos do conjunto F_A^x são os endereços MAC relacionados na entrada da tabela de encaminhamento da ponte A referente à porta x. Lembrando que estes endereços MAC presentes nestas entradas são alterados quando computadores da rede são deslocados, quando novos computadores são anexados, ou ainda quando uma das entradas da tabela expira. Neste método, o termo N representa o conjunto de todos os nós presentes na sub-rede ethernet. Dentro deste conjunto N, podem-se subdividir dois outros conjuntos: o conjunto das estações, representado por E, e ainda o conjunto de equipamentos roteadores, repetidores e demais equipamentos da rede denominados de R.

Ao verificar a figura 3 obtém-se de maneira dedutiva o teorema da conexão direta, expresso a seguir.

Se F_A^x e F_B^y são completos, então as duas pontes A e B estão diretamente conectadas através das portas x e y se e somente se $F_A^x \cap F_B^y = \emptyset$ e $F_A^x \cup F_B^y = N$.

Mas é enganoso afirmar a simplicidade da confirmação de tais expressões. Por infelicidade das circunstâncias não é possível garantir que a tabela completa de encaminhamento de endereços seja obtida facilmente para qualquer porta da ponte. Pois para

se completar essa tabela muitas vezes se faz necessário gerar um número excessivo de *pings* e comunicações de ponta a ponta que nem sempre tem resultado efetivo, mesmo existindo o enlace real entre esses dois pontos.

O método discutido acima é uma teoria que ajuda a entender como se obtêm um desenho da topologia física da rede utilizando processos automáticos para a descoberta. Deve-se então utilizar este método como ponto de partida para estudos que envolvam o processo de descoberta de topologias físicas e afins. De fato, o que vem a seguir são teorias e métodos que discutem a validade deste teorema e ainda como complementá-lo ou contribuir para este.

4.3.1.2 - Teorema da Conexão Indireta

Como descrito por Lowekamp (2000), uma conexão indireta (referenciada como conexão compartilhada por Lowekamp,2000) pode ser descoberta se todos os membros presentes entre essas duas pontes tiverem seus respectivos endereços MAC presentes nas entradas das tabelas de encaminhamento referentes às interfaces de conexão entre estas duas pontes.

Dentre as citações em Lowekamp (2000), o teorema da conexão indireta foi ilustrado em termos de um segmento compartilhado denominado por S. Além disso, a(b) identifica a porta da ponte "a" ao qual se encontra o endereço "b". Já S_b é o conjunto de pontes conectadas ao segmento S compartilhado e S_e representa os pontos finais ou estações ligadas a este segmento S. A partir destas definições pode-se formalizar o teorema da conexão indireta: S consiste em um segmento compartilhado entre duas pontes em S_b se e somente se $\forall a \in S_b, \forall b,c \in S : a(b) = a(c)$. Esta afirmação supõe que as tabelas de encaminhamento de S e Sb estejam completas.

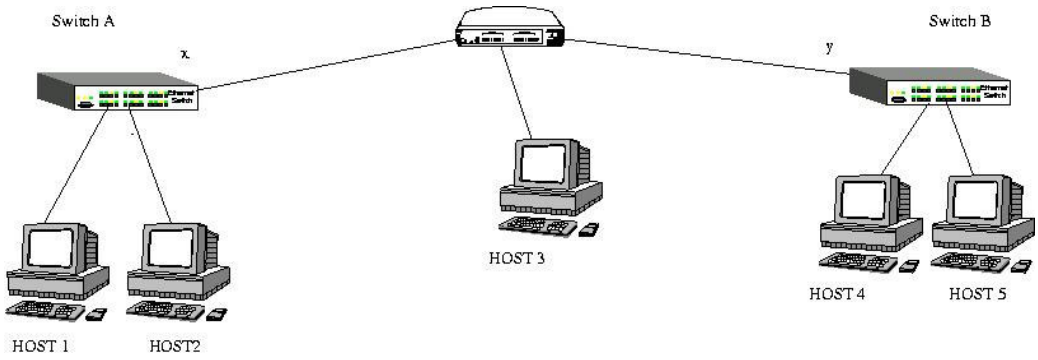


Figura 4: Pontes A e B interligadas por segmento não gerenciável

Observa-se na figura 4 que existem elementos entre a porta x de A e a porta y de B. Isto pode ser descoberto através da presença do endereço MAC da estação 3 nas portas x da ponte A e y da ponte B. Além disso, todos os endereços MAC presentes nas entradas da tabela de encaminhamento de A, excluindo-se a porta x, estão presentes na entrada referente à porta y da tabela de encaminhamento de B e vice-versa, sempre supondo-se que a tabela de encaminhamento esteja completa.Apesar da sucinta citação deste teorema, deve-se ressaltar a utilidade deste na determinação de segmentos não gerenciáveis durante o processo de descoberta de topologia. Esta técnica pode ser aproveitada como método alternativo ou como referência a um método de identificação de repetidores ou mesmo pontes não gerenciáveis na descoberta de topologia. Em suma, estes estudos de conexão indireta e direta foram introduzidos visando ajudar na descoberta da topologia da rede.

4.3.1.3 – Limitações para o teorema da conexão direta

O teorema da conexão direta, tal como proposto é bem consolidado e também formulado com base no conhecimento do funcionamento de redes ethernet. Entretanto para que se

obtenham bons resultados uma única condição limitante é imposta: o conhecimento das tabelas completas de encaminhamentos das pontes.

Para uma pequena quantidade de pontes ou redes pequenas, esta condição não se torna fator crítico. Todavia, quando os números de estações ou pontes aumentam, há um grau de dificuldade muito maior em se obter as tabelas de encaminhamento completas.

Ainda assim, se houverem muitas estações fica difícil forçar o tráfego entre elas. Para fazer com que todas as estações façam uso da rede, é necessário realizar um acesso remoto até as estações ou forçar para que haja, por exemplo, comunicação ICMP entre elas. De fato, esta premissa para a conexão direta torna-se uma condição trabalhosa e difícil de alcançar em grande parte das situações (Lowekamp, 2000).

Por estas razões é que se fazem necessários métodos alternativos que permitam visões menos rigorosas dos ambientes e exijam menos informações gerenciáveis. São, portanto, estas visões que serão abordadas (a partir deste trecho do estudo).

4.3.1.4 – Teorema da conexão simples

Devido às dificuldades em se encontrar as tabelas de encaminhamento completas em redes locais ethernet é que se fez necessária a apresentação de um método alternativo de determinação de conexão entre pontes.

Desta forma, Lowekamp (2000) define como determinar uma conexão simples entre duas pontes. Note que o termo simples indica que duas portas de diferentes pontes estão conectadas de maneira direta, isto é sem intermediários, ou também de maneira indireta, com equipamentos interligando-as.

Para se entender a interconexão entre duas portas de duas pontes é necessário fazer uso dos casos de contradições que por ventura existam. Eliminando as contradições é possível montar um desenho que seja capaz de ilustrar a real topologia da rede.

A figura 5 apresenta, por meio de ilustração, a tabela de encaminhamento nas pontes relacionando os endereços MAC registrados em cada uma das portas das pontes.

A tabela 3, baseada na figura 5 permite verificar quais situações poderiam ser factíveis

tendo em vista as tabelas de encaminhamento descritas. A coluna de mapeamento descreve todas as combinações possíveis para as conexões diretas ou indiretas entre as duas pontes da figura 5. A sintaxe dessa coluna é direta e descreve a seqüência de conexão estabelecida pelos elementos. Dessa forma quando o endereço MAC Y estiver conectado diretamente com a ponte B teremos a seguinte designação: {Y}B. De outra forma, se o endereço MAC X for aprendido entre duas pontes A e B, formando uma interconexão teremos a seguinte designação: A{X}-{X}B. Por fim, se o MAC Z for aprendido em uma porta de A e o MAC Y for aprendido em outra porta de B e ainda assim A e B estiverem conectadas diretamente por duas outras portas quaisquer, teríamos a representação: {Z}A-B{Y}.

Nota-se que os endereços de estações são colocados entre chaves({}), enquanto que as conexões são escritas como traços (-). O que se deseja explicar é uma maneira de transcrever as possibilidades de interconexão entre as pontes e às estações (representadas pelos endereços MAC), como se pode ver na tabela 3 adiante.

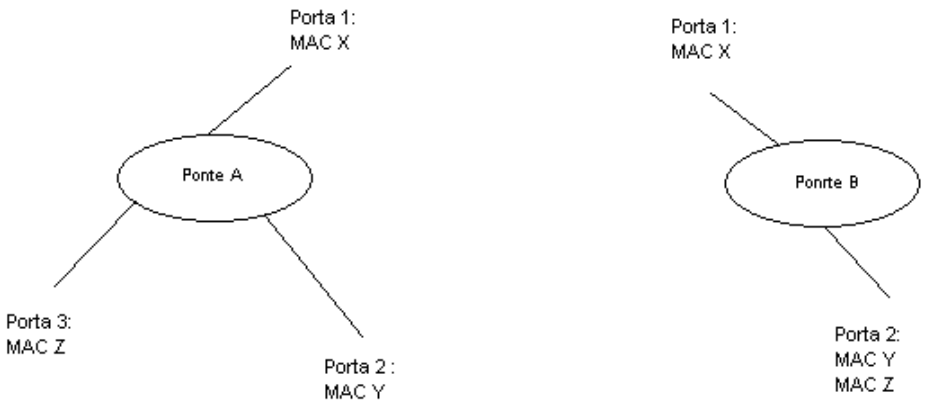


Figura 5: Exemplo de tabelas de encaminhamento das pontes A e B com conexão simples.

Tabela 3 : Verificação de contradições para conexão simples entre pontes A e B.

Conexão entre Pontes			
Porta em A	Porta em B	Mapeamento	Contradição
1	1	{Z,Y}A{X}-{X}B{Y,Z}	Y e Z
3	1	{Y,X}A{Z}-{X}B{Y,Z}	Y
2	2	{Z,X}A{Y}-{Y,Z}B{X}	X
2	1	{Z,X}A{Y}-{X}B{Y,Z}	Z
1	2	{Z,Y}A{X}-{Y,Z}B{X}	Nenhuma
3	2	{Y,X}A{Z}-{Y,Z}B{X}	X

A tabela 3 exibe exatamente como seriam os prováveis mapeamentos de topologias, possibilitando a eliminação daqueles que possuem contradições. A terceira coluna exibe como seriam as tabelas de encaminhamento se as conexões das colunas 1 e 2 fossem seguidas. Isto é, na última linha da tabela 3 apresenta-se a situação em que a porta 3 de A está ligada a porta 2 de B, com isso o endereço Z é aprendido proveniente da ponte B enquanto os endereços Y e X são aprendidos ou através de outras pontes ou mesmo de estações diretamente ligadas a quaisquer portas que não a porta 3. O conflito aparece quando o endereço X é aprendido em dois sentidos diferentes da conexão proposta entre a porta 3 de A e a porta 2 de B.

Como se pode ver no exemplo da figura 6, quando as portas 1 de A e 1 de B estão conectadas tem-se o conflito dos endereços MAC Z e MAC Y pois em uma rede ethernet não é permitida a existência de laços, o que impede que Y e Z sejam aprendidos em pontos opostos da rede local. O mesmo tipo de conflito ou contradição pode ser visto em todas as situações exceto na qual a porta 1 de A se conecta à porta 2 de B, o que induz a concluir que esta seja a forma com que estas pontes estão conectadas, seja de forma direta ou indireta.

Este teorema vem resolver o problema da necessidade em se obter a tabela completa de encaminhamento. Entretanto ainda assim são necessários alguns requisitos imprescindíveis.

O teorema da conexão simples exige que haja um conhecimento mínimo da tabela de encaminhamento. Caso contrário, não é possível construir as contradições esperadas para eliminação de possibilidades.

Este conhecimento mínimo (Lowekamp, 2000) pode ser entendido através de um exemplo prático como visto na tabela 4 e figura 6.

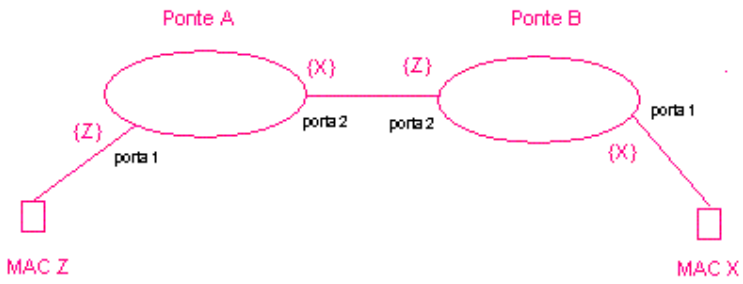


Figura 6 : Falta de conhecimento na determinação de uma conexão simples.

Tabela 4 : Verificação do conhecimento mínimo.

Porta em A	Porta em B	Mapeamento	Contradição
1	1	{X}A{Z}-{X}B{Z}	Nenhuma
1	2	{X}A{Z}-{Z}B{X}	X
2	2	{Z}A{X}-{Z}B{X}	Nenhuma
2	1	{Z}A{X}-{X}B{Z}	Z

Neste exemplo devido ao conhecimento de apenas dois endereços não foi possível determinar uma única disposição possível da rede. A solução para este caso em específico seria conhecer mais um endereço das tabelas de encaminhamento capaz de gerar contradições.

Mais formalmente, o conhecimento mínimo pode ser enunciado no seguinte teorema auxiliar:

As portas que conectam as pontes A e B são unicamente determinadas se e somente se umas das três condições a seguir forem satisfeitas:

1. Cada ponte contenha uma entrada para o endereço MAC da outra (MAC A ou MAC B), ou
2. A ponte A contenha uma entrada contendo o endereço MAC de B associado À porta x em sua tabela de encaminhamento e $\exists k \neq x : F_B^{\ y} \cap F_A^{\ k} \neq 0;$ ou
3. As pontes A e B contenham em suas tabelas de encaminhamento ao menos três nós (estações finais representados por endereços MAC) em comum. Este nós devem aparecer em duas portas de uma ponte (seja A ou B) e em três portas na outra. Além disso, este conjunto de portas deve conter x e y.

Assim, o teorema da conexão simples dá grande poder à descoberta da topologia de rede e se torna uma solução simples e eficaz na descrição das conexões entre pontes em uma rede Ethetnet. Este método foi proposto e estudado por Lowekamp (2000) e pode ser encontrado na ferramenta de diagnóstico de rede REMOS (Lowekamp et al., 2001), a qual é base para a formulação do estudo corrente.

4.3.2 – Descoberta de conexão de nós folhas

Para finalmente realizar a descoberta completa da topologia é necessário identificar os computadores ligados à rede e relacionar quais são as portas dos equipamentos aos quais se conectam.

Como fora citado no capítulo 3, este mapa pode ser construído através da obtenção de informações presentes nas MIB (ver seção 3.5). Em especial a relação MAC1 = {porta1.Er1} pode ser extraída de dois objetos da MIB bridges existentes na tabela dot1dTpFdbTable.

Através destes dois objetos e um índice de valor comum é possível saber qual porta possui um determinado endereço MAC

Um ponto importante a ser considerado é de que as portas previamente citadas como interconexões de pontes devem ser eliminadas nesta busca de nós folhas. Uma situação hipotética que ilustra isso é quando duas pontes A e B e uma estação com MAC Y têm as seguintes relações válidas: conexão0 = <A.1,B.2>, MACY = {porta1.B,porta1.A}. Neste caso, o endereço MAC Y deve aparecer nas portas 1 de B e 1 de A, mas para efeitos de construção do desenho de topologia deve-se considerar apenas a relação MACY = {porta1.B}, pois a relação MACY = {porta1.A} existe proveniente do fato da porta 1 de A ter aprendido todos endereços pertencentes à B, uma vez que a porta 2 de B está cascateada na porta 1 de A.

Após terem sido mapeados todos os relacionamentos MAC={porta.Er}, deve-se realizar o passo de tradução de endereço, contemplando todas relações do tipo MAC = {IP}. Em outras palavras realizar a tradução ARP, e se conveniente até uma possível resolução de nomes.

Uma das possíveis formas de se obter a tradução de endereço MAC em endereço IP é através da consulta de uma tabela ARP. Porém, não se garante que existam todas as traduções presentes na tabela. Para forçar esta completude da tabela a estação monitora tem que estabelecer comunicação via protocolo IP com todas as estações da mesma sub-rede. Isso pode ser realizado através de sucessivas execuções do comando ping, o que forçará a realização da tradução de endereço IP em endereço MAC via protocolo ARP.

Em seguida é possível consultar a tabela ARP com requisições SNMP em busca de um objeto já existente nas MIB. Este objeto é o OID ipNetToMediaPhysAddress (1.3.6.1.3.1.4.22) da MIB2. Os índices para estas entradas indicam os endereços IP enquanto os valores dos objetos são os endereços MAC relativos a estes índices (IP).

Um exemplo de retorno de uma consulta SNMP para resolver a tradução IP em MAC pode ser vista a seguir:

IP-MIB::ipNetToMediaPhysAddress.24.200.144.145.41 = STRING: 0:1:3:d0:ce:d7

Nesta linha é apresentada a associação do endereço IP 200.144.145.41 que também é índice do objeto e por sua vez deve ser traduzido no endereço MAC 0:1:3:d0:ce:d7.

A presença de um servidor DHCP poderia facilitar consideravelmente a tradução MAC={IP}. Mas este tipo de serviço não é sempre utilizado em configurações de ambientes críticos. Seria muito útil o uso de tal sistema, haja vista que o próprio sistema de *log* do servidor DHCP disponibiliza traduções de endereços MAC em IP.

Através dessas técnicas é possível descobrir os nós ou estações ligadas à rede e com isso finalizar o desenho da rede. A tarefa seguinte é examinar a aplicação destas técnicas e

verificar possíveis melhorias e seus resultados obtidos.

4.4 – Técnicas e práticas para descoberta de topologia física

Após terem sido apresentadas as teorias e técnicas necessárias à descoberta de topologia física e o mapeamento de endereços de camada intra-rede (endereço MAC) em endereço de rede (endereço IP), tem-se nesta seção o detalhamento destas quando aplicadas em conjunto na tentativa prática de solucionar o problema central: a descoberta da topologia física e em específico os nós folhas.

4.4.1 – Técnica de descoberta ordinária de topologia física

Este é um método trivial que, em geral, é muito utilizado nas principais ferramentas de mercado desde o inicio do desenvolvimento de aplicações gerenciadoras (Chen; et al, 1998). Os passos de seu funcionamento serão discutidos a seguir bem como ilustrados na figura 7.

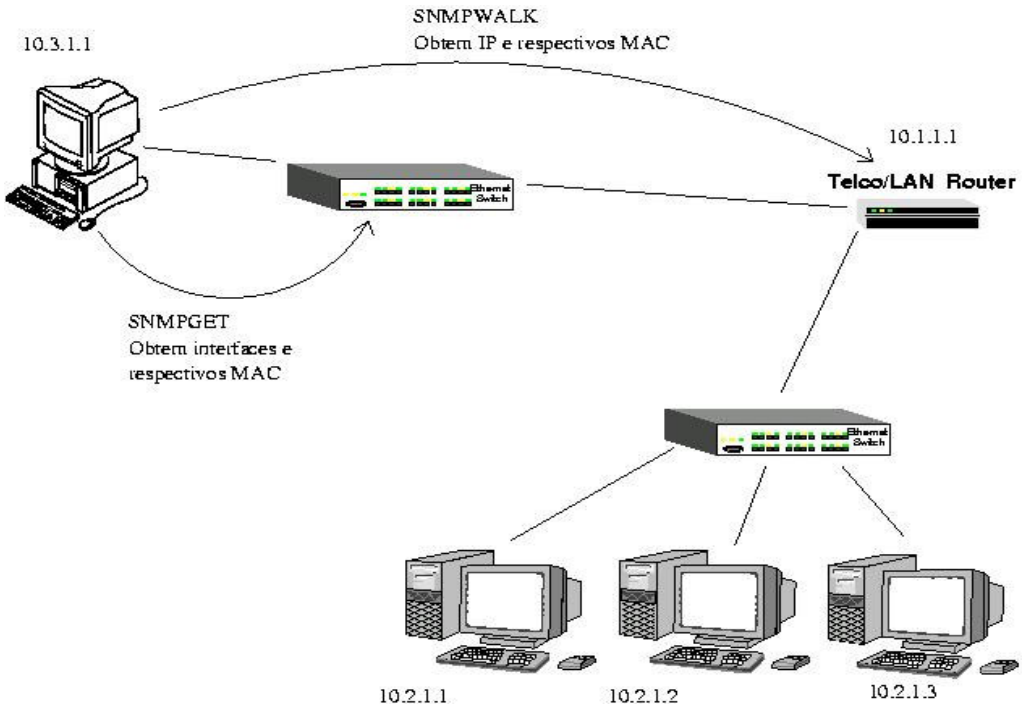


Figura 7: Descoberta de endereços através de consultas ao roteador

Esta técnica pode ser dividida nos seguintes passos:

a) Descoberta de equipamentos: presente em todas prévias de descoberta de topologia como já fora descrito na seção 4.2. Para este passo o requisito é conhecer uma faixa de endereços IP, máscara de rede IP ou endereço de rede IP. Com isto, mensagens ICMP são enviadas a todos os endereços possíveis a fim de encontrar os equipamentos ativos. Após encontrá-los, estes endereços IP são relacionados em uma lista de endereços IP ativos. Ainda, neste processo, é possível fazer uma identificação dos tipos de cada equipamento encontrado. Neste caso eles podem ser um repetidor, uma ponte ou um roteador.

b) Identificação do tipo de equipamentos: Através do envio de requisições SNMP são identificados os equipamentos gerenciáveis. As requisições SNMP para o objeto SysServices possibilitam identificar a classe do equipamento: repetidor, ponte, roteador ou computador. As listas aqui criadas devem ser mantidas durante todo o processo, pois elas definem quem faz parte da topologia de núcleo e quem faz parte da borda (supostamente nó folha).

c) Construção da topologia: Através de requisições SNMP para as pontes e repetidores existentes torna-se possível rastrear com ajuda de algoritmos quais são as ligações entre os elementos de rede e através de que portas o fazem.

Depois de serem determinadas as portas de interconexão ou portas de interligação da rede restam somente portas pertencentes aos nós folhas, e estas são tratadas no item a seguir.

d) Identificação de equipamentos folhas: Os equipamentos pertencentes aos nós folhas são identificados através da listagem obtida em b), mais especificamente através do restante da subtração do conjunto de total de equipamentos com os conjuntos de roteadores, pontes e repetidores (Nós Folhas = Equipamentos – Pontes – Repetidores – Roteadores).

Feito isso, é necessário em alguns casos mapear o nível lógico da rede. Isto é, deve-se estabelecer o relacionamento com a camada 3 da rede, IP={MAC}. Para isto, deve-se consultar através de mensagens SNMP ao roteador da rede. Esta consulta deve retornar a tabela ARP referente a todas as relações MAC={IP} satisfazendo agora a identificação em nível IP dos nós folhas existentes.

4.4.2 - Técnica de descoberta de topologia com variante na tradução ARP de nós folhas

Este segundo método é uma variação do anterior e pode ser utilizado somente em redes que estejam diretamente conectadas à estação de gerenciamento. A variação ocorre no encontro do conjunto solução MAC={IP} que identifica um único nó folha através da lógica de funcionamento do protocolo ARP.

A cada segmento de rede ao qual se deseja encontrar as triplas MAC, IP e porta, é necessário se adicionar uma estação de gerenciamento. Infelizmente essa necessidade leva a afirmar que neste método o processo parcial de descoberta da topologia se torna um requisito e não mais parte integrante do desenvolvimento da solução. Isto é, para descobrir a rede, é

necessário conhecer ou saber algo de antemão.

Em caráter elucidativo, a figura 8 mostra o panorama de um típico ambiente em que este tipo de configuração é aplicado. Cada um dos segmentos de rede, neste caso representado por pontes não interconectadas possui uma interface da estação gerenciadora conectada à rede responsável.

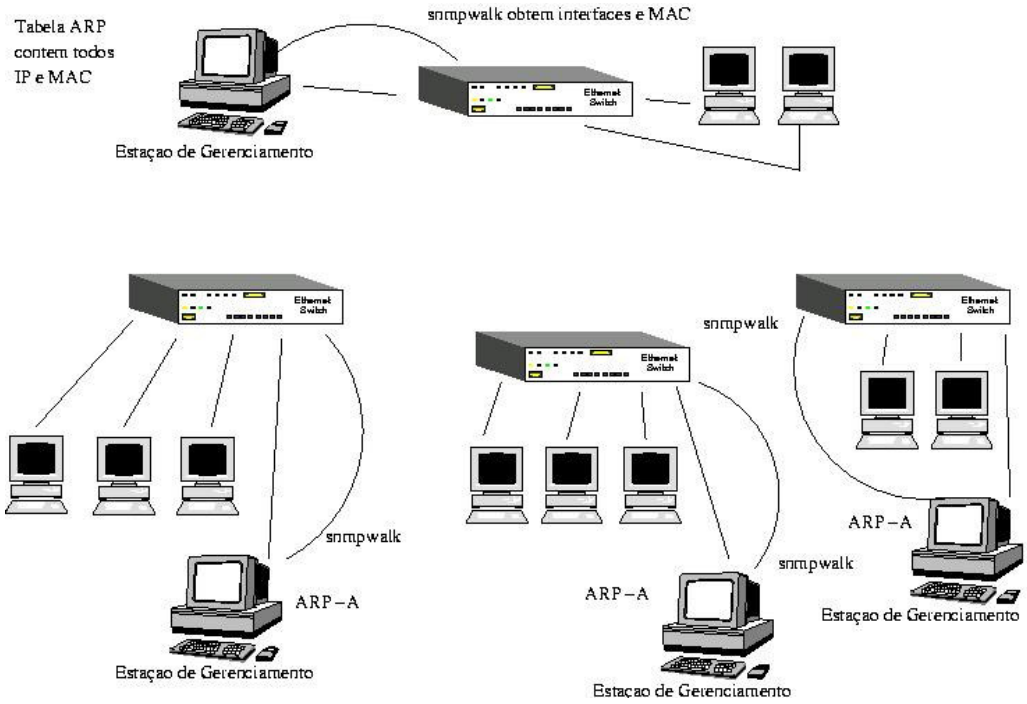


Figura 8 : Descoberta de endereços em segmentos locais

Os passos para efetivação do método são idênticos ao processo ordinário exceto pelo passo d que poderia ser reescrito assim:

d) Identificação de equipamentos folha: Utilizando os conceitos do protocolo ARP, a estação gerenciadora envia mensagens *arp request* para obter a resposta de todos IP locais. Nesta tentativa de estabelecimento de comunicação ocorre a montagem da tabela ARP com todas as estações ativas naquele momento. Isso permite à estação de gerenciamento consultar a tabela ARP local e obter todas as

relações MAC={IP} ativas.

4.4.3 - Método de descoberta de topologia com variante para teoremas da conexão simples e indireta

Esta terceira técnica utiliza os teoremas de 4.3.1.1 e 4.3.1.2 para identificar as interconexões entre as pontes e repetidores da rede. Deste modo é possível através de um requisito menos rigoroso obter todas as informações necessárias para a construção da topologia.

O passo necessariamente diferente neste método é o item c de 4.4.1 que poderia ser reescrito como:

c) Construção da topologia: Através de um conjunto de pontes ou repetidores é possível conhecer suas interligações através de algoritmos que façam uso do teorema da conexão simples. Isto é, através da análise dos conjuntos de endereços MAC dos elementos de rede presentes nas tabelas de encaminhamento é possível com apenas três endereços conhecidos para cada tabela gerar as inconsistências que por sua vez eliminam as conexões improváveis. Da mesma maneira é possível encontrar segmentos indefinidos através do teorema da conexão indireta. Para que isso seja possível novamente é necessário se analisar o conjunto de endereços relativos a cada porta e assim certificar a existência de um meio compartilhado em uma interconexão.

5 – Descoberta de topologia pela ferramenta REMOS

As técnicas citadas no capítulo anterior são bastante utilizadas e, em geral, não apresentam problemas para a maioria dos ambientes de rede existentes no universo prático.

Ocorre que, em determinados casos específicos e por determinadas circunstâncias é difícil realizar a descoberta de maneira totalmente eficaz.

O algoritmo de descoberta adotado pela ferramenta REMOS foi escolhido como uma ferramenta base para se poder fazer uma análise e diagnosticar quais são os casos específicos em que a descoberta de topologia pode ser prejudicada e de que maneira isto ocorre.

A ferramenta REMOS foi adotada não por ser uma ferramenta pioneira, mas sim por ser eficaz em termos de resultados obtidos e também por ser construída e disponibilizada em código livre. Outras ferramentas serão citadas apenas como referências e parâmetros de comparação.

5.1 – O funcionamento da ferramenta REMOS

A ferramenta REMOS tem um propósito além do mapeamento da topologia da rede. A aplicação foi desenvolvida com o intuito de diagnosticar e gerar informações para aquelas aplicações que dependem do uso da rede. Ela desempenha a função de uma API para outras aplicações que desejam utilizar a rede (Lowekamp et al., 2001). Ela informa também quais são os recursos disponíveis e como melhor os utilizar. Entre outras atividades a ferramenta

monitora o desempenho da rede para poder decidir qual melhor caminho para um determinado fluxo de dados de aplicação. Tendo em vista isso, a ferramenta necessita de um mapa topológico prévio da rede. Este processo de geração do mapa topológico se relaciona diretamente com este estudo.

O módulo de descoberta de topologia (Lowekamp, 2001) é um software em código aberto capaz de construir e descrever a topologia da rede baseado na pilha TCP/IP e na tecnologia ethernet. A seguir é apresentado o funcionamento deste módulo de software e analisado atentamente seu método.

5.1.1 – O algoritmo da descoberta de topologia

A aplicação REMOS que realiza o mapeamento topológico utiliza as técnicas de descoberta baseadas nos teoremas da conexão simples (item 4.3.1.4) e também no teorema da conexão indireta (item 4.3.1.2). Em específico pode-se retirar de Lowekamp (2000) toda a comprovação e detalhamento do funcionamento que se façam interessantes.

Basicamente, o núcleo do sistema de descoberta de topologia REMOS tem uma seqüência de ações que podem ser divididas nos seguintes passos:

- Preparação
- Aprendizado
- Derivação da topologia e algoritmo de mapeamento
- Mapeamento de nós folhas

Estes passos são detalhados nas seções a seguir.

5.1.2 – Preparação

A preparação do algoritmo de descoberta de topologia consiste em uma prévia descoberta dos dados envolvidos no cenário em que se executa a aplicação. Para que o processo se inicie, a estação de gerenciamento deve estar conectada a uma rede ethernet cujo conjunto de nós E e o conjunto de pontes e repetidores B seja conhecido (endereços IP dos equipamentos da rede). Todos esses conjuntos devem necessariamente estar ligados à mesma rede ethernet. Com isso é possível fazer uma preparação de dados para o processamento da descoberta da topologia da rede considerando sempre o fato de que a estação que realiza esta descoberta esteja diretamente conectada a esta rede, isto é, que não existam roteadores entre a estação de gerenciamento e a rede que se realiza a descoberta.

A estação gerenciadora deve executar *pings* a todos os endereços de pontes e de nós folhas para obter os dados de tradução MAC={IP} existentes na tabela ARP local, de forma que estes sejam utilizados posteriormente na análise da topologia. Além de realizar a tradução, este tráfego de mensagens ICMP faz com que as tabelas de encaminhamento das diversas pontes venham a ser preenchidas, uma vez que as estações estabelecem comunicação com a estação gerenciadora.

Além disso, a estação gerenciadora requisita via SNMP às pontes e aos repetidores quais são as quantidades de portas existentes. Com estas consultas a estação gerenciadora poderá construir uma estrutura de dados contendo todas as pontes e suas respectivas portas. Estas informações serão posteriormente úteis na solução do encaminhamento de quadros através da identificação dos endereços MAC em questão.

5.1.3 – Aprendizado

O processo de aprendizado (descoberta de topologia física) é simples e requer somente que a estação gerenciadora obtenha as tabelas de encaminhamento das pontes presentes no ambiente da rede. Isto mais uma vez é realizado através de requisições SNMP.

Durante estas consultas, execuções contínuas de *ping* aos endereços IP são realizados em paralelo. Esta execução contínua se dá através de uma aplicação nomeada de PING_SERVER que deve estar ativa enquanto se estiver executando a aplicação REMOS.

Esta aplicação roda como plano de fundo para certificar que ao menos os endereços dos computadores que estiverem ativos deverão aparecer nas tabelas de encaminhamento das pontes.

5.1.4 – Derivação da topologia e algoritmo de mapeamento

Após o passo de levantamento das informações do ambiente de rede, a próxima tarefa da aplicação REMOS é iniciar a construção das interligações entre as pontes existentes.

A primeira fase consiste em eleger uma ponte que seja raiz de todas as outras. Esta ponte raiz deve conter informações suficientes para que o requisito do conhecimento mínimo não falhe para as demais filhas. Isto significa que a heurística adotada para se encontrar a ponte raiz leva em conta a maior quantidade de endereços mapeados na maior quantidade de portas possíveis.

A quantidade de endereços encontrada em cada porta de cada ponte é somada. Esta soma de endereços desconsidera a porta que contém o maior valor de endereços mapeados.

Assim, a ponte que possuir a maior soma é eleita como ponte raiz.

Esta supressão da porta que possui a tabela de encaminhamento mais preenchida possibilita a escolha da ponte que contém muitos endereços em múltiplas portas, ou seja, pontes que tenham suas tabelas de encaminhamentos bem preenchidas e balanceadas.

Depois de adotar uma ponte raiz deve-se procurar em suas portas por pontes que estejam diretamente conectadas.

Para se comprovar se uma ponte está diretamente conectada a uma porta da ponte raiz deve-se utilizar o teorema da conexão simples. Isto é feito somente com o uso do conjunto de endereços dos próprios elementos de rede (pontes).

Quando um endereço de uma ponte filha aparece em uma porta candidata da ponte raiz, deve-se consultar a tabela de encaminhamento da porta da ponte filha que contenha o endereço da ponte raiz (porta de *uplink*) e verificar pela existência de outras pontes que também apareçam na porta candidata (porta em que esta ponte filha havia sido encontrada na ponte raiz). Se não existirem endereços de outras pontes que estejam nesta porta de *uplink,* então esta porta bem como a porta candidata da ponte raiz pode ser considerada como a interconexão direta entre ambas as pontes. De outro modo, se o endereço de uma ponte que exista na porta candidata for encontrado também na possível porta de *uplink,* então a conexão não pode ser direta já que existe uma terceira ponte intermediária.

Na figura 9 pode ser visto um exemplo da situação onde o mínimo conhecimento é atendido de maneira indireta, já que ao menos 3 endereços foram conhecidos: o endereço da raiz, o endereço de A e o endereço ou de B ou de C. A figura 9 mostra a ponte A ligada diretamente à ponte raiz, enquanto a figura 10 mostra como seria a interligação da ponte raiz com as pontes B e C intermediando.

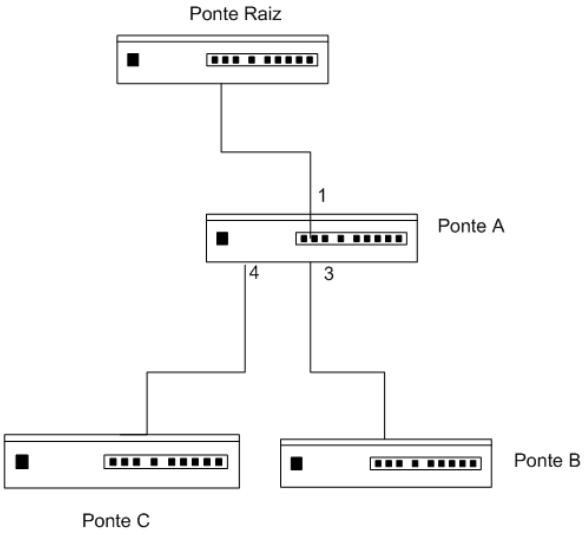


Figura 9 : Ponte A ligada diretamente à ponte raiz

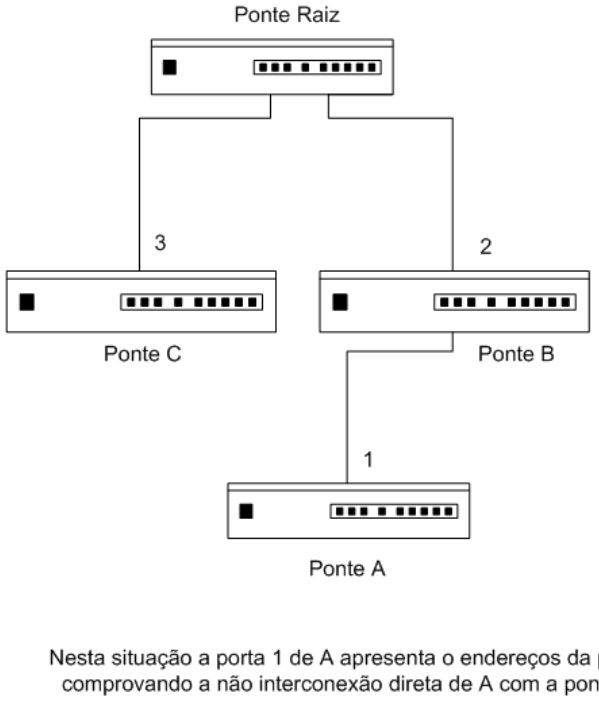
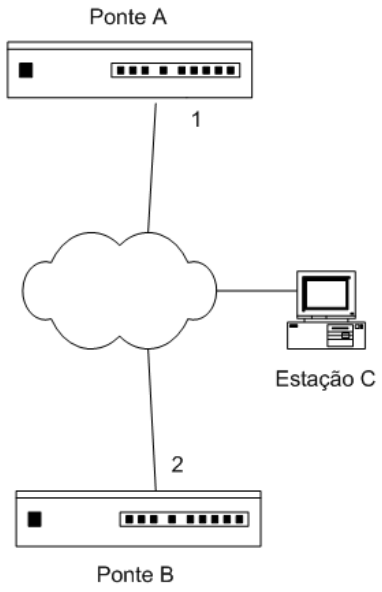


Figura 10: Ponte A ligada indiretamente à ponte raiz

Este processo deve ser executado continuamente até que se acabem as pontes a serem mapeadas. Após mapear as ligações para a ponte raiz deve-se realizar a eleição de novas pontes raízes, filhas daquela ponte raiz do processo anterior. Isto caracteriza a recursividade

do algoritmo. Deve-se entender que o ponto crucial neste passo é que para cada porta x e y das pontes A e B que sejam possíveis candidatas à interconexão deve-se tentar resolver se $F_{A}^{x} \cap F_{B}^{y} = \emptyset$ tentando comprovar a interligação entre tais portas.

Existem maneiras de se minimizar o efeito causado por erros encontrados devido à existência de pontes ou repetidores não gerenciáveis interconectando duas ou mais pontes como foi descrito pelo teorema da conexão indireta (seção 4.3.2). Neste caso um ou mais endereços desconhecidos aparecem tanto na porta da ponte raiz quanto na porta de interligação da ponte filha. Além disso, o endereço MAC da ponte raiz aparece na tabela de encaminhamento para a porta da ponte filha assim como o endereço MAC da filha aparece na tabela para a porta de interligação da ponte raiz. Como na figura a seguir.



A nuvem indica a existência de uma ponte ou repetidor não gerenciável. Assim o endereço da estação C aparece nas tabelas de A e B provando que as portas 1 e 2 não estão ligadas diretamente.

Figura 11: Pontes interligadas por nuvem não gerenciável

Quando estas situações ocorrem, é necessário introduzir na topologia o que se chama de elemento de rede não gerenciável. Este deve interligar dois segmentos de rede que a priori se pensou que estivessem ligados diretamente. Depois de inserir estes equipamentos virtuais podem-se ligar as pontes filhas nessas nuvens de rede geradas por estes equipamentos e dar procedimento no mapeamento dos restantes dos nós e pontes.

Em conjunto com conhecimento mínimo, esta técnica de equipamento não gerenciável forma o grande trunfo (Lowekamp, 2000) desta aplicação de descoberta de topologia para a

ferramenta REMOS.

5.1.5 – A determinação dos nós folhas

Como cita Lowekamp (2000) a grande maioria dos casos para mapeamento dos nós folhas é realizado subtraindo-se os endereços IP dos repetidores e das pontes gerenciáveis do conjunto total de endereços IP descobertos.

Já para os casos em que se deseja identificar repetidores ou pontes não gerenciáveis deve-se notar a presença de um ou mais endereços MAC na tabela de encaminhamento de uma porta candidata à porta de nó folha. Nestas condições, o que é muito comum encontrar duas possibilidades:

- Ligação de um novo repetidor não gerenciável em uma extremidade da rede.
- Ligação de uma ponte não gerenciável em uma extremidade da rede.

Verificando a determinação dos nós folhas, pode-se segmentar o processo em duas fases distintas e independentes:

- Obtenção do mapeamento IP em MAC do nó folha.
- Determinação da porta da ponte em que se encontra o MAC.

Percebe-se que a determinação da porta em que se encontram os endereços MAC não pode ser realizada de forma diferente a não ser pela já citada e realizada no processo de aprendizado. Entretanto para a tradução existem algumas alternativas distintas e que consistem de fato no principal assunto que se deseja discutir mais a fundo nesta dissertação.

A partir daí quer se mostrar alguns ambientes de rede e suas possíveis influências nas considerações de tradução dos nós folhas assim como os efeitos destes ambientes em uma ferramenta como esta detalhada.

6 – Proposta de método de resolução e preenchimento da tabela ARP

A descoberta dos nós folhas foi explicitada anteriormente, entretanto as possíveis dificuldades ou adversidades provenientes das configurações de ambiente são escassamente citadas na maioria das literaturas referenciadas. Com isso, os itens que se seguem abordam problemas apresentando métodos que solucionem ou possam agregar em qualidade no resultado final do processo de descoberta de topologia. A primeira atitude nesse sentido é enumerar as características que podem compor cada um dos ambientes existentes nestes tipos de redes.

6.1 – Cenários que influenciam a determinação de nós folhas

Quatro tipos principais de redes são passíveis de discussão quando se trata da disposição de equipamentos gerenciáveis. O parâmetro diferencial entre as redes escolhidas como nas comparações consiste no endereçamento de nível de rede (nível IP) dos equipamentos de rede gerenciáveis e também na localização na rede das estações gerenciadoras.

Desta forma, são citados estes quatro tipos de redes bem definidos cujas nomenclaturas foram apresentadas no capítulo 2. Sendo elas:

- Sub-rede IP não segregada com roteador gerenciável: Sub-rede ethernet em que os equipamentos de rede e os nós folhas estão em uma mesma sub-rede ou domínio de broadcast IP;
- Sub-rede IP não segregada com roteador não gerenciável: Contém todas as

características anteriormente citadas, entretanto não dispõe de elementos de roteamento gerenciáveis via SNMP MIB II. Neste caso, situações típicas são roteadores baseados em computadores utilizando roteamento TCP/IP, como exemplo estações com plataforma linux interligando duas sub-redes IP diferentes;

- Sub-rede IP segregada com roteador gerenciável: Nesta sub-rede ethernet os equipamentos de rede estão em uma sub-rede IP diferente das estações e, conseqüentemente, a estação de gerenciamento que executa a aplicação de descoberta de topologia não poderá se comunicar com uma ponte via IP sem antes atravessar um roteador comum entre ambos.
- Sub-rede IP segregada com roteador não gerenciável: Este caso é idêntico ao anterior, no entanto não há roteadores que forneçam informações nos moldes da SNMP MIB-II. Supostamente este ambiente é o que apresenta o maior grau de dificuldade para as ferramentas de descoberta de topologia dada a grande quantidade de restrições que o mesmo estabelece.

6.2 – Descrição da proposta

A proposta deste trabalho é utilizar uma técnica para melhorar a qualidade do processo de descoberta. Nesta alternativa de descoberta o gerenciador utiliza processos não usuais de comunicação, forçando aos equipamentos gerenciáveis de camada 2 armazenarem todas informações pertinentes ao conjunto solução procurado. O intuito desta técnica é eliminar as consultas aos roteadores da rede, delegando essa responsabilidade somente às pontes ou a quaisquer outros equipamentos gerenciáveis em nível de enlace. Assim, na tentativa de completar a relação MAC1={porta1.Er1} e MAC1={IP1}, deve-se fazê-la através de pesquisas concentradas nos elementos gerenciáveis de nível 2, em geral *switches*. Para o sucesso dessa operação é necessário conhecer os equipamentos gerenciáveis existentes e também fazer com que estes se comuniquem de alguma forma com todas as estações alcançáveis ao menos uma vez. A figura 12 reflete mais claramente a filosofia deste método.

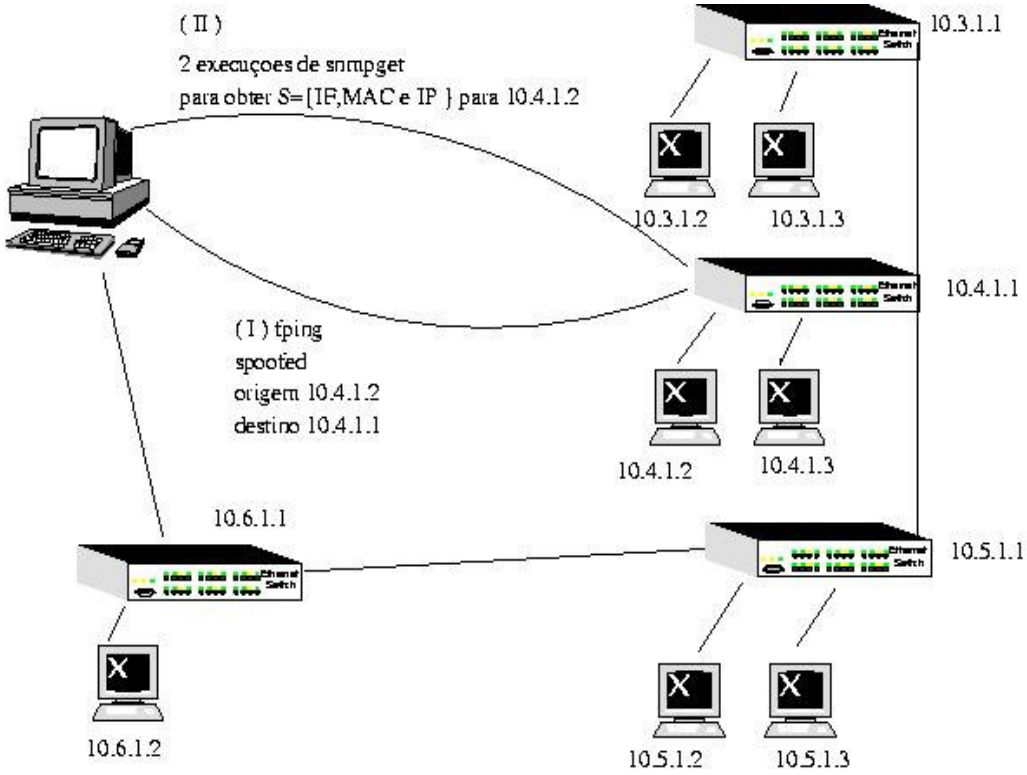


Figura 12: Descobrimento de endereços através de pings forjados

Os passos de execução deste processo são vistos a seguir:

- Processo de descoberta: Através de uma faixa de endereços IP faz-se consultas SNMP a fim de encontrar os equipamentos gerenciáveis e as pontes. Ao fim destas consultas os equipamentos descobertos são relacionados para serem utilizados no próximo passo de busca.

- Processo de busca: Conhecendo-se as pontes existentes, são executados estímulos sobre essas a fim de estabelecer comunicação ethernet entre as estações e cada ponte. A estação gerenciadora envia um pacote ICMP *echo request* com o endereço origem forjado. O endereço forjado corresponde ao endereço IP de uma determinada estação ao qual se deseja encontrar a solução. Dessa forma, a estação responde a ponte com um ICMP *echo reply*. A ponte por sua vez mantém a tradução do IP em MAC em sua MIB ou tabela ARP.

- Processo de identificação: Sabendo que todas as informações estão armazenadas na MIB do equipamento, são realizadas consultas SNMP as quais retornam a solução explícita de IP, MAC e interface para os objetos consultados. Mais uma vez aqui é referenciada a MIB descrita nas RFC 1213 (McCloghrie; 1991).

Assim esta técnica além de ser suporte em situações críticas específicas, deve também ser incorporada em ferramentas de descoberta de topologia a fim de tornar eficaz e permitir que estas atinjam um grau de sucesso maior.

6.3 – Análise comparativa entre os métodos de descoberta de nós folhas

Conhecendo os ambientes existentes e os métodos descritos, torna-se possível formular uma comparação entre estes três métodos de descoberta e assim construir uma visão mais crítica em relação à descoberta de topologia.

Suponha o método convencional ou ordinário sendo executado em uma rede que não dispõe de um roteador gerenciável via SNMP. Isto de fato irá tornar impossível a consulta das relações MAC={IP} por causa da falta de informações provenientes do roteador. Neste caso em específico o método induzido proposto aqui pode solucionar este problema sem exigir novos recursos e requisitos a não ser os já existentes que são o fato das pontes possuírem gerenciamento SNMP acessível.

Caso exista uma VLAN definida em nível de endereço IP ou porta, a estação de gerenciamento pertencente a uma VLAN não pode traduzir ou resolver através da tabela ARP o relacionamento MAC={IP} se o valor de IP pertencer a uma outra VLAN remota. De fato, isto é impossível e fica mais crítico ainda se neste ambiente acrescenta-se um roteador não gerenciável via SNMP. Nesta situação o método induzido de comunicação vem preencher de maneira correta a lacuna não atingida na tradução MAC={IP} da VLAN externa. Vale lembrar, que o roteador ou concentrador das VLANs deve em todos casos permitir o encaminhamento de pacotes forjados, já que em alguns casos ainda que internos à rede; o administrador bloqueia nos roteadores esses tipos de pacotes.

Por fim, outra vantagem que se assemelha muita à citada anteriormente é quando se deseja descobrir a topologia de uma rede local além de um roteador. Nesta situação a ferramenta REMOS não consegue levantar informações, pois exige que a cada rede local exista uma estação de gerenciamento. Se também nesta situação o roteador permitir que pacotes forjados sejam repassados, então o método de descoberta induzido pode de forma satisfatória descobrir a topologia de uma rede local além do roteador. A figura 13 a seguir exibe essa situação com clareza.

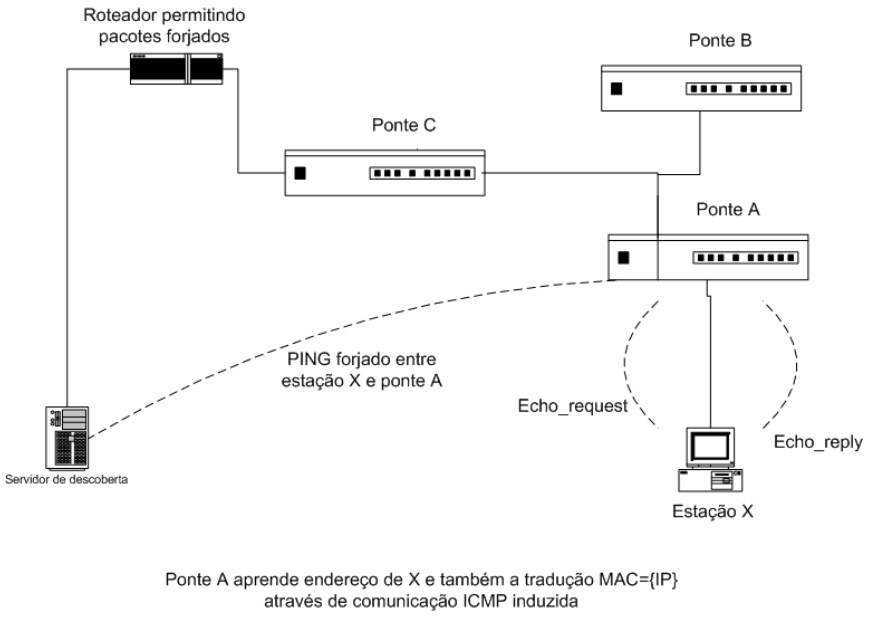


Figura 13: Descoberta além de um roteador usando técnica de comunicação induzida

Ao se aplicar pacotes ICMP *echo_request* forjados para as estações e pontes da rede remota, pode-se executar o algoritmo de descoberta de topologia já que este necessita de informações apenas de nível UDP/IP neste tipo de método.

Estas considerações motivaram a construção de um protótipo para a descoberta da topologia que unissem as já consolidadas técnicas utilizadas na ferramenta REMOS com as técnicas para tradução propostas aqui. Esta construção e execução de testes são discutidas no próximo capítulo.

6.4 – Limitação de escopo de utilização dos testes

Após estas considerações sobre as resoluções dos nós folhas, há informações suficientes para que sejam planejados testes e experimentos destes métodos de descoberta em ambientes pré-conhecidos.

A fim de realizar uma análise comparativa serão abordados ambientes diversos para a execução de testes de tradução MAC={IP} e MAC={porta.er} somente.

O escopo dos testes será limitado por estas resoluções já que é conhecida a vantagem do método proposto de tradução induzida nas identificações das relações entre endereço MAC e endereço IP. Grosso modo, quer se afirmar que o método proposto deve melhorar o mapeamento entre os níveis 2 e 3 dos modelos de referência OSI e, portanto os testes a serem realizados no capítulo seguinte levarão em conta somente os resultados para tais traduções e não mais problemas referentes à descoberta topológica e interconexão entre as pontes.

7 – Desenvolvimento, execução e análise dos testes

Neste capítulo são apresentados os ambientes de testes e também as ferramentas utilizadas nas análises dos métodos discutidos e propostos até o momento.

7.1 – A ferramenta proposta

A ferramenta "prova de conceito" para descoberta de topologia reúne um conjunto de métodos. Estes são inspirados principalmente na ferramenta REMOS e também no conceito da comunicação induzida disposta no capítulo anterior.

O módulo de software que realiza a tradução ou comunicação induzida é aquele responsável em descobrir a relação entre endereço MAC e IP e é baseado na comunicação de pacotes ICMP forjados. Este foi construído em scripts, salvo exceção do código que realiza a geração de pacotes ICMP *echo_request* forjados que foi escrito em linguagem C. O módulo de descoberta de conexões diretas ou descoberta de topologia (inspirado em REMOS) foi escrito em linguagem *perl* e scripts *bash*. Todos estes códigos são colocados mais à frente nos anexos da dissertação para a conveniência do leitor.

A ferramenta proposta composta por tais códigos pode ser dividida em algumas rotinas ou módulos de software distintos.

- Construção da topologia: módulo que realiza a descoberta das conexões físicas entre as pontes utiliza os mesmos métodos da ferramenta REMOS (teorema da conexão simples). Além disso, esta seção do software realiza a consulta das relações MAC={porta.Er}, ou seja,

a tabela de encaminhamento de cada porta. Nesta parte do programa o método de comunicação induzido, embora sendo dispensável, também é utilizado no intuito de forçar o aprendizado dos endereços MAC de todas pontes nas tabelas de encaminhamento de maneira mais rápida. Isto é, se uma ponte tenta se comunicar com outra ponte, então os endereços MAC de ambas ficarão armazenados nas respectivas tabelas de encaminhamento. Com isso, o requisito do conhecimento mínimo (capítulo 4) para a comprovação das conexões diretas pode ser alcançado mais facilmente caso seja feito uso desta técnica no momento anterior ao da descoberta de topologia. Como conseqüência desta comunicação induzida, as pontes acabam contendo ao menos os endereços MAC umas das outras além dos endereços dos equipamentos folhas.

- Determinação dos endereços IP e nós folhas: este módulo de programa descreve as relações entre endereços MAC e endereços IP da rede. Para que isto seja possível são executadas comunicações forjadas conforme o método de tradução induzido já citado. Essas comunicações forjadas preliminares são importantes para solucionarem o problema da tradução de endereço MAC em endereço IP. Após sucessivas comunicações induzidas, é necessário realizar as leituras finais SNMP que são responsáveis em obter os valores soluções para todos os endereços de nós folhas. Esta comunicação induzida bem como a leitura subseqüente dos valores MAC={IP} pode ser realizada em único equipamento (elemento) da rede ou então em múltiplos equipamentos. Esta configuração é dada como parâmetro de entrada do sistema. Isto traz flexibilidade de escolha, permitindo à ferramenta realizar a tradução ARP em um determinado roteador ou então em grupo específico de pontes.

7.1.2 – Considerações teóricas sobre a ferramenta proposta

A explicação das possibilidades e capacidades da ferramenta proposta tem como finalidade engrossar a justificativa para o desenvolvimento. Esta ferramenta proposta pode de certa maneira levar vantagem na realização da descoberta de topologia de redes que estejam além de um roteador em relação à ferramenta REMOS.

Desde que o roteador permita a passagem de pacotes forjados e havendo conhecimento da faixa de endereços IP da rede e dos endereços IP das pontes de uma rede além deste roteador, é possível fazer a construção da topologia de pontes e em seguida através de uma única ponte ou até do próprio roteador de interligação fazer a comunicação para com todas as estações através do *echo_request* forjado.

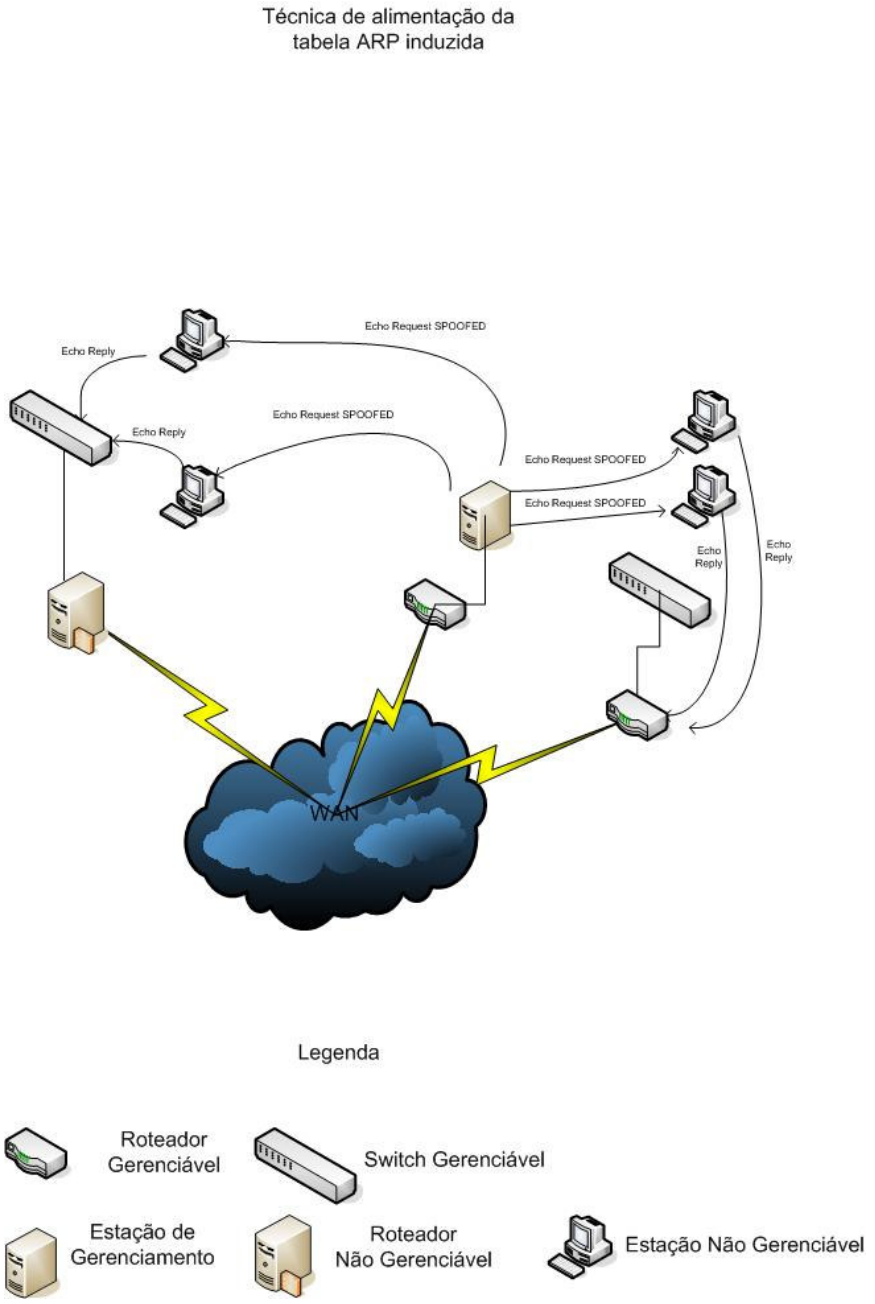


Figura 14 – Cenário representando atividade para tradução induzida MAC em IP.

Outra consideração a ser notada é a capacidade do funcionamento desta ferramenta em sub-redes com VLANs definidas em endereços IP e com roteadores não gerenciáveis. Se o roteador não é gerenciável via SNMP, então as informações MAC={IP} devem ser buscadas ora nas estações ou em quaisquer equipamentos gerenciáveis que façam parte da VLAN em questão. Nesse caso, a ferramenta pode encontrar um equipamento gerenciável em cada VLAN e forçar a desejada tradução. Esta é uma situação muito peculiar e que, de certa forma, é pouco tratada nas soluções de software tradicionais.

Essas características, ainda que não perfeitamente encontradas nos ambientes de testes reais, podem ser simuladas e utilizadas de forma aproximada nos testes que são relatados mais à frente neste capítulo.

7.2 - Designação dos ambientes e ferramentas auxiliares para comparação

A escolha das ferramentas de testes teve como critério a capacidade de descoberta da topologia e, por sua vez, a identificação dos nós folhas. Adotou-se também o critério de privilegiar um software que fosse o mais compatível possível com o parque de equipamentos (pontes, roteadores e repetidores) de rede ethernet.

A ferramenta eleita foi o 3COM Transcend. Esta foi escolhida por ser bastante utilizada e por ter sido de fácil acesso e o mais compatível possível com os equipamentos existentes para os testes. Isto quer dizer que se espera um resultado ótimo para o uso do Transcend, já que o parque de testes de *switches* e roteadores pertence ao mesmo fabricante deste software.

A versão do Transcend utilizada é 5.0 para UNIX, em plataforma SPARC SUN Ultra 10, 500 Mhz com 512 Mbytes de RAM e sistema operacional Solaris 8 Server.

A ferramenta desenvolvida durante a prova de conceito foi chamada de *ifip2mac*. A estação de gerenciamento tem arquitetura *pentium 4* com 2,8Ghz e 1 Gbyte de RAM sob o sistema operacional FreeBSD 5.4.

Com estas escolhas, pode-se fazer uma comparação sólida entre a ferramenta

desenvolvida ao longo dos estudos e uma ferramenta já homologada e conhecida no mercado e nos ambientes de redes gerenciáveis. Supostamente, os resultados destas comparações indicam a validade do estudo em questão e sugerem discussões de como se encontrar um método ideal para descobrir o conjunto solução das relações MAC = {porta.Er} e MAC = {IP}.

7.3 - Execução dos Testes

Os testes foram realizados em 4 cenários selecionados conforme as descrições da seção 6.1, sendo eles:

- Sub-rede IP não segregada com roteador gerenciável
- Sub-rede IP não segregada com roteador não gerenciável
- Sub-rede IP segregada com roteador gerenciável
- Sub-rede IP segregada com roteador não gerenciável

A localização da estação de gerenciamento é importante para o melhor entendimento de como se trataram os testes.

Os testes aplicaram-se a estes ambientes que são cenários dentro da rede PUCSPNet como pode-se visualizar na figura abaixo.

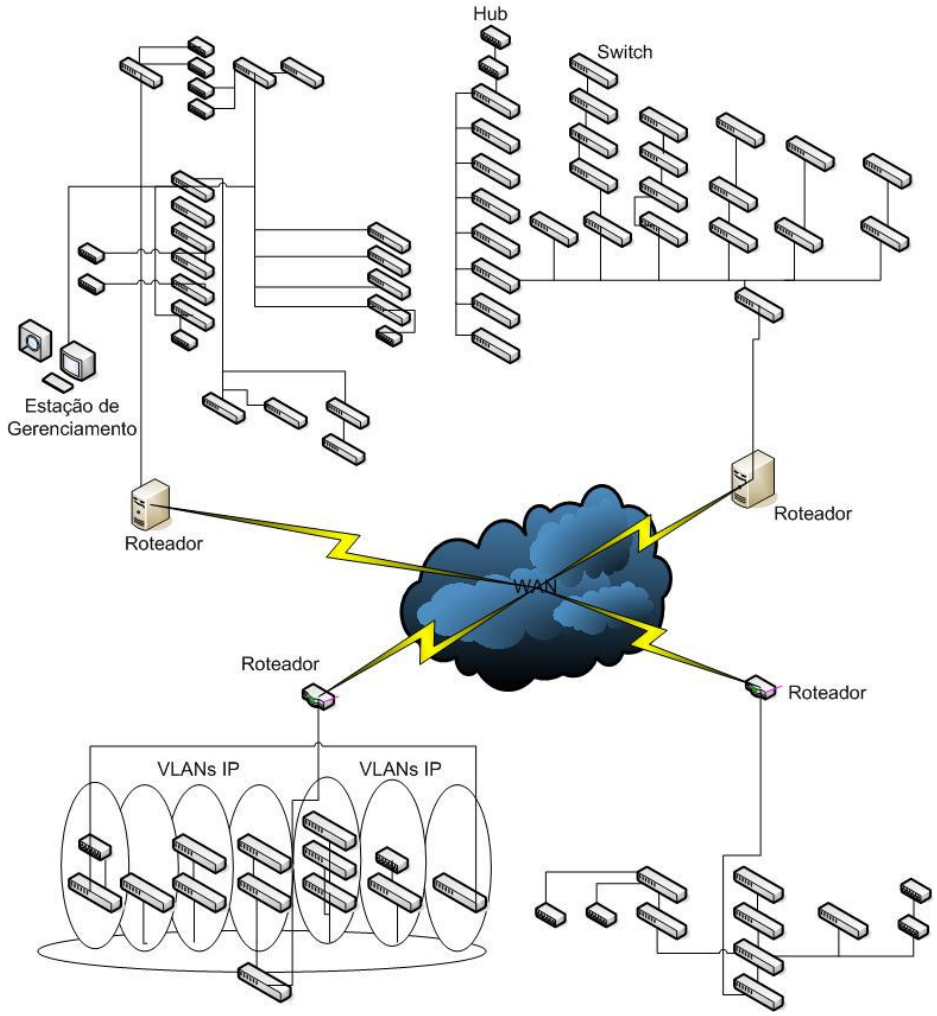


Figura 15 – Os quatro ambientes e o posicionamento da estação de gerenciamento.

7.3.1 - Cenário 1: Sub-rede IP não segregada com roteador gerenciável

A sub-rede IP não segregada se diferencia das demais pelo fato de conter estações e equipamentos de redes pertencentes ao mesmo domínio de rede ou *broadcast* nível 3, incluindo a existência de um roteador de saída gerenciável. Desta forma, se uma estação tem endereço 10.2.1.5 e possui máscara 255.255.255.0, então a ponte ou equipamento mais

próximo deve também ter uma interface que pertença à rede 10.2.1.0 com máscara 255.255.255.0.

Com isto, percebe-se que a determinação IP e MAC se torna mais ágil e eficiente, muito embora a maioria dos administradores de rede não adote esta configuração de rede por razões de segurança e privacidade das redes de gerenciamento.

Esta rede de testes pertence ao *backbone* da PUCSPnet cujas características atendem a estas especificações e apresenta uma quantidade expressiva de equipamentos como pode ser vista na tabela 6 abaixo.

Tabela 6 – Equipamentos da sub-rede IP não segregada usando roteador gerenciável.

Equipamentos	***Quantidade de equipamentos***	***Equipamentos Gerenciáveis***	***Total de portas nos equipamentos***
Pontes	16	16	388
Repetidores	3	0	72
Estações conhecidas	180	0	187 (placa de rede)

Além destes valores, deve-se considerar a existência da VLAN IP em cada uma das interfaces dos equipamentos de núcleo desta rede. Este fator deve ser considerado, pois com VLANs definidas nas interfaces IP dos equipamentos de núcleo, torna-se impossível fazer a tradução ARP local para um IP quando a estação cliente (quem executa a requisição ARP) não se encontra ligado à mesma VLAN da estação ao qual se deseja traduzir.

O fato de existirem VLANs não significa que as sub-redes destas VLANs sejam segregadas em relação aos equipamentos gerenciáveis e os computadores. Ocorre que, dentro de cada VLAN, os computadores e equipamentos gerenciáveis pertencem à mesma sub-rede IP. Por isso esta rede foi definida como rede não segregada.

A rede abordada pode ser visualizada na figura a seguir.

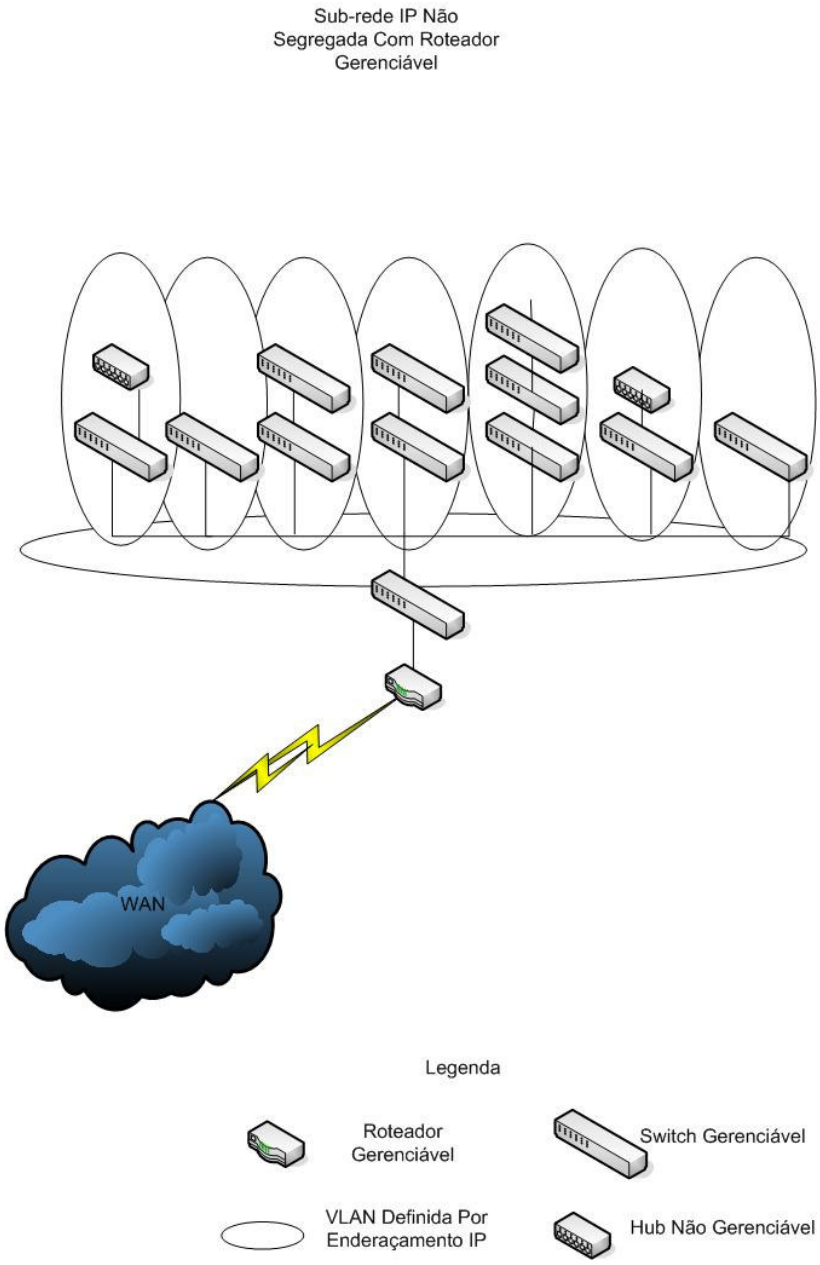


Figura 16 – Sub-rede IP não segregada com roteador gerenciável para testes

Foram realizados testes com as duas ferramentas relacionadas e assim os resultados obtidos estão apresentados a seguir. Para esta rede sabe-se que existem 180 estações com 187 interfaces de rede, das quais na fase de testes estavam ativas 88. Desse modo, o resultado esperado para a descoberta de topologia é que sejam listados 88 endereços MAC.

7.3.1.1 - Resultados utilizando a ferramenta ifip2mac

Para a execução da ferramenta foi necessária uma fase preliminar de descoberta de equipamentos gerenciáveis que acarretou um acréscimo de tempo, cerca de 50 s para descobrir todas as pontes gerenciáveis. A localização da estação de gerenciamento era remota, isto é através de uma rede *frame relay* passando por dois roteadores como descrito na figura 15.

Após a descoberta, teve-se um total de 2 min e 50 s para a descoberta de todos os 88 endereços MAC, considerando a identificação de endereços IP para suas interfaces. Como era de se esperar, as portas dos repetidores não foram identificadas. Portanto, os endereços MAC foram encontrados em interfaces de pontes e 92 endereços IP.

Assim, as relações MAC = {porta.Er} e MAC ={IP} foram obtidas com sucesso para este método em uma rede homogênea como a apresentada. Atenta-se para o fato da existência de mais de um endereço IP relacionado a um mesmo endereço MAC, caracterizando endereços IP *alias*.

7.3.1.2 - Resultados utilizando a ferramenta 3COM Transcend

Utilizando esta ferramenta gastou-se um tempo prévio de execução para se cadastrar todos os equipamentos gerenciáveis. A estação executando a ferramenta foi colocada junto à rede local, isto é, conectada diretamente em uma das VLANs em questão. O tempo total de execução, não considerando esta fase prévia, foi de 34 s. No momento da execução havia 79 interfaces de rede ativas.

Este tipo de ambiente se mostrou favorável para o uso desta ferramenta. De maneira excelente foram encontrados todos 79 MAC, 83 IP e suas interfaces.

As relações MAC = {porta.Er} e MAC = {IP} foram obtidas com sucesso, lembrando, mais uma vez, que nuvens de repetidores não gerenciáveis foram ignoradas.

7.3.2 - Cenário 2: Sub-rede IP não segregada com roteador não gerenciável

Esta rede local de testes interliga os setores administrativos dentro da PUCSPnet. Em sua grande maioria ela é constituída de repetidores não gerenciáveis, o que de certa forma dificulta a determinação da localidade de grande parte dos computadores. Outra característica desta rede é o serviço de DHCP, que não será abordado neste trabalho.

Em termos de elementos, a rede é constituída pelos equipamentos listados na tabela 5.

Tabela 5 – Equipamentos da sub-rede não segregada com roteador não gerenciável.

Equipamentos	***Quantidade de Equipamentos***	***Equipamentos Gerenciáveis***	***Total de portas nos Equipamentos***
Pontes	15	15	370
Repetidores	11	0	240
Estações conhecidas	574	0	574 (placa de rede)

Outro dado essencial a ser exigido é o número de estações existentes na rede no momento de execução dos testes. Nesta ocasião anotou-se a existência de 574 estações.

O roteador desta sub-rede é uma estação servidora executando roteamento de pacotes IP em um sistema operacional Linux. Geralmente, neste tipo de sistema não são habilitados agentes ou aplicações servidoras de informações SNMP nestes roteadores de borda. A topologia de tal rede pode ser visualizada através da figura 17 a seguir.

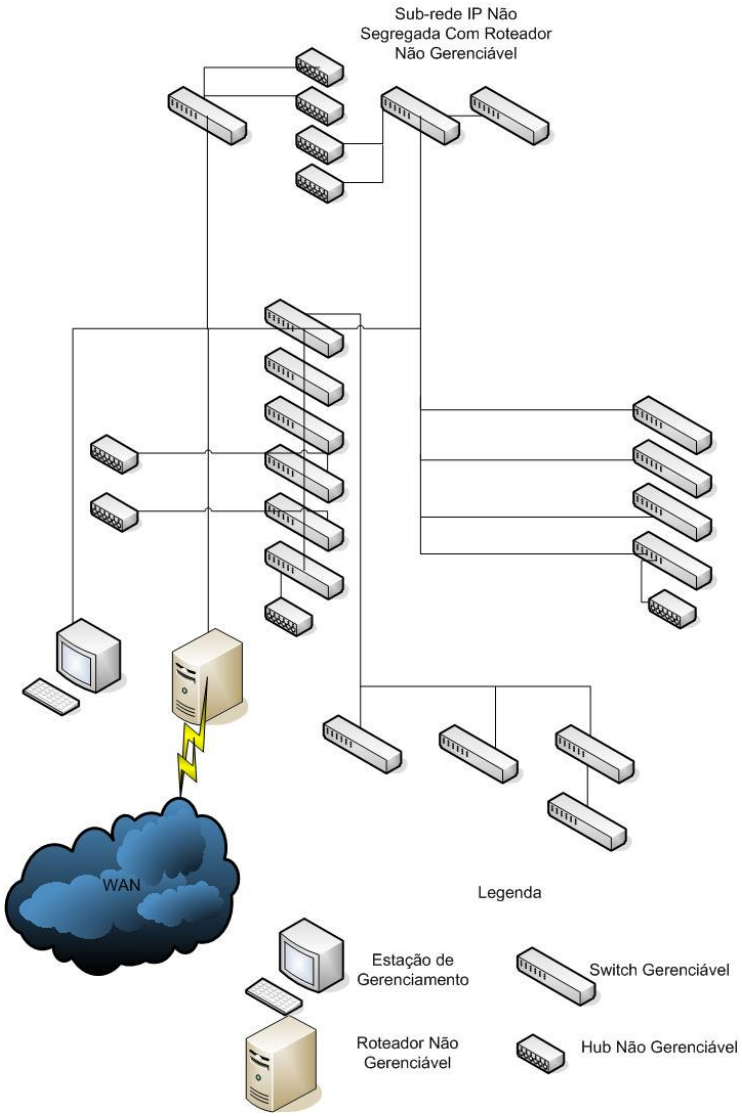


Figura 17– Sub-rede IP não segregada com roteador não gerenciável para testes.

A estação de gerenciamento para este cenário também faz parte da rede local onde foram executados testes com as ferramentas ifip2mac e 3Com Transcend, cujos resultados estão apresentados a seguir. No momento da realização dos testes estavam ativos, respondendo ao ICMP *echo_request,* um total de 534 computadores dos 574 conhecidos.

7.3.2.1 – Resultados utilizando a ferramenta ifip2mac

Para a execução da ferramenta houve um consumo de tempo de 4 min e 3 s. Este tempo final engloba a descoberta de todas as pontes gerenciáveis da rede em questão, bem como suas interligações e a busca dos conjuntos soluções desejados. Ao final da execução foram obtidos todos os 534 endereços MAC e todos os endereços IP em suas respectivas portas das pontes. Mais uma vez, as portas ou interfaces dos repetidores não foram identificadas, haja vista que estas não eram gerenciáveis. Neste caso, 221 endereços MAC foram encontrados em interfaces de pontes, mas que estavam diretamente ligados ao que se pode chamar de nuvens de rede ethernet. Como já se conhecem, nestes casos estas nuvens são os repetidores não gerenciáveis.

Portanto, as relações MAC = {porta.Er} e MAC ={IP} foram identificadas com sucesso neste método em uma rede homogênea como a apresentada.

7.3.2.2 - Resultados utilizando a ferramenta 3COM Transcend

Utilizando a ferramenta 3Com Transcend gastou-se um tempo prévio de execução para se cadastrar todos os equipamentos gerenciáveis, assim como ocorreu também na execução do ifip2mac. Este tempo foi igualmente ignorado por não servir como variável de comparação. O tempo de execução para a descoberta da solução foi de 46 s.

De maneira satisfatória foram encontrados todos 534 MAC e as portas. Desta forma as relações MAC = {porta.Er} foram atendidas com sucesso para uma rede homogênea sem a presença de um roteador MIB-II. Mais uma vez, vale lembrar a desconsideração dos

repetidores, que não foram identificados pela ferramenta e novamente podem ser considerados como pontos críticos neste estudo de descoberta de topologia.

Ao concluir os testes com o 3COM Transcend notou-se a falha da ferramenta em traduzir os endereços do nível físico (ethernet) para o nível lógico (IP), o que de fato era um dos objetivos dos testes.

7.3.3 Cenário 3: Sub-rede IP segregada com roteador gerenciável

A rede segregada com roteador gerenciável dentro do ambiente da PUCSPnet tem um pequeno número de pontes gerenciáveis e poucos repetidores, o que de certa forma deveria colaborar no processo de descoberta de topologia. Entretanto, o que se torna ruim para este processo é justamente o fato da rede segregada exigir que a comunicação SNMP entre a estação de gerenciamento e os equipamentos atravesse um roteador comum as duas sub-redes.

O número de 127 estações com 129 placas de rede de certa forma indica a menor rede utilizada até aqui, mas que por sorte tinha 86 estações ativas contendo 88 interfaces de rede respondendo ao *echo_request* no momento de execução dos testes. A simplicidade desta topologia pode ser vista na tabela 7 e figura 19.

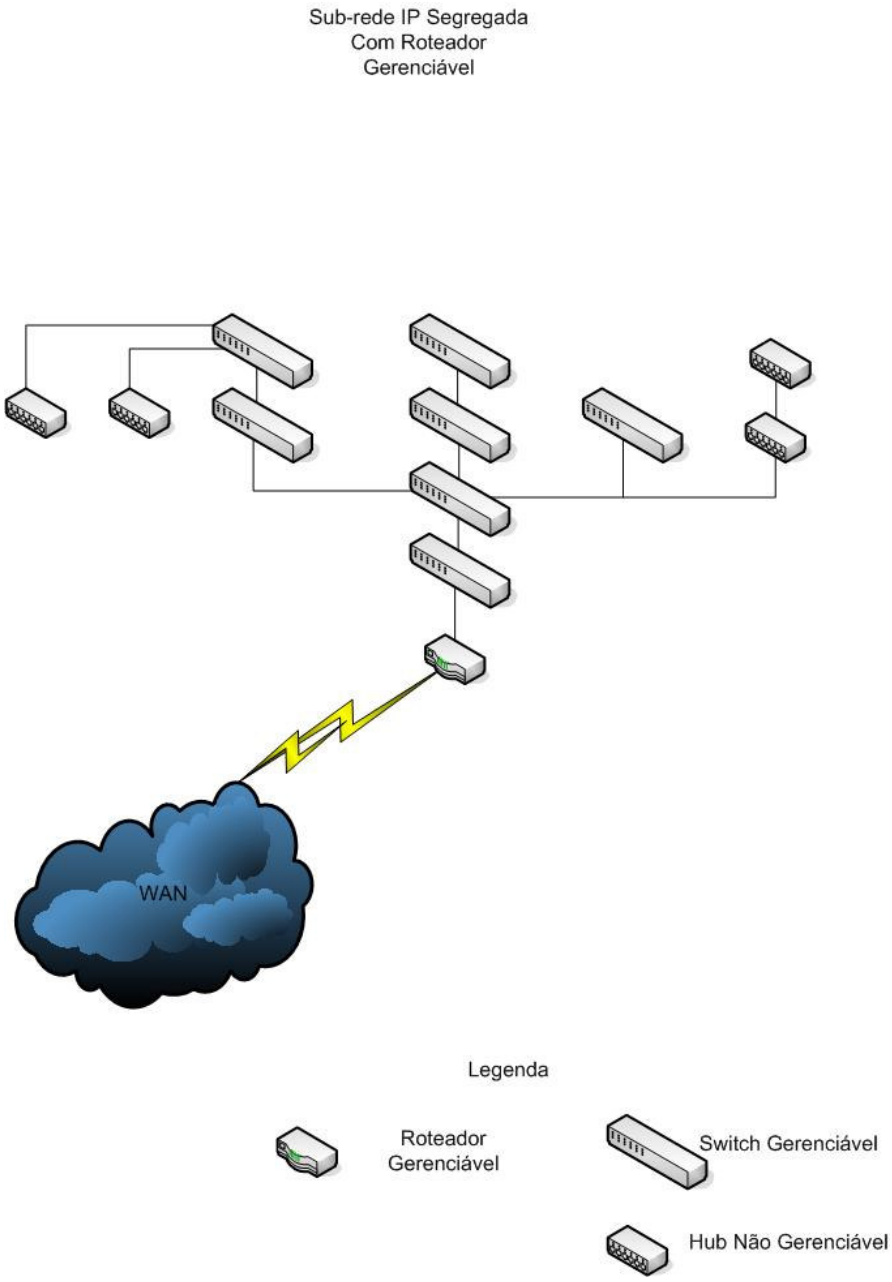


Figura 19 – Sub-rede IP segregada com roteador gerenciável para teste

Tabela 7 – Equipamentos da sub-rede segregada com roteador gerenciável.

Equipamentos	*Quantidade de equipamentos*	*Equipamentos Gerenciáveis*	*Total de portas nos equipamentos*
Pontes	7	7	176
Repetidores	4	0	96
Estações conhecidas	127	0	129

Os resultados de testes de cada uma das ferramentas são demonstrados a seguir.

7.3.3.1 Resultados utilizando a ferramenta ifip2mac

Como já realizado nos outros testes, a estação que roda a ferramenta fica localizada fora da rede local. Após o cadastramento correto dos endereços de rede, roteador principal e também de suas pontes, a descoberta teve-se um total de 2 min e 2 s para a descoberta de todos os 88 endereços MAC. Neste caso em específico a relação MAC={IP} foi obtida através de consultas SNMP ao roteador já que este é o único equipamento conectado em ambas redes e a ferramenta permite indicar (parâmetro de entrada) quem deve resolver esta consulta. Com isso, além da descoberta de todos os endereços MAC, foi possível concluir com sucesso todas as 88 relações MAC={IP}.

7.3.3.2 Resultados utilizando a ferramenta 3COM Transcend

Mais uma vez a ferramenta tomou um tempo prévio de trabalho manual de cadastramento dos equipamentos gerenciáveis e a localização da estação que executa o Transcend é a rede local. Para um período de 27 s foram obtidas todas as 88 relações MAC = {porta.Er} e todas relações MAC = {IP}. Desta vez a ferramenta mostrou–se viável, pois o fato de se considerar o roteador como elemento de rede foi imprescindível para a tradução MAC em IP.

7.3.4 - Cenário 4: Sub-rede IP segregada com roteador não gerenciável

Há que se esperar que este ambiente seja o mais difícil para qualquer procedimento, pois como se sabe, todas as ferramentas ou consultam os roteadores ou as pontes e *switches* que estão na rede gerenciável. Este ambiente foi simulado no ambiente da PUCSPnet através da utilização da rede heterogênea com um roteador de borda em uma estação de plataforma Linux sem agentes SNMP ativos.

Uma desvantagem na rede proposta para teste é a existência de VLAN 802.1Q configurada em algumas pontes. Esta configuração excluiu 212 portas das 672 existentes já que o roteador para esta VLAN pertencia a uma outra sub-rede IP e protegida por um servidor Proxy e NAT que naturalmente não encaminha datagramas IP das estações clientes de fora para dentro e vice-versa.

No momento dos testes eram conhecidas 191 estações existentes nesta rede com 191

placas de rede, quando de fato 82 destas estações estavam ativas.

A rede heterogênea de testes pode ser visualizada na figura 18, juntamente com as informações de valores quantitativos da tabela que segue:

Tabela 8 – Equipamentos da sub-rede segregada com roteador não gerenciável.

Equipamentos	***Quantidade de equipamentos***	***Equipamentos Gerenciáveis***	***Total de portas nos equipamentos***
Pontes	28	28	672
Repetidores	2	0	48
Estações conhecidas	191	0	191 (placas de rede)

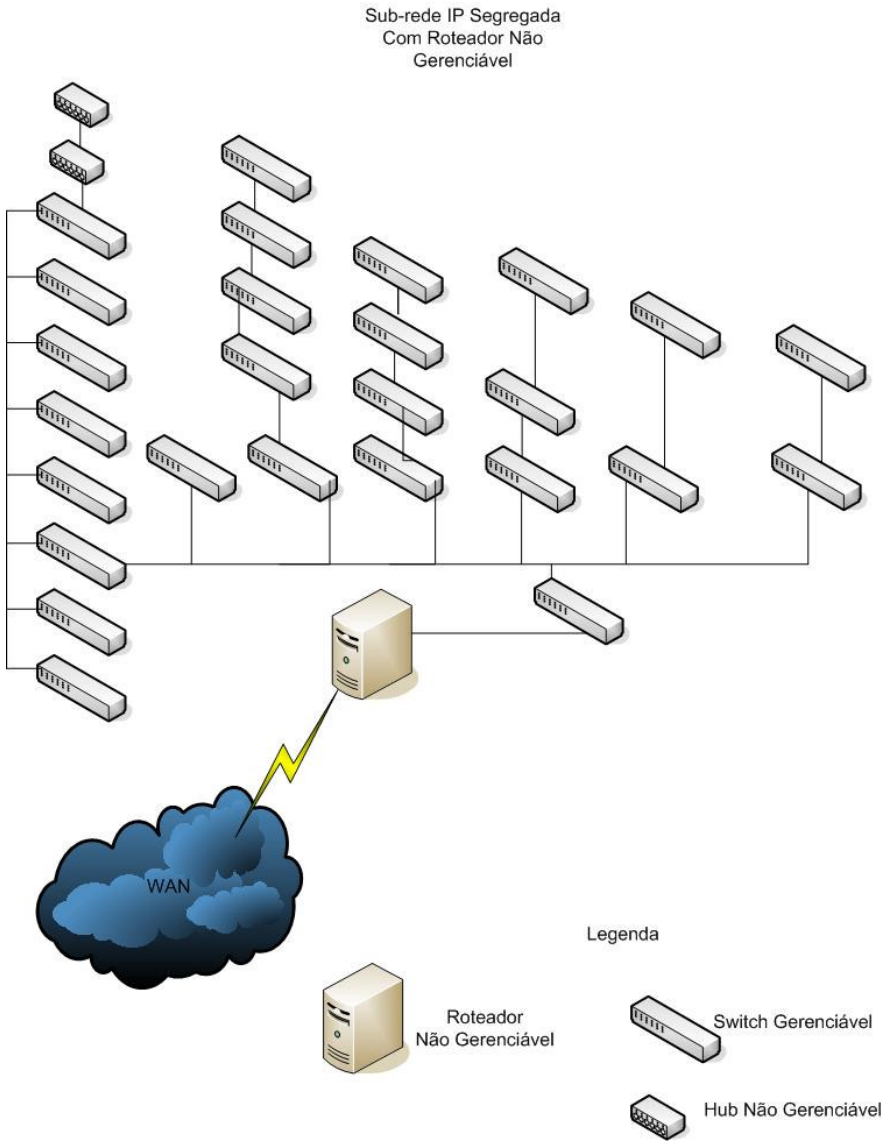


Figura 18 – Sub-rede segregada com roteador não gerenciável

7.3.4.1 - Resultados utilizando a ferramenta ifip2mac

Neste cenário a estação de gerenciamento esta remotamente localizada, atravessando dois roteadores como descrito na figura 15. Após a inclusão dos dados referentes aos equipamentos de rede no arquivo de configuração, pode-se iniciar a descoberta. O processo de descoberta mais derivação dos nós folhas consumiu um tempo total de 2 min e 30 s.

Foram descobertos todos os 82 endereços MAC ativos no momento da execução, mas por outro lado não foram encontradas as relações MAC={IP}.

7.3.4.2 - Resultados utilizando a ferramenta 3COM Transcend

Mais uma vez a ferramenta tomou um tempo prévio de trabalho manual de cadastramento dos equipamentos gerenciáveis. A localização da estação de gerenciamento mais uma vez é a rede local. A diferença aqui é que neste momento havia 86 placas de rede respondendo ao *echo_request.* O processo de descoberta durou 32 s e foram obtidas todas as relações MAC = {porta.Er}, ao todo 86, e nenhuma relação MAC = {IP}.

7.4 - Sumário dos resultados

Os testes para cada um dos ambientes foram realizados por um conjunto considerável de vezes. Entretanto como os resultados obtidos em cada uma das execuções não apresentaram variações, tornou-se mais prático escolher ao acaso um resultado para cada um dos ambientes. Esta escolha também foi realizada em razão dos valores obtidos terem sido representativos e também por conta de que o escopo deste estudo não é realizar uma abordagem estatística dos métodos discutidos.

Finalmente, os resultados apresentados levam a discutir a utilidade das ferramentas e qualificar a interferência de cada uma delas nos processos de descoberta e na obtenção dos dados finais. De maneira objetiva os resultados de cada um dos testes anteriormente foram dispostos nas tabelas 9,10,11 e 12 com intuito de melhor exibir os resultados alcançados.

Tabela 9 – Síntese dos resultados obtidos para sub-rede IP não segregada com roteador gerenciável.

Tipo de teste	**Transcend**	**Ifip2mac**
Numero de IP ativos	83	92*
Numero de MAC ativos	79	88
Relações MAC={IP}	83	92
Relações MAC={porta.Er}	79	88

***OBS:Existência de IP alias**

Tabela 10 – Síntese dos resultados obtidos para sub-rede não segregada com roteador não gerenciável

Tipo de teste	**Transcend**	**Ifip2mac**
Numero de IP ativos	534	534
Numero de MAC ativos	534	534
Relações MAC={IP}	0	534
Relações MAC={porta.Er}	534	534

Tabela 11 – Síntese dos resultados obtidos para sub-rede IP segregada com roteador gerenciável.

Tipo de teste	**Transcend**	**ifip2mac**
Numero de IP ativos	88	88
Numero de MAC ativos	88	88
Relações MAC={IP}	88	88
Relações MAC={porta.Er}	88	88

Tabela 12 – Síntese dos resultados obtidos para sub-rede IP segregada com roteador não gerenciável.

Tipo de teste	**Transcend**	**Ifip2mac**
Numero de IP ativos	86	82
Numero de MAC ativos	86	82
Relações MAC={IP}	0	0
Relações MAC={porta.Er}	86	82

7.5 – Análise dos Resultados

Ao final da execução dos testes foi possível analisar as vantagens do método de tradução induzida através dos resultados do cenário 2. Neste ambiente foram encontrados com sucesso as relações MAC={IP} enquanto que através dos métodos tradicionais como os da ferramenta Transcend não foi possível se obter nenhuma relação MAC={IP}.

Estes resultados apontam para a tendência que se discutia nos capítulos anteriores, onde se propôs que este método de comunicação forjada deveria ser vantajoso em redes sem elementos de roteamento gerenciáveis.

No cenário 4 (rede IP de gerenciamento segregada sem roteador gerenciável) percebe-se que a tradução ARP (MAC={IP}) é muito prejudicada pelo fato de não existir nenhum equipamento gerenciável que faça parte da rede IP dos equipamentos e da rede de nós folhas ao mesmo tempo. Nestas situações, para qualquer uma das ferramentas, a solução é procurar um equipamento gerenciável para o segmento IP das estações. Caso seja encontrado algum equipamento gerenciável na mesma rede IP das estações, então se pode a partir deste equipamento realizar todas as traduções.

Outro fator que pode ser considerado é a validade desta técnica para descoberta de topologia além de roteadores. Desde que configurados para este propósito, estes roteadores podem permitir que o tráfego forjado seja repassado.

8 – Considerações Finais

Após o término da fase de testes dos métodos de obtenção dos nós folhas pôde-se concluir e identificar as situações e aspectos tanto negativos quanto positivos a respeito dos processos de descoberta de topologia física e de estações que utilizam IP dentro de redes gerenciáveis ethernet.

Esse capítulo visa analisar a proposta do método de tradução induzida através da ferramenta *ifip2mac* contra a proposta convencional observada nos testes para a ferramenta Transcend (3Com, 1998).

8.1 – Métodos de descobertas e ambientes considerados críticos.

Para os ambientes de testes usados pôde-se identificar que alguns dos cenários de redes apresentam detalhes ou empecilhos capazes de contribuírem para o mau funcionamento dos algoritmos de descoberta dos nós folhas.

O ambiente que se mostrou menos problemático foi o da sub-rede IP não segregada contendo equipamentos de comunicação (pontes) e roteadores gerenciáveis. Nesta classe de redes, não há problemas, como de fato já apontava a intervenção teórica.

Entretanto, nos demais ambientes, como os segregados e os sem roteadores gerenciáveis apresentaram-se dificuldades para determinadas condutas de busca dos nós folhas.

As redes sem elementos de roteamento gerenciáveis foram boas justificativas para o

uso do método induzido de descoberta de nós folhas como bem mostraram os testes com a ferramenta ifip2mac. Nestas situações, a técnica de descoberta induzida se faz valer da possibilidade de influenciar automaticamente a comunicação de equipamentos. O fato é que, em sua configuração convencional, a ferramenta Transcend não pôde automaticamente resolver os conjuntos soluções para os nós folhas em cenários como estes, pois ao que tudo indica, suas informações de tradução são todas buscadas em roteadores gerenciáveis.

Analisando os problemas encontrados nos testes, nota-se que grande parte das dificuldades se resume na incapacidade da estação de gerenciamento em conseguir acessar aos dados que informem sobre a topologia da rede.

Para as situações em que as redes estão subdivididas e os roteadores não são gerenciáveis vê-se que a solução alternativa de contorno requer intervenção humana ou uso de algoritmos mais avançados que sejam capazes de identificar automaticamente tais configurações. Em outras palavras, a estação que faz a varredura deve ser hábil o suficiente para procurar um elemento gerenciável comum às redes IP que estão segmentadas. Caso este elemento não possa ser encontrado, então a plataforma de gerenciamento deve se tornar tal elemento, quando possível (isto significa que a estação tem conexão direta a esta rede). Com isso a estação passa a traduzir a tabela ARP para as redes segmentadas em questão.

O método da comunicação induzida foi proposto como alternativa para mostrar que este tem realmente uma técnica válida para algumas situações críticas, já que é mais fácil obter a tabela ARP de um elemento que esteja ao alcance de comunicação (SNMP) do que tentar fazer com que a estação de gerenciamento torne-se automaticamente um elemento ligado diretamente a diversas redes.

Para finalizar, deve-se ressaltar que em todos ambientes, percebeu-se que a técnica de tradução induzida traz uma facilidade, pois esta alimenta as tabelas de encaminhamento das pontes existentes. A comunicação forjada faz com que as pontes tenham suas tabelas de encaminhamento preenchidas pelos endereços MAC das estações e possivelmente de outras pontes. Com isso a descoberta de topologia física torna-se mais fácil do ponto de vista dos teoremas da conexão simples e direta.

8.2 - Reconhecimento e tratamento de equipamentos não gerenciáveis

Em relação aos equipamentos não gerenciáveis, pouco foi comentado e, de fato, esta questão é menos frequentemente abordada em literaturas ou referências com ênfase em gerenciamento de redes.

Durante os estudos, pôde-se perceber que algumas situações podem indicar ou exibir rastros da existência de equipamentos não gerenciáveis.

Um exemplo convincente é o teorema da conexão compartilhada. Este identifica a posição de um equipamento não gerenciável quando este interliga dois outros segmentos de rede gerenciáveis. Neste aspecto, o teorema da conexão compartilhada resolve ou indica a posição de um equipamento não gerenciável, seja este uma ponte ou um repetidor.

Por outro lado, os métodos de descoberta de nós folhas construídos na ferramenta ifip2mac também podem ser úteis neste problema. Neste ângulo de visão não se deseja mais discutir como descobrir endereços e suas portas, mas sim como os valores de endereços e portas podem ajudar a esclarecer a topologia composta de equipamentos não gerenciáveis.

Para o caso de pontes não gerenciáveis, os dados a serem examinados são simples. Se o número de elementos do conjunto tabela de encaminhamento F_A^n={MACx,...} for > 1, ou seja, o conjunto não é unitário, então pode-se pressupor que a porta n do equipamento de comunicação A está ligando uma nuvem ethernet. Neste caso, um possível cenário é de que a porta n em questão deve representar uma interface física que conecta um equipamento não gerenciável no nível logo abaixo (nível da árvore do diagrama da topologia da rede), salvo algumas comprovações.

Se um endereço MAC pertence ao conjunto da tabela de encaminhamento da porta 2 do equipamento A (MAC$\in F_A^2$), então a interface associada pode tanto estar ligada diretamente a esta porta ou então estar ligada em outro equipamento que direta ou indiretamente esta conectada a esta porta. Por exemplo: conexao1=<A.porta2,B.porta1> e MAC$\in F_B^1$. Este

tratamento para determinação de níveis ou saltos entre um nó folha e o equipamento ao qual se está diretamente ligado não é simples.

Dessa forma, ainda existe um novo problema que reside no desconhecimento de quantos níveis de cascatas existem a partir desta porta. De maneira teórica, é possível que existam até 4 repetidores cascateados (restrição para *fast ethernet*) a partir da porta encontrada.

Enfim, esta técnica descrita acima se torna uma forma auxiliar para a determinação de equipamentos ou meios não gerenciáveis nas extremidades das redes. Enquanto isso, a maneira de se encontrar esses meios não gerenciáveis no núcleo da rede ainda deve ser feita através do uso do teorema da conexão compartilhada (Lowekamp, 2000) e que, de forma prática, é realizada através da ferramenta REMOS.

Nesta dissertação todas as considerações foram realizadas somente acerca de pontes gerenciáveis. Não foi objetivo incluir o tratamento para repetidores, porém os conceitos podem ser estendidos para englobar situações como estas.

Para os repetidores gerenciáveis pode-se obter na MIB *repeater* em cada instante qual é o último endereço que fora encaminhado através daquele repetidor. Já que o objeto possui uma única entrada, este terá seu valor constantemente alterado conforme as diferentes estações forem encaminhando seus pacotes através daquela porta. Concluindo, a identificação das conexões de um repetidor gerenciável deve ser feita através de uma leitura comparativa ao longo do tempo do objeto SNMP gerenciado do repetidor e assumir que ao menos duas estações estejam ativas no meio. Com isso, o objeto deve ter seu valor alternado entre os valores de MAC que estejam no meio compartilhando. Mas como não há dados que indiquem a existência de um meio não gerenciável abaixo de um repetidor. Isto ocorre pela natureza das informações que a MIB *repeater* dispõe, levando-se a afirmar que o segmento ligado a um repetidor (mesmo que gerenciável), constituiu-se em uma nuvem ethernet.

Estas colocações envolvem muito mais considerações a respeito do histórico das informações e este será discutido a seguir.

8.3 - Tratamento histórico das informações

A manutenção e mineração histórica dos dados coletados não foram discutidas até o momento, pois não fazia parte do escopo deste trabalho. Porém podem-se discutir algumas aplicações interessantes.

Em primeiro lugar, a topologia e disposição da rede podem ser constantemente alteradas ou ainda, como é comum, passar por transformações decorrentes do crescimento de pontos.

Isto sugere que o armazenamento ao longo de um histórico dos dados pode vir a auxiliar o gerenciamento de mudanças, identificando o instante de alteração de posicionamento de um equipamento na rede, ou também a entrada ou saída de um equipamento da rede.

Outra questão compreende a formulação de um modelo de sistema de dados que armazene todas estas condições críticas apresentadas, e não somente seja uma coleção de dados no qual se tenha que fazer um estudo complexo para que se possam concluir problemas ou questões quaisquer relativas aos nós da rede. Exemplo disso é a criação de um modelo de dados que seja capaz de armazenar problemas no uso da rede quando, por exemplo, duas estações provoquem conflito no uso de endereço IP. O sistema de dados deve fornecer o momento e a localização em que se identificou o conflito.

Uma última consideração é a freqüência de alimentação da base de dados. Esta deve ter um valor que chegue a um senso comum, admitindo qual a melhor estimativa para o ciclo de execução das leituras (via ifip2mac) dos pontos de nós folhas da rede.

Assim, concluí-se que a melhor forma para atender a tais colocações, vem a ser o uso de um banco de dados. Deseja-se que uma proposta futura para incorporação de banco de dados à ferramenta ipif2mac seja realizada para que esta se apresente como uma ferramenta que atende às expectativas de tantas outras encontradas no mercado atualmente.

8.4 – Conclusão

Ao fim do trabalho concluí-se que o método proposto de descoberta induzida pode vir a ser uma forma auxiliar para determinação da topologia no caso em específico citado nos testes.

A qualidade do método se traduz nos testes que comprovaram o poder do método comunicação induzida (presente na ferramenta ifip2mac) quando utilizada em ambientes críticos para a descoberta da topologia física e de rede mediante um conjunto pré-conhecido de dados de entrada.

Vê-se também que, apesar do método da tradução induzida ser simples, existe pouca referência a esta proposta em literaturas deste segmento do conhecimento de gerenciamento de redes. Assim, quer-se concluir que os estudos são válidos na medida em que comprovam estas afirmações e permitem caminhos futuros que se utilizem destas construções e resultados para um refinamento e melhoria da descrição dos diagramas físicos de redes locais.

8.5 – Dificuldades encontradas

As principais dificuldades durante a realização deste estudo foram em relação ao desenvolvimento da ferramenta de prova de conceito. Isto se nota pela quantidade de variáveis envolvidas que algumas vezes traziam problemas para a obtenção dos resultados.

Dentre estas dificuldades, pode-se citar o bloqueio dos *firewalls* para pacotes forjados. Pode-se também citar a existência de VLANs com definição via IP, o que torna a execução da

ferramenta de maneira muito fracionada. Em suma, detalhes técnicos encontrados na prática são sempre fatores que contribuem para o atraso dos testes.

Uma última consideração impeditiva é a falta de documentação das ferramentas de descoberta de topologia, que na grande maioria das vezes não disponibilizam os algoritmos para a comunidade tanto acadêmica quanto comercial.

9 - Bibliografia

3Com **Transcend Network Control Services** Versão 5.0 para UNIX Solaris 2.5.1. 1998, Santa Clara, CA. 3Com Corporation. Sistema Solaris 8 Sun Ultra 10 UltraSparc IIi 44- Mhz 512 MB RAM. 1 CD-ROM.

BERNAL, V.;.**Sistema de diagnóstico: O modelo de configuração**. Relatório Técnico. Laboratório de Sistemas Integráveis – POLI-USP. Dezembro de 2000.

BIERMAN, A. & Jones, K. **Physical topology MIB**. The Internet Engineering Task Force. Request for comments 2922 . Disponível em : http://www.ietf.org/rfc/rfc2922.txt?number=2922 . Acesso em : 15 de março de 2005.

BREITBART, Y.; GAROFALAIS, M.; MARTIN, C.; RASTOGI, R.; SESHADRI, S.; e SILBERSCHATZ, A. .**Topology discovery in heterogeneous IP networks**. CASE, J. D.; FEDOR, M.; SCHOFFSTALL, M. L.; DAIN, J. **Simple Network Management Protocol**. The Internet Engineering Task Force. Request for comments 1157. Disponível em : http://www.ietf.org/rfc/rfc1157.txt?number=1157 . Acesso em : 15 de março de 2005. Proceedings. Apresentado em INFOCOM, 2000, Tel-Aviv.

COMER, D. E. et al. **Interligação em rede com TCP/IP**. Volume II. Rio de Janeiro : Editora Campus, 1999.

DECKER, E.; LANGILLE, P.; RIJSINGHANI A.; MCCLOGHRIE., K. **Definitions of Managed Objects for Bridges**. The Internet Engineering Task Force. Request for comments 1493. Disponível em : http://www.ietf.org/rfc/rfc1493.txt?number=1493 . Acesso em : 15 de março de 2005.

GKANTSIDIS, C. **Experiment and Learn to Discover Network Topology**. Georgia : Institute of technology, 1999. (Relatório Técnico).

GRAAF, K.; ROMASCANU, D.; McMASTER, D.; McCLORGHRIE K.; .**Definitions of Managed Objects for IEEE 802.3 Repeater Devices using SMIv2**. The Internet Engineering Task Force. Request for comments 2108. Fevereiro de 1997. Disponível em :

http://www.ietf.org/rfc/rfc2108.txt?number=2108 . Acesso em : 15 de março de 2005.

KUROSE, J. F. et al. **Redes de Computadores e a Internet**. Edição 1. São Paulo : Addison-Wesley, , 2003.

LOWEKAMP, B**. Discovery and Application of Network Information**. 2000. Phd Thesis - Computer Science Department School of Computer Science Carnegie Mellon University, Pittsburgh.

LOWEKAMP, B.; SUBHLOK, J.; GROSS, T.; STEENKISTE, P.; SHUTERLAND, D.; DEWIT, T.; MILLER, N. **The Architecture of the Remos System.** Proceedings of the 10th IEEE International Symposium on High Performance Distributed Computing. IEEE Computer Society .Washington, DC, USA . 2001. 252 Páginas

LOWEKAMP, B.; O'HALLARON , D. R.; e GROSS., T. R. .**Topology Discovery for Large Ethernet Networks. Proceedings**. In : ACM SIGCOMM 2001 ACM Press, 2001, San Diego - California.

MANJUNATH, D.; BAJAJ, K**. Intranet Topology Discovery Using Untwine**. New-Delhi : Indian Institute of Technology, 2002. (Relatório Técnico).

MCCLOGHRIE, K. & ROSE, M.. **Management Information Base – II** . The Internet Engineering Task Force. Request for comments 1213. Disponível em : http://www.ietf.org/rfc/rfc1213.txt?number=1213 . Acesso em : 15 de março de 2005.

PERLMAN, R., **Interconnections** : Bridges and Routers. Boston : Addison-Wesley, 1992. 375p.

Project ARGUS: **Network topology discovery, monitoring, history, and visualization**. Disponível em: <http://www.cs.cornell.edu/boom/1999sp/projects/Network%20Topology/topology.html> Acesso em 02/04/2005.

Project OCTOPUS: **Network topology discovery**. Disponível em: <http://www.cs.cornell.edu/cnrg/topology_aware/topology/Default.html> Acesso em 02/04/2005.

SEDGEWICK, R. **Algorithms in C**. Edição 3. Boston : Addison-Wesley, 1998.

SPURGEON, E. C. **Ethernet: The Definitive Guide**. Edição 1. O'Reilly. 2000 520 p.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, RMON 1 and 2**. Edição 3. Boston : Addison-Wesley, 1999. 619p.

TANENBAUM, A. S. **Computers Networks**. 3 Ed. New Jersey. Prentice Hall.1996. 813 p.

WALDBUSER, S.; COLE, R; KALBFLEISCH, C.; ROMASCANU, D. **Introduction to the Remote Monitoring (RMON) Family of MIB Modules**. The Internet Engineering Task

Force. Request for comments 3577. Disponível em : http://www.ietf.org/rfc/rfc3577.txt?number=3577 . Acesso em : 15 de março de 2005.

Anexo A
Ping Forjado

```
#include <stdio.h>
#include <linux/ip.h>
#include <linux/icmp.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <stdlib.h>
#include <unistd.h>
#include <arpa/inet.h>
#define ETH_P_IP 0x800

u_short in_cksum(unsigned short *addr, int len)
{
       u_short *word = (u_short*) addr;
       u_long acc = 0;

        while((len -= 2) >= 0)
                       acc += *(word++);

        return ~(*(u_short*)&acc + *((u_short*)&acc + 1));
}

int main (int argc, char **argv)
{
  struct iphdr *ip;
  struct icmphdr *icmp;
  struct sockaddr_in addr;
  //
  struct sockaddr_in spoof;
  //
  int sock, optval, result;
  char *packet, *buffer;
   /*   int s; */

  if(argc != 3) {
              fprintf(stderr,"usage: %s <ip_source_spoof> <ip_destination>\n",argv[0]);
              return(1);
               }
```

```
   ip   = (struct iphdr *) malloc(sizeof(struct iphdr));
   icmp = (struct icmphdr *) malloc(sizeof(struct icmphdr));
   packet  = (char *) malloc(sizeof(struct iphdr) + sizeof(struct icmphdr));
buffer  = (char *) malloc(sizeof(struct iphdr) + sizeof(struct icmphdr));
   addr.sin_family = AF_INET;
   addr.sin_addr.s_addr = inet_addr(argv[2]);
   //
   spoof.sin_family = AF_INET;
   spoof.sin_addr.s_addr = inet_addr(argv[1]);
   //
   ip = (struct iphdr *) packet;
   /* ip->frag_off |= htons(0x2000); */
   ip->ihl     = 5;
   ip->version = 4;
   ip->tos     = 0;
   ip->tot_len = sizeof(struct iphdr) + sizeof(struct icmphdr);
   ip->id      = htons(getuid());
   ip->ttl     = 255;
   ip->protocol = IPPROTO_ICMP;
   ip->daddr    = addr.sin_addr.s_addr;
   //
   ip->saddr    = spoof.sin_addr.s_addr;
   //
   ip->check    = in_cksum((unsigned short *)ip, sizeof(struct iphdr));
   icmp = (struct icmphdr *) (packet + sizeof(struct iphdr));
   icmp->type = ICMP_ECHO;
   icmp->code = 0;
   icmp->un.echo.id = 0;
   icmp->un.echo.sequence = 0;
   icmp->checksum = 0;
   icmp->checksum = in_cksum((unsigned short *)icmp,sizeof(struct icmphdr));

   if((sock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP)) < 0) {
            fprintf(stderr,"error opening raw socket.\n");
            return(-1);
             }

      setsockopt(sock, SOL_IP, IP_HDRINCL, &optval, sizeof(int));
      /* s = socket(AF_PACKET, SOCK_RAW, htons(ETH_P_IP)); */




      sendto(sock,packet,ip->tot_len,0,(struct sockaddr *)&addr,sizeof(struct sockaddr));
//    result = recv(sock,buffer,sizeof(struct iphdr)+sizeof(struct icmphdr),0);

//    if(result>-1) {

//            printf("%d: ICMP ECHO Reply...\n",result);
//            /* printf("%s\n",buffer);  */
//                 }
```

```
        close(sock);
        return(0);
}
```

Anexo B
Módulos da ferramenta ifip2mac para descoberta de topologia

################################main..sh##############################

```
!#/usr/local/bin/bash
echo "Forcando comunicacao entre pontes..."
./topologia/batch_fping.sh
echo "Realizando varredura das tabelas de bridge..."
./walk_mac_porta.sh
echo "Iniciando busca e montagem da topologia..."
cd topologia
./topologia.sh
echo "Verificando portas e enderecos fisicos..."
cd ..
./main_ifbond_mac.sh
echo "Finalizando a traducao entre MAC e IP..."
./ifbond_ip.sh $1 $2
```

################################walk_mac_porta.sh##############################

```
#!/usr/local/bin/bash
IFS='
'
switches=`cat switches.dat`
rm -f dados/*

 for i in $switches
do

snmpwalk -v 1 -c dlmots $i  mib-2.17.4.3.1.1.0 >> dados/enderecos_$i.dat
snmpwalk -v 1 -c dlmots $i mib-2.17.4.3.1.2.0 >> dados/portas_$i.dat

   lixo=`cat dados/enderecos_$i.dat`
   for j in $lixo
      do
       echo  $j   |  awk  -F" = Hex-STRING:"  {'print  $1  $2'}  |  awk  -F"SNMPv2-SMI::mib-2.17.4.3.1.1.0"  {'print  $2'}    >>
dados/indice_mac_$i.dat
      done

       lixo2=`cat dados/indice_mac_$i.dat`
```

```
        for k in $lixo2
         do

           indice=`echo $k | awk -F" " {'print $1'}`
           mac=`echo $k | awk -F" " {'print $2 $3 $4 $5 $6 $7'}`
           porta=`grep $indice dados/portas_$i.dat | awk -F"INTEGER:" {'print $2 '}`
           echo $porta $mac >> dados/porta_mac_$i.dat
         done
echo -n "."
echo -ne \\a
done
```

################################topologia.sh#####################################

```
#!/usr/local/bin/bash
IFS='
'
rm -f ../dados/switches_mac*
rm -f ../dados/portas_excluidas*

cat ../modelo_switches.dat > ../switches.dat

localhost=`head -n 1 ../switches.dat`
sublocalhost=`tail -n 1 ../switches.dat`
switches=`grep -v $localhost ../switches.dat`

./fping $sublocalhost $localhost
./fping $sublocalhost $localhost

 mac=`snmpwalk -c dlmots -v1 $sublocalhost mib-2.4.22.1.2 | grep $localhost | awk -F"STRING:" {'print $2'} | awk -F" " {'print $1'}`
 mac=`./mac.pl $mac`
 echo $mac $localhost >> ../dados/switches_mac.dat


for i in $switches
do
  ./fping $localhost $i
  ./fping $i $localhost
  mac=`snmpwalk -c dlmots -v1 $localhost mib-2.4.22.1.2 | grep $i | awk -F"STRING:" {'print $2'} | awk -F" " {'print $1'}`
  mac=`./mac.pl $mac`
  echo $mac $i >> ../dados/switches_mac.dat

done


switches=`cat ../switches.dat`
cat ../dados/switches_mac.dat > ../dados/switches_mac2.dat
for  j in $switches
do
```

```
mac_pai=`grep $j ../dados/switches_mac2.dat | awk -F" " {'print $1'}`
filhos=`grep -v $mac_pai ../dados/switches_mac2.dat`
valor=0
for k in $filhos
 do

    mac_filho=`echo $k | awk -F" " {'print $1'}`
    ip_filho=`echo $k | awk -F" " {'print $2'}`
    porta_pai=`grep -i $mac_filho ../dados/porta_mac_$j.dat | awk -F" " {'print $1'}`
    #echo "MAC PAI $mac_pai e MAC FILHO $mac_filho"
    if [ -n "$porta_pai" ]
then

     grep -w $porta_pai ../dados/porta_mac_$j.dat > ../dados/outros_filhos

     grep -v $mac_pai ../dados/switches_mac.dat | grep -v $mac_filho | awk -F" " {'print $1'} > ../dados/outros_filhos_restantes


      irmaos=`cat ../dados/outros_filhos_restantes`
      rm -f ../dados/sobra.dat
      for l in $irmaos
      do
       grep -i $l ../dados/outros_filhos >> ../dados/sobra.dat
      done


      valor=`cat ../dados/sobra.dat | wc -l`

      if [ $valor -eq 0  ]
      then
         echo -ne \\a
         porta_filho=`grep -i $mac_pai ../dados/porta_mac_$ip_filho.dat | awk -F" "  {'print $1'}`
         echo "1 PORTA FILHO $porta_filho MAC PAI $mac_pai"
         echo "A porta $porta_filho do SWITCH $ip_filho esta ligado na porta $porta_pai de $j"
         echo   $porta_filho >> ../dados/portas_excluidas_$ip_filho
         echo   $porta_pai >>  ../dados/portas_excluidas_$j
      else
          resto=`cat ../dados/sobra.dat | awk -F" " {'print $2'}`

          porta_filho=`grep -i $mac_pai ../dados/porta_mac_$ip_filho.dat | awk -F" " {'print $1'}`

         rm -f ../dados/sitm.dat
          if [ -n "$porta_filho" ]
          then

              for m in $resto
              do
              grep -w $porta_filho ../dados/porta_mac_$ip_filho.dat > ../dados/outros_pais
              grep -i $m  ../dados/outros_pais >> ../dados/sitm.dat
        valor=`cat ../dados/sitm.dat | wc -l`
```

```
                done
            else
                valor=-1
            fi

            if [ $valor -eq 0  ]
            then
              echo -ne \\a
              echo "2 PORTA FILHO $porta_filho MAC PAI $mac_pai"
              echo "A porta $porta_filho do SWITCH $ip_filho esta ligado na porta $porta_pai de $j"
              echo   $porta_filho >> ../dados/portas_excluidas_$ip_filho
              echo   $porta_pai >>  ../dados/portas_excluidas_$j
            fi

        fi
    fi
    done
  cat ../dados/switches_mac2.dat | grep -v -w $j > ../dados/tmp
  cat ../dados/tmp > ../dados/switches_mac2.dat
done
```

############################main_ifbond_mac.sh###################################

```
#!/usr/local/bin/bash
IFS='
'
rm -f dados/mac_portas_switches.dat
ips=`cat modelo_switches.dat`

for i in $ips
do
./ifbond_mac.sh $i
done
```

############################ifbond_mac.sh############################

```
#!/usr/local/bin/bash
ipswitch=$1

set ignorecase
IFS='
'
rm -f dados/macs.$ipswitch.dat
rm -f dados/portas.$ipswitch.dat
```

```
echo "Fazendo consultas de $ipswitch"

snmpwalk -v 1 -c dlmots $ipswitch mib-2.17.4.3.1.2.0 | awk -F"17.4.3.1.2." {'print $2'} >> dados/portas.$ipswitch.dat
snmpwalk -v 1 -c dlmots $ipswitch mib-2.17.4.3.1.1.0 | awk -F"17.4.3.1.1." {'print $2'} >> dados/macs.$ipswitch.dat
addr=`cat dados/macs.$ipswitch.dat`

for i in $addr
do

 addr2=`echo $i | awk -F"=" {'print $1'}`
 addr3=`echo $i | awk -F":" {'print $2'}`
 prt=`grep $addr2  dados/portas.$ipswitch.dat`
 prt=`echo $prt | awk -F":" {'print $2'}`
 prt=`echo $prt | sed 's/^[ \t]*//;s/[ \t]*$//'`

 resultado_filtro='0'

if [ -n "$prt" ]
then

 if [ -e dados/portas_excluidas_$ipswitch ]
 then
  resultado_filtro=`grep -c -w $prt dados/portas_excluidas_$ipswitch`
 fi

 if [ -n "$resultado_filtro" ]
  then
   if [ $resultado_filtro -eq 0 ]
     then
      if [ $prt -ne 25 ]
       then
         echo "ADDR $addr3 ESTA NA PORT $prt de $ipswitch" >> dados/mac_portas_switches.dat
      fi
   fi
 fi

fi
done
```

##########################ifbond_ip.sh############################

```
#!/usr/local/bin/bash

iprange=$1
router=$2

set ignorecase
IFS='
'

rm -f dados/todos_ips.dat
```

```
./cidr_range.sh $iprange >> dados/todos_ips.dat
all_ip=`cat dados/todos_ips.dat`


index=`snmpgetnext -c dlmots -v1 $router mib-2.4.22.1.1 | awk -F"INTEGER: " {'print $2'}`
echo "INDICE $index"

 for i in $all_ip
do

./fping $i $router
. /fping $router $i

mac=`snmpget -c dlmots -v1 -O0 $router mib-2.4.22.1.2.$index.$i 2>/dev/null | awk -F "STRING:" {'print $2'}`

if  [ -n "$mac"  ]
  then
   mac=`perl ./mac.pl $mac`
   resultado_final=`grep $mac dados/mac_portas_switches.dat`
   echo "IP $i $resultado_final"
  fi
done
```