FACULDADE NOVO MILÊNIO
COORDENADORIA DE ENGENHARIA ELÉTRICA
PROJETO DE GRADUAÇÃO

FREDERICO CHACARA ROCHA
GISELLE SALVADOR DE PAIVA

PRÁTICA DE ROTEAMENTO UTILIZANDO ROUTERBOARD MIKROTIK

VILA VELHA - ES
JUNHO/2011

FREDERICO CHACARA ROCHA
GISELLE SALVADOR DE PAIVA

PRÁTICA DE ROTEAMENTO UTILIZANDO ROUTERBOARD MIKROTIK

Trabalho de Conclusão de Curso apresentado à Faculdade Novo Milênio como requisito para a obtenção da graduação em Engenharia Elétrica.

Orientador
Prof. Robert Mota Oliveira

VILA VELHA – ES
JUNHO/2011

FREDERICO CHACARA ROCHA
GISELLE SALVADOR DE PAIVA

PRÁTICA DE ROTEAMENTO UTILIZANDO ROUTERBOARD MIKROTIK

Trabalho de Conclusão de Curso apresentado à Faculdade Novo Milênio como requisito para a obtenção da graduação em Engenharia Elétrica.

Aprovados em 08 de julho de 2011.

COMISSÃO EXAMINADORA

_____

Prof. Robert Mota Oliveira
Faculdade Novo Milênio
Orientador

_____

Prof. Adjuto M. Vasconcelos Júnior
Faculdade Novo Milênio

_____

Prof. Leonardo Amorim
Faculdade Novo Milênio

Dedico este trabalho a minha Avó Geny e Mãe Elisabeth por dedicarem grande parte do seu tempo a me criar, e sempre se preocuparem comigo, não me deixando desistir nessa longa jornada.

Frederico Chacara Rocha

Eu dedico esse trabalho a minha mãe Letícia, que me criou para ser uma grande mulher, sempre me apoiando com muita força, carinho e ajuda no que eu precisava, principalmente para concluir minha graduação.

Giselle Salvador de Paiva

AGRADECIMENTOS

Agradeço a Deus por ter me guiado e presenteado com a família em que nasci e os amigos que conheci.

Agradeço a minha mãe Elisabeth e a minha avó Geny por serem as pessoas mais importantes na minha vida, pois sem elas eu não teria chegado até onde estou.

Agradeço ao Professor Robert por ter indicado o tema deste trabalho e a Giselle, pois sem a perseverança dela, este trabalho não teria sido concluído.

Agradeço meus familiares por me ajudarem sempre que foi preciso pela força e apoio.

Agradeço aos meus colegas de turma, pelos trabalhos que fizemos juntos, as aulas.

Agradeço aos meus amigos Michael, Neto, por desde o nosso Ensino Médio, ser amigos e aos tantos outros que tropeçaram na minha vida.

Frederico Chacara Rocha

AGRADECIMENTOS

Eu agradeço primeiramente a Deus por me dar forças e paciência nesses cinco anos de muita dedicação e estudo.

Agradeço a pessoa mais importante da minha vida, a minha mãe pela grande ajuda nos momentos necessários e compreensão nos meus horários de estudo. Também ao meu pai por proporcionar a minha formação e ao meu irmão por torcer pela minha vitória na conclusão de minha graduação.

Aos meus amigos de classe, desejo sempre o melhor e agradeço pelos anos de apoio, ajuda para com trabalhos, estudos fora do horário de aula e bons momentos de lazer.

Agradeço a duas mulheres maravilhosas, Rogeany Aledi e Leizirré Suniga que são grandes amigas, me incentivando a lutar pelos meus sonhos e ajudando no que for preciso em todos os momentos.

Também agradeço a todas as minhas amigas e familiares que me apoiaram e incentivaram a concluir o curso e ainda a todas as pessoas que torceram pelo meu sucesso.

Agradeço ao meu parceiro de TCC, Fred, que contribuiu muito para a conclusão deste trabalho em todos os dias de seu desenvolvimento.

Agradeço ao meu namorado Rodrigo pelo apoio, carinho e principalmente compreensão nas horas de ausência para a conclusão desse trabalho.

E finalmente agradecer aos professores, pela atenção dada durante suas aulas e até mesmo fora de seus horários, e em especial ao meu professor orientador Robert Mota Oliveira que de um grande professor se tornou um grande mestre contribuindo para a conclusão deste trabalho.

Giselle Salvador de Paiva

RESUMO

Esse trabalho foi desenvolvido com a intenção de sugerir a criação de um laboratório de roteamento e a formação de instrutores para uso didático, utilizando o roteador *Routerboard MikroTik*. Este tipo de equipamento possui uma interface gráfica, fácil de ser configurada, disponibilizando todas as suas funções na barra de menus do programa *Winbox*. Com isso, antes de demonstrar estes vários tipos de configuração, deve-se entender como funciona essa rede, quais as topologias utilizadas nas experiências. E também entender como um dado (datagrama) chega ao seu destino e o que é utilizado para que se ocorra à comunicação entre computadores em uma rede cabeada. Dessa forma será mostrada a utilidade de cada particularidade para o funcionamento desta rede, com o objetivo de se entender as experiências realizadas. Para que se possa demonstrar no futuro em laboratórios próprios de roteamento com pessoas instruídas e habilitadas a configuração do roteador da empresa *MikroTik*.

Palavras - chave: laboratórios de roteamento, *Routerboard MikroTik*, *Winbox,* experiências, rede cabeada, *MikroTik.*

ABSTRACT

This study was developed with the intention to suggest the creation of routing laboratories and the formation of instructors which will use the router *Routerboard MikroTik* to teach. This device has a graphic interface, easy to configure that provides all of its functions on the menu bars on the *Winbox* program. Thus, before demonstrating these various types of settings, it is needed to understand how this network operates and which topologies were used in the experiments. Also learn how a data (datagram) arrives at yours destiny and what is used to make the communication between computers with a cabled network to occur. Therefore every particularity of the functioning of this network will be shown with the objective to understand the experiments performed. In order to demonstrate in the future, on routing laboratories with instructed and qualified personnel, the configuration of the routers from the company *MikroTik*.

Keywords: routing laboratories, *Routerboard MikroTik*, *Winbox,* experiences*,* cabled network, *MikroTik.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

APs – *Access Point* (Ponto de Acesso)

ARIN – *American Registry for Internet Numbers* (Registro Americano para Números da Internet)

ARP – *Address Resolution Protocol* (Protocolo para Resolução de Endereços)

AS – *Autonomous System* (Sistema Autônomo)

ATM – *Asynchronous Transfer Mode* (Modo Assíncrono de Transferência)

BGP – *Border Gateway Protocol* (Protocolo de Borda do Gateway)

CIDR – *Classess Inter-Domain Routing* (Roteamento Inter-Domínio sem Classe)

CRC – *Cyclical Redundance Check* (Verificação Cíclica de Redundância)

DD or DBD – *DataBase Description* (Descrição do Banco de Dados)

DHCP – *Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de Terminal)

DNS – *Domain Name System* (Sistema de Nomes de Domínios)

ECMP – *Equal Cost Multipath Routing* (Roteamento por Multicaminhos com Mesmo Custo)

EGP – *Exterior Gateway Protocol* (Protocolo do Gateway Externo)

EIGRP – *Enhanced Interior Gateway Routing Protocol* (Protocolo do Roteamento de Gateway Interior Realçado)

FTP – *File Transfer Protocol* (Protocolo de Transferência de Arquivo)

HTTP – *HyperText Transfer Protocol* (Protocolo de Transferência de HiperTexto)

IANA – *Internet Assigned Numbers Authority* (Autoridade para Atribuição de Números na Internet)

ICMP – *Internet Control Message Protocol* (Protocolo de Mensagem de Controle da Internet)

IEN – *Iternet Engeneering Notes* / *Iternet Experiment Notes* (Notas da Engenharia de Internet / Notas da Experiência da Internet)

IETF – *Internet Engineering Task Force* (Força Tarefa da Engenharia da Internet)

IGMP – *Internet Group Management Protocol* (Protocolo de Gerência de Grupos da Internet)

IGP – *Interior Gateway Protocol* (Protocolo do Gateway Interno)

IGRP – *Interior Gateway Routing Protocol* (Protocolo do Roteamento de Gateway Interior)

IHL – *Internet Header Length* (Comprimento do Cabeçalho da Internet)

IID – *Interface IDentifier* (Identificador de Interface)

IP – *Internet Protocol* (Protocolo de Internet)

IPv4 – *Internet Protocol version* 4 (Protocolo de internet versão 4)

IPv6 – *Internet Protocol version* 6 (Protocolo de internet versão 6)

IPSeC – *IP Security Protocol* (Protocolo de Segurança IP)

IPX – *Internetwork Packet Exchange* (Troca de Pacote da Intranet)

ISO – *International Standards Organization* (Organização Internacional para a Padronização)

ISP – *Internet Service Provider* (Provedor de Serviço de Internet)

LACNIC – *Latin American and Caribbean Internet Address Registry* (Registro de Endereços da Internet da América latina e Caribe)

LAN – *Local Area Network* (Rede de Área Local)

LSA - *Link-State Announcement* (Anúncio de Estado do Link)

LSAck - *Link-State Acknowledge* (Reconhecimento de Estado do Link)

LSDB – *Link-State Database* (Banco de Dados do Estado do Link)

LSR – *Link-State Request* (Requisição do Estado do Link)

LSU – *Link-State Update* (Atualização do Estado do Link)

L2TP – *Layer 2 Tunneling Protocol* (Protocolo de Tunelamento da Camada 2)

MAC – *Media Access Control* (Controle de Acesso ao Meio)

MS-DOS – *Microsoft-Disk Operation System* (Sistema Operacional em Disco da Microsoft)

MSS – *Maximum Segment Size* (Tamanho Máximo do Segmento)

MTU – *Maximum Transfer Unit* (Unidade Máxima de Transferência)

NDP – *Neighbor Discovery Protocol* (Protocolo da Descoberta de Vizinhos)

NLSP – *Netware Link Service Protocol* (Protocolo do Serviço de Ligação de Netware)

OSPF – *Open Shortest Path First* (Protocolo Aberto de Roteamento Baseado no Estado do Link)

OSI – *Open Systems Interconnection* (Interconexão de Sistemas Abertos)

PC – Personal Computer (Computador Pessoal)

PNNI – *Private Network-to-Network Interface* (Interface de Rede para Rede Privada)

PPPoE – *Point-to-Point Protocol over Ethernet* (Protocolo Ponto-a-Ponto sobre Internet)

PPtP – *Point-to-Point tunneling Protocol* (Protocolo de tunelamento ponto-a-ponto)

PING – *Packet Internet Grouper* (*Groper*) (Procurador de Pacotes da Internet)

QoS – *Quality of Service* (Qualidade do Serviço)

RARP – *Reverse Address Resolution Protocol* (Protocolo de Resolução Reversa de Endereços)

RFC – *Request for Comments* ("Requisição para Comentários", Padronização de Protocolos)

RIP – *Routing Information Protocol* (Protocolo de Informação de Roteamento)

RIPv1 – *Routing Information Protocol version 1* (Protocolo de Informação de Roteamento versão 1)

RIPv2 – *Routing Information Protocol version 2* (Protocolo de Informação de Roteamento versão 2)

RIPv6 or RIPng – *Routing Information Protocol version 6* ou *Routing Information Protocol next generation* (Protocolo de informação de Roteamento versão 6 ou Protocolo de Informação de Roteamento próxima geração)

RTMP – *Real Time Messaging Protocol* (Protocolo de Mensagem Tempo Real)

SMTP – *Simple Mail Transfer Protocol* (Protocolo Simples de Transferência de Correio)

SNMP – *Simple Network Management Protocol* (Protocolo Simples de Gerência de Rede)

TCP – *Transmission Control Protocol* (Protocolo de Controle de Transmissão)

TCP/IP – *Transmission Control Protocol* / *Internet Protocol* (Protocolo de Controle de Transmissão / Protocolo de Internet)

TTL – *Time to Live* (Tempo De Vida)

UDP – *User Datagram Protocol* (Protocolo de Datagrama de Usuário)

VRRP – *Virtual Router Redundancy Protocol* (Protocolo de Redundância de Roteador Virtual)

WAN – *Wide Area Network* (Rede de Área Ampla)

Zeroconf – Zero Configuration Networking (Trabalhos em Configuração de rede Zero)

SUMÁRIO

INTRODUÇÃO

Como esta cada vez mais comum encontrar uma rede de roteamento nas residências, pensou-se em proporcionar um melhor aprendizado de como se configura e funciona este tipo de rede. Pois nesse trabalho será mostrado na teoria e na prática como foram realizadas as experiências com o *Routerboard MikroTik.*

Assim primeiramente será mostrado todo o assunto proposto sobre redes, suas particularidades, como o roteador, equipamento do nosso estudo, que substituiu o *switch* antes utilizado como periférico concentrador e agora obsoleto. Afinal o roteador esta mais barato e tem a principal função de interligar redes diferentes que são os chamados *Gateways*, sendo atualmente o mais utilizado na internet.

E a cada ano a rede mundial de computadores cresce incontrolavelmente, principalmente a rede sem fio, pois não usa cabeamento e pode ser acessada de qualquer lugar, aumentando a comodidade e facilidade de acesso do usuário comum. E como no decorrer dos anos a *wireless* (rede sem fio) foi substituindo uma rede cabeada que utiliza um modem, que quase sempre se têm problemas como muitos fios conectados, a corrosão dos mesmos expostos ao tempo e também por não se poder acessar de qualquer lugar. A rede sem fio só não cresce mais, por causa da sua desvantagem em relação às redes cabeadas, sua ineficiência em grandes transferências de dados com a parte de multimídia como músicas, filmes e jogos.

Como disse TANENBAUM, 2003, p.86:

> A internet atual é na realidade um conjunto com muitos milhares de redes, e não uma única rede. O que caracteriza e o uso da pilha de protocolos TCP/IP em toda sua extensão. [1]

Esta pilha será explicada e também relacionada com o modelo OSI (*Open Systems Interconnection*) que foi criado pela *International Standards Organization* (ISO), uma das primeiras organizações a definir uma forma de conexão entre computadores. Afinal essa pilha que mostra de que forma um dado (datagrama) chega ao seu destino, explicando cada uma das quatro camadas que possui para se obter este resultado.

A parte de roteamento é muito extensa, mas será restringida a parte de roteamento com cabos de rede e utilizando o roteador da empresa *MikroTik*, o chamado

Routerboard MikroTik. Pois quando acessado pelo seu programa *Winbox*, tem facilidade de acesso e configuração por ter uma interface gráfica.
Na parte final depois de entender a respeito de redes, suas topologias, protocolos de roteamento, utilização e função da pilha de protocolos do TCP/IP (*Transmission Control Protocol* / *Internet Protocol*) e saber como configurar o roteador utilizado. Serão descritas as experiências práticas para concluir o que foi mostrado durante o desenvolvimento desse trabalho. Onde o objetivo final é fazer o leitor entender e aprender sobre configuração de roteamento, utilizando o *Routerboard MikroTik* para depois aplicar nestas experiências e quem sabe aprimorar em novos trabalhos.

1.1 MOTIVAÇÃO

A maior motivação foi aprender algo que antes se achava muito difícil de resolver, que é a questão de construir uma rede de roteamento, porque parecia complexo montar este tipo de rede tendo que configurar roteadores em linhas de comando no *MS-DOS* (*Microsoft-Disk Operation System*).
Por isso foi pensado em trabalhar com o *Routerboard* (roteador) da *MikroTik*, por ter uma interface gráfica com facilidade de acesso e configuração.
Depois de aprender esse tipo de rede, a motivação foi ainda maior para realizar a parte prática com as devidas configurações para cada experiência proposta. Com isso têm-se várias experiências realizadas e mostradas no estudo de caso com clareza para qualquer pessoa entender e tentar desenvolver.

1.2 OBJETIVO

Esse trabalho tem o objetivo de proporcionar um entendimento amplo de uma rede utilizando roteamento com o *Routerboard MikroTik*, que possui uma interface gráfica proporcionada pelo programa *Winbox*. Assim será utilizado como exemplo para que qualquer pessoa possa entender seu funcionamento e consiga configurá-lo.
Dessa forma, foram realizadas muitas experiências pensando na criação de um laboratório de roteamento com instrutores capazes de ensinarem, para que muitas

pessoas entendam sobre o assunto e consigam criar esse tipo de rede sem muitos problemas. Afinal o crescimento da internet é incalculável a cada dia, aumentando consideravelmente o número de novos usuários a cada ano.

1.3 DESCRIÇÃO DOS CAPÍTULOS

Capítulo 2: Topologias de Redes – Neste capítulo será abordado, os principais tipos de topologias que foram utilizadas no desenvolvimento desse trabalho para proporcionar o entendimento das experiências realizadas no estudo de caso.
Capítulo 3: Pilha de protocolos TCP/IP – Este capítulo aborda a função de cada camada comparada com as do modelo OSI e quais protocolos são utilizados, descrevendo-se os principais protocolos TCP (*Transmission Control Protocol*), IP (*Internet Protocol*) e ICMP (*Internet Control Message Protocol*); e ao final é mostrado o IPv6 (*Internet Protocol version* 6).
Capítulo 4: Roteamento – Este capítulo descreve quais são os tipos mais utilizados de protocolos de rede e de que forma estes interferem no processo de transferência de um datagrama IP; comentando sobre os protocolos RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*) e BGP (*Border Gateway Protocol*).
Capítulo 5: *MikroTik Routerboard* – Neste capítulo será apresentado a empresa que criou o roteador utilizado nas experiências, suas funcionalidades e como se tem acesso ao mesmo.
Capítulo 7: Estudo de Caso: Laboratório prático, Estudo de experiência – Serão mostradas as experiências realizadas; a configuração detalhada do estudo de caso, mostrando o passo - a - passo de como se configura um *Routerboard MikroTik*.
Capítulo 8: Conclusão – Capítulo final é a parte que conclui tudo que foi descoberto durante a realização de cada experiência, se suas configurações foram eficazes e o que ocorreu, o que se achou do desenvolvimento do estudo de caso, com isso o que se aprendeu e entendeu com a parte prática desse trabalho. E também a sugestão de que possa ser realizadas experiências utilizando outras funções do *Routerboard MikroTik*. Afinal foram mostradas muitas experiências no estudo de caso com o intuito de proporcionar curiosidade e interesse das pessoas, para quem sabe ser utilizados em trabalhos futuros e na criação de um laboratório de roteamento.

2 TOPOLOGIAS DE REDE

“O termo topologia refere-se à maneira com que os computadores de uma rede local estão conectados.” (TORRES, 2009, p. 20)

Uma rede de computadores é constituída por um computador ligado (conectado) a outro, graças a uma linha de comunicação que são os cabos de rede, e também elementos materiais como as placas de rede.

“Uma topologia da rede é um mapa da rede. ’ ‘A topologia física da rede descreve o layout dos cabos e postos de trabalho e a localização de todos os componentes da rede.” [13]

Dessa forma têm-se as seguintes topologias físicas:

- *Bus* (Barramento)
- *Star* (Estrela)
- *Ring* (Anel)

2.1 TOPOLOGIA BARRAMENTO (LINEAR)

“Nesta configuração todos os nós (estações) se ligam ao mesmo meio de transmissão. ’ ‘A barra é geralmente compartilhada em tempo e freqüência, permitindo transmissão de informação.” [11]

Nesse tipo de topologia cada nó conectado a esse barramento pode ter acesso a todas as informações transmitidas. Com isso todos os outros computadores dessa rede podem se comunicar entre si.

“Nessa topologia todos os computadores estão ligados a um cabo contínuo que é determinado em ambas às extremidades por uma pequena ficha com uma resistência ligada entre a malha e o fio central do cabo (terminadores). ’ ‘A função dos “terminadores” é de adaptarem a linha, isto é, fazerem com que a impedância vista para interior e para o exterior do cabo seja a mesma, senão constata-se que há reflexão do sinal e, conseqüentemente, perda da comunicação.” [13]

“A comunicação no barramento é feita por broadcast, isto é, a informação transmitida é recebida por todos os nós da rede, afinal é passada para o cabo que todos estão conectados mais só é recebido pelo nó de destino. ’ ‘Pois cada nó tem

seu endereço e se este não for o da mensagem recebida é descartada. ’ ‘O desempenho de um sistema em barramento é determinado pelo meio de transmissão, número de nós conectados, controle de acesso, tipo de tráfego entre outros fatores. ’ ‘O tempo de resposta pode ser altamente dependente do protocolo de acesso utilizado.” [11]

De acordo com as referências [12] e [13], temos as seguintes vantagens e desvantagens dessa topologia.

Vantagens:

- Facilidade de instalação e expansão;
- Fácil de entender seu funcionamento;
- É uma topologia relativamente confiável e econômica;
- Usa menos cabo que as outras topologias, sendo mais barata.

Desvantagens:

- Dificuldade de mudar ou mover nós;
- Não tem tolerância a falhas, caso falhe um dos nós toda rede é comprometida, ficando sem funcionamento;
- A rede fica mais lenta em períodos de uso mais intenso;
- Dificuldade de diagnosticar falha ou erro.

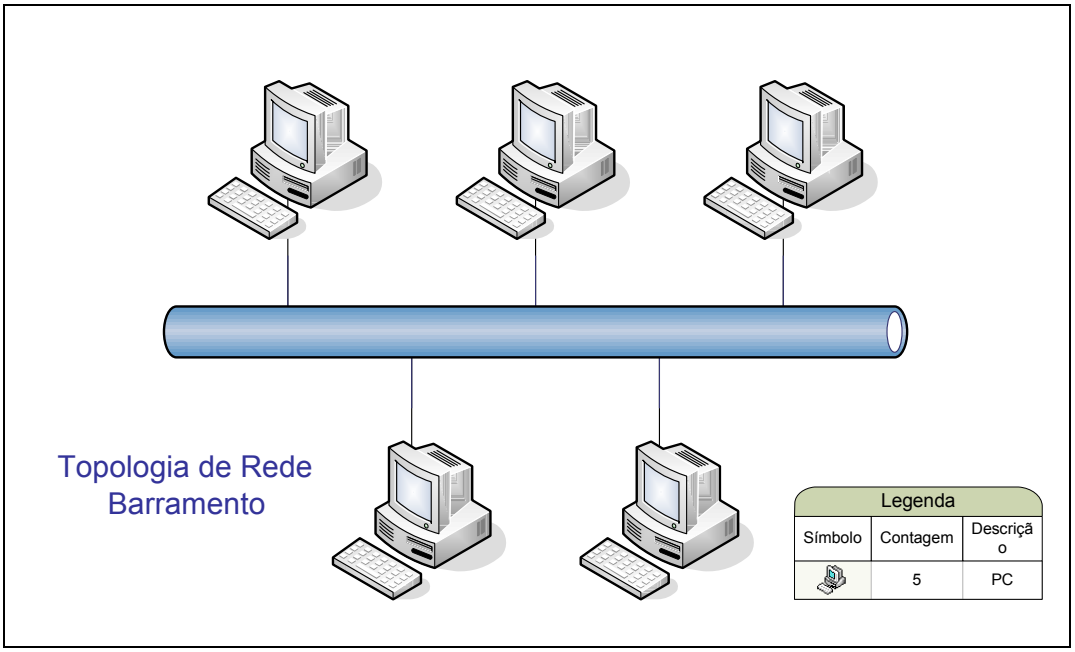

Figura 1 - Formato da Topologia Barramento (Linear)

2.2 TOPOLOGIA ESTRELA

Nessa topologia os computadores da rede estão ligados a um periférico concentrador representado na figura 2 por um roteador.

A função dessa topologia é encaminhar uma informação para o *host* (computador) de destino. “Dessa forma quando um dado for enviado de um *host* A para um *host* B, passando pelo roteador ligado a essa rede ele manda o dado para o *host* B. ’ ‘Caso algum *host* pare a conexão essa rede não fica comprometida, uma vez que quem transmite a troca de informação é o equipamento central. ’ ‘Assim só o *host* sem funcionamento não poderá utilizar essa rede, e os demais continuaram suas conexões independente de cada outro *host*.” [10]

“O desempenho obtido numa rede em estrela depende da quantidade de tempo requerido pelo nó central (roteador) para processar e encaminhar mensagens, e da carga de tráfego de conexão, ou seja, é limitado pela capacidade de processamento deste nó.” [11]

De acordo com as referências [12] e [13], temos as seguintes vantagens e desvantagens dessa topologia.

Vantagens:

- Facilidade de modificação do sistema, já que todos os cabos convergem para um só ponto;
- Se um *host* falhar só ele é afetado;
- A codificação e adição de novos *hosts* são simples;
- Fácil detecção e isolamento de falhas, pois o roteador está diretamente ligado a todos os outros;
- Simplicidade no protocolo de comunicação. Resume-se a selecionar qual o computador que receberá a informação do roteador.

Desvantagens:

- Maior comprimento de cabo para efetuar ligações. A distância máxima sem amplificação é de apenas 100 m;
- Dependência do roteador, se este falhar, a rede não funciona;
- O número de portas de um periférico concentrador é limitado e quando for atingido o limite de portas disponíveis é necessário adquirir outro e interligá-lo com o existente;
- Seus custos são mais elevados, afinal utilizam mais equipamentos.

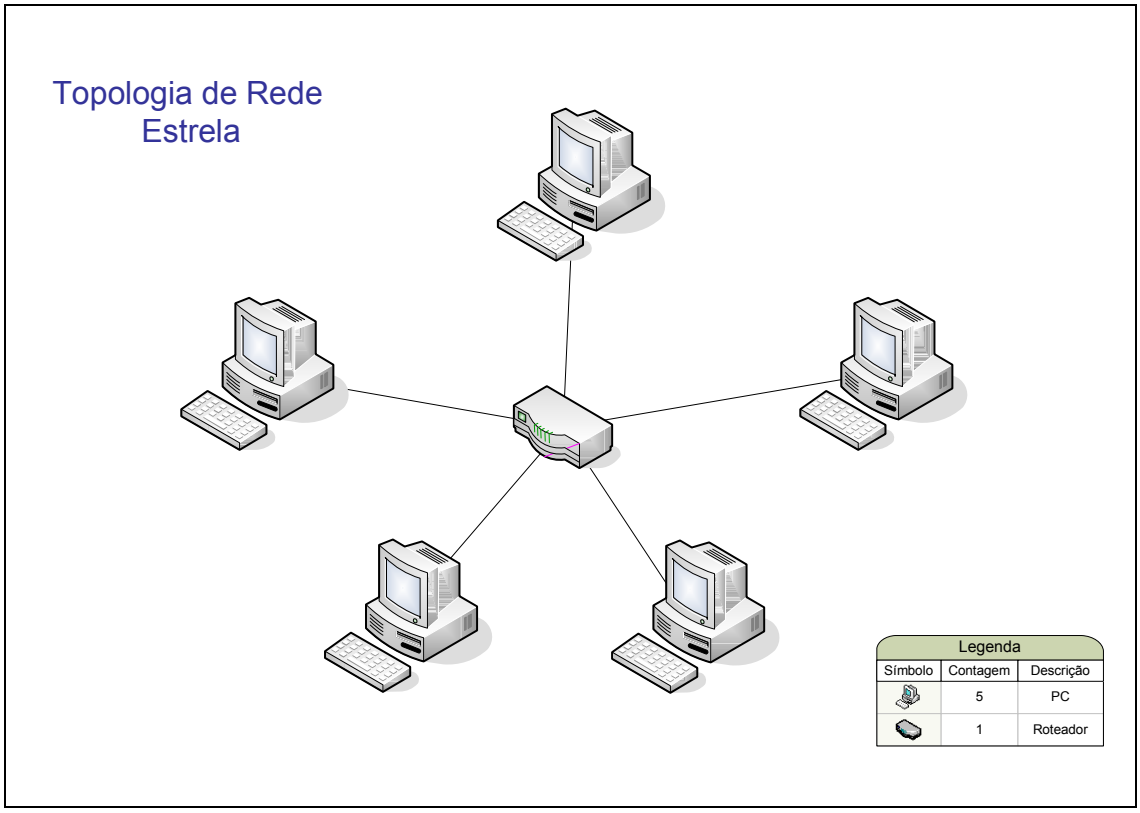

Figura 2 - Formato da Topologia Estrela, utilizando um periférico concentrador

2.3 TOPOLOGIA ANEL

Nessa topologia cada computador está ligado ao anterior e ao próximo num circuito fechado no formato de círculo, representação de uma rede em anel, podendo receber dados em qualquer direção, “mas as configurações mais usuais são de redes unidirecionais, de forma a tornar menos sofisticado os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em seqüência ao destino”. [11]

Dessa forma se um computador deixar de funcionar comprometerá o restante da rede, deixando essa rede sem conexão afinal quando o dado transmitido chegar até ele não será transmitido para os demais, voltando a funcionar quando for resolvido o problema. Mais isso pode ser resolvido se no lugar usar uma rede bidirecional, pois nenhum nó ficaria inacessível, já que poderia ser atingido pelo outro lado.

Essa topologia funciona da seguinte forma: o sinal originado por um nó passa em torno do anel, sendo que em cada nó o sinal é regenerado e retransmitido. Como

acontece em qualquer topologia, cada estação, ou nó, atende por um endereço que, ao ser reconhecido por uma estação, aceita a mensagem e a trata.
De acordo com as referências [12] e [13], temos as seguintes vantagens e desvantagens dessa topologia.

Vantagens:

- Pequeno comprimento de cabo;
- Todos os computadores acessam a rede igualmente;
- Permitir a um nó receber pacotes enviados por qualquer outro nó da rede, independentemente de qual seja o nó destino;
- Sem impacto no desempenho da rede ao adicionar um novo computador.

Desvantagens:

- A falha de um computador afeta o restante da rede, só voltando ao seu funcionamento com a resolução do problema ocorrido;
- Dificuldade de localização de falhas (a falha de um nó provoca a falha de todos os outros);
- Dificuldade em reconfigurar a rede (instalação de vários nós em locais diferentes);
- Erro de transmissão e de processamento pode fazer com que uma mensagem continue eternamente a circular no anel;
- Um problema é que nas redes unidirecionais, se uma linha entre dois nós cair, todo sistema sai do ar até que o problema seja resolvido;
- Dificuldade no estabelecimento de protocolo de acesso à rede, dado que cada nó terá que assegurar a continuidade da informação e só depois poderá enviar a sua própria informação após a certificação de que a rede está disponível.

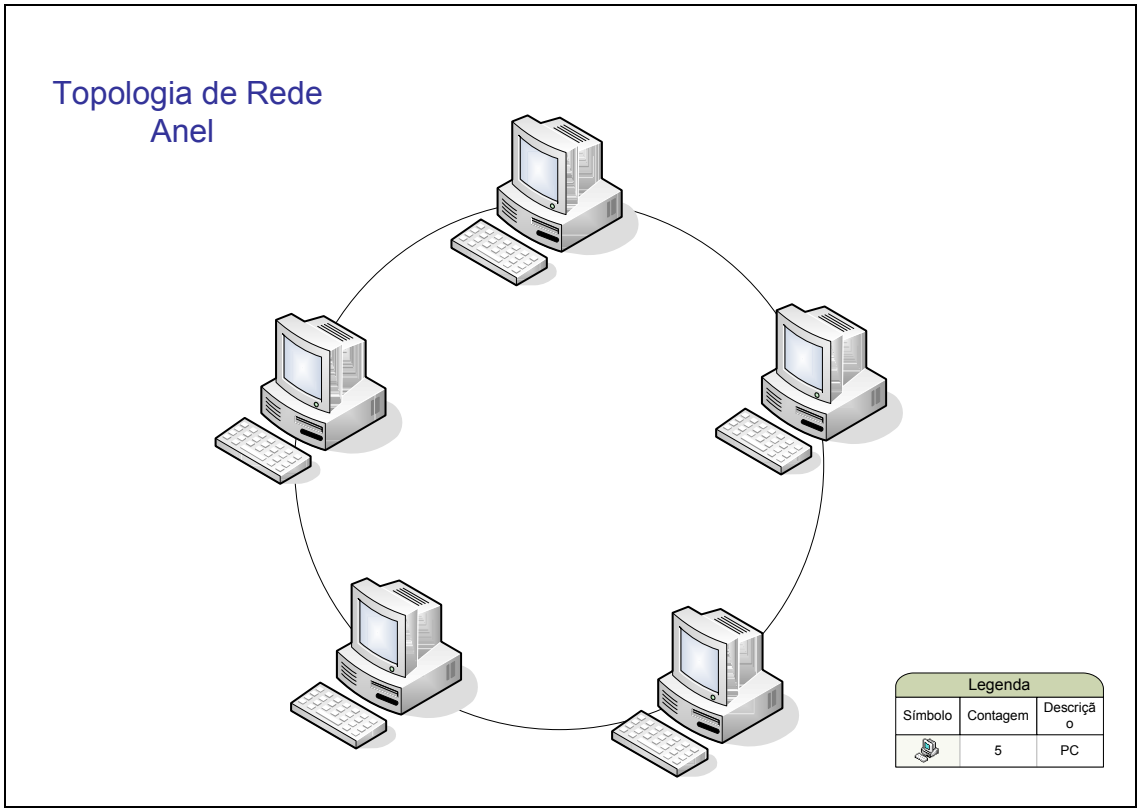

Figura 3 - Formato da Topologia Anel

Existem também os tipos de topologias de redes que são uma mistura de topologias já existentes como as descritas anteriormente, mas que não serão utilizadas em nossas experiências, por exemplo: Estrela Hierárquica ou Árvore, Estrela Estendida, Malha (*Mesh*), sem fio (*Wireless*), espinha dorsal (*Backbone*), Híbrida, dentre outras. Assim os assuntos referentes a estas topologias não serão aprofundados.

3 PILHA DE PROTOCOLOS TCP/IP

De acordo com TORRES, 2001, p. 39:

> Quando as redes de computadores surgiram, as soluções eram, na maioria das vezes, proprietárias, isto é, uma determinada tecnologia só era suportada por seu fabricante. Não Havia possibilidade de se misturar soluções de fabricantes diferentes. Dessa forma, um mesmo fabricante era responsável por construir praticamente tudo na rede. [5]

Para resolver esse problema a ISO criou o modelo ISO/OSI com o objetivo de ser uma referência para os fabricantes, porém a pilha de protocolo TCP/IP não segue totalmente esse modelo.

Enquanto o modelo ISO/OSI possui sete camadas o TCP/IP está dividido em quatro, entretanto estas divisões de camadas podem ser comparadas.

De acordo com TORRES, 2001, p. 43 a 46; no modelo OSI as sete camadas são as seguintes:

- Camada de Aplicação: responsável por fazer a interface entre o protocolo de comunicação e o aplicativo;
- Camada de Apresentação: traduz o dado recebido da camada de aplicação para o protocolo que será usado;
- Camada de Sessão: estabelece uma sessão entre duas aplicações, nesta sessão as aplicações definem a transmissão de dados e colocam marcações nos dados para poder restabelecer a transmissão em caso de falha da rede;
- Camada de Transporte: recebe os dados da camada de sessão e os divide em pacotes repassando-os para a camada de rede;
- Camada de Rede: endereça os pacotes de dados recebidos da camada de transporte, converte endereços lógicos em endereços físicos para que os pacotes cheguem ao endereço correto, também define a rota que os pacotes tomarão para chegar ao destino;
- Camada de Link de Dados: transformam em quadros os pacotes de dados entregues pela camada de rede, adicionando o endereço da placa de rede de origem, endereço da placa de destino, dados de controle e o CRC (*Cyclical Redundance Check*) que tem a função de verificar erros no quadro transmitido, e entregar para a camada física;

- Camada Física: recebe os quadros e os transforma em sinais (elétricos, ópticos, etc.) que vão ser transmitidos no meio, não se preocupando com o mesmo, no máximo com o tipo de cabo e o tipo de conector.

Esse modelo TCP/IP é uma coleção ou pilha de protocolos de comunicação entre computadores em rede, praticamente usada em qualquer rede hoje em dia. Esse sucesso é devido à popularização da Internet, e por ele ser roteável e possuir uma arquitetura aberta mostrada no quadro 1.

Camada	Modelo ISO/OSI	TCP/IP
7	Aplicação	Aplicação
6	Apresentação	
5	Sessão	
4	Transporte	Transporte
3	Rede	Rede
2	Enlace	Interface com a Rede
1	Física	

Quadro 1 - Arquitetura da pilha TCP/IP comparado com o modelo ISO/OSI
FONTE: [2]

Note que cada camada da pilha TCP/IP pode ter vários protocolos operando, sendo por isso chamado de pilha, e cada protocolo dessa pilha é documentado no RFC que são documentos de descrição completa de todos os protocolos. Estes protocolos estão localizados nas três camadas superiores desse modelo. Assim cada camada tem a seguinte função:

- Camada de Aplicação: define os protocolos de aplicativos TCP/IP e como os programas *host* estabelecem uma interface com os serviços de camada de transporte para usar a rede; os protocolos utilizados são o SMTP (*Simple Mail Transfer Protocol*), o HTTP (*HyperText Transfer Protocol*), o FTP (*File Transfer Protocol*), o SNMP (*Simple Network Management Protocol*), o DNS (*Domain Name System*) e o Telnet.
- Camada de Transporte: fornece gerenciamento de sessão de comunicação

entre computadores *host*. Define o nível de serviço e o status da conexão usada durante o transporte de dados; existem dois protocolos nesta camada o TCP e o UDP (*User Datagram Protocol*).

- Camada de Rede: empacota dados em datagramas IP, que contêm informações de endereço de origem e de destino usadas para encaminhar datagramas entre *host*s e redes. Executa o roteamento de datagramas IP; existem vários protocolos que podem operar nesta camada como o IP, ICMP, IGMP, ARP (*Address Resolution Protocol*), RARP (*Reverse Address Resolution Protocol*) e o NDP (*Neighbor Discovery Protocol*); e também o DHCP (*Dynamic Host Configuration Protocol*) que, apesar de tecnicamente ser um protocolo de aplicação, lida com a distribuição de endereços IP para máquinas da rede.
- Camada de interface com a Rede: especifica os detalhes de como os dados são enviados fisicamente pela rede, inclusive como os bits são assinalados eletricamente por dispositivos de hardware que estabelecem interface com um meio da rede, como cabo coaxial, fibra óptica ou fio de cobre de par trançado.

"Os protocolos TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*) foram criados com o intuito de realizar a intercomunicação de computadores. ' 'A configuração destes protocolos tem a função de controlar a maneira que a informação é passada de uma rede a outra, e como manipular o endereçamento contido nos pacotes, a fragmentação dos dados e a checagem de erros." [19]

"O TCP é o protocolo da camada de transporte, orientado a conexão e especifica o formato dos pacotes de dados e de reconhecimento que dois computadores trocam para realizar uma transferência confiável." [15]

O TCP é definido na RFC 793 e suas principais características são:

- Executar a segmentação e o reagrupamento de grandes blocos de dados enviados pelos programas.
- Garantir o seqüenciamento adequado e a entrega ordenada de dados segmentados (datagrama IP) de comprimento variável a fim de "entregar" ao protocolo IP. [18]

- Verificar a integridade dos dados transmitidos usando cálculos de soma de verificação, e também verificar a onda de dados para evitar a saturação da rede.
- Enviar mensagens positivas dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos.
- Oferecer um método preferencial de transporte para programas que precisam usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de email.
- Permitir multiplexar os dados, quer dizer, fazer circular simultaneamente informações que provêm de fontes (por exemplo, aplicações) distintas numa mesma linha. [18]
- Permitir, por ultimo, o começo e o fim de uma comunicação de maneira educada. [18]

Já o protocolo IP é um protocolo de datagrama para a comunicação de redes internet definido na RFC 791, responsável principalmente pelo endereçamento e roteamento de pacotes entre *host*s. Sendo este sem conexão significando que uma sessão só é estabelecida após a troca de dado, sendo também não confiável afinal não garante a entrega de dados, mas sempre está fazendo o melhor para tentar entregar um pacote. Este pacote IP pode ser perdido, entregue fora da seqüência, duplicado ou atrasado, sendo que esse protocolo não tenta se recuperar destes tipos de erros. Já a confirmação de pacotes entregues e a recuperação de pacotes perdidos é responsabilidade de um protocolo de camada superior, como o TCP. Assim as funções do protocolo IP de acordo com a referência [20], são:

- Não possui mecanismos de retransmissão.
- Não da garantia de uma transmissão integra ou ordenada.
- Utiliza os "endereços IP" como base para o direcionamento dos datagramas.
- Descarta um datagrama se ele não for entregue ou se passar muito tempo trafegando na Internet.
- Suas operações e padrões estão descritos em vários RFC's (*Request for Comments*) e IEN's (*Iternet Engeneering Notes*).

"O TCP especifica o formato dos pacotes de dados e de reconhecimento que dois computadores trocam para realizar uma transferência confiável, assim como os

procedimentos que eles usam para assegurar que os dados cheguem corretamente, que são: transferência de dados confiável fim - a - fim (onde todo pacote transmitido requer um *Ack* que é um bit de reconhecimento, há a recuperação de dados perdidos, o descarte de dados duplicados e a reorganização dos dados recebidos fora de ordem); comunicação bidirecional (*full - duplex*) entre cliente - servidor; e o seqüenciamento: bytes de segmentos são numerados, de forma a garantir a entrega em ordem e a detecção e eliminação de duplicatas, sendo voltado para atuar sobre redes heterogêneas com tamanhos máximos de pacotes variáveis, faixas de passagem variáveis e topologias distintas." [16]

Como o TCP/IP foi criado para ser usado em diversas redes podem existir redes que tenham um MTU (*Maximum Transfer Unit*) menor do que o da rede que originou o quadro do pacote de dados, com isso este quadro que tem no máximo 1.500 bytes de acordo com a Ethernet, terá que ser fragmentado para passar nessa rede com o MTU menor, dividindo esse valor original em dois pacotes de 600 bytes, para não deixar de ser transmitido por não "caber" no quadro do meio do caminho, e ser transmitido para o quadro da rede de destino.

3.1 ENDEREÇAMENTO IP

Para entregar um pacote de dados, a rede precisa conhecer o endereço da máquina que tem que ser alcançada. Cada máquina possui dois endereços: o físico (endereço MAC, *Media Access Control*), que é gravado na placa de rede da máquina, e um endereço lógico (endereço IP, no caso do protocolo TCP/IP), que é configurado por *software*.

Numa rede local quando uma máquina quer enviar um pacote de dados, ela envia o quadro de dados para a rede que contém o endereço físico da máquina de destino, nas redes *Ethernet* comuns todas as máquinas conseguem ver o quadro de dados, mas só a maquina de destino (a que possui o endereço físico) que o captura. O Problema é que se este processo fosse usado para, varias redes conectadas a outras várias redes geraria um tráfego absurdo. Assim para resolver este problema o endereçamento lógico precisa ser usado.

O endereçamento lógico funciona de maneira padronizada e organizada, podendo-se atravessar várias redes sem congestioná-las. O envio de pacotes de uma rede a outra é responsável pelo periférico chamado de roteador e a grande vantagem do protocolo IP é ser roteável.

O endereçamento IP é divido em duas versões usadas: IPv4 e IPv6, a versão quatro é usada em quase todos os computadores hoje em dia e a IPv6 foi criada devido ao esgotamento de número de endereços do IPv4.

Os endereços IPs são controlados pela IANA (*Internet Assigned Numbers Authority*) entidade global que os regulariza e que distribui para as entidades Regionais, no caso dos EUA a ARIN (*American Registry for Internet Numbers*) e do Brasil a LACNIC (*Latin American and Caribbean Internet Address Registry*).

O endereçamento IPv4 é feito com 32 bits dispostos em 4 octetos e são escritos em decimal (192.89.45.234) cada octeto varia de 0 a 255 sendo 256 combinações por octeto, gerando um total de 4.294.967.296 endereços possíveis com os 4. Para haver uma melhor distribuição desses endereços eles foram separados por classes, mostradas nos quadros 2 e 3:

<table>
<tr><td></td><td></td><td>A</td><td>B</td><td>C</td><td>D</td></tr>
<tr><td>Classe A</td><td>θ</td><td>Identificação da rede (7bits)</td><td colspan="3">Identificação da maquina (24 bits)</td></tr>
<tr><td>Classe B</td><td>1 θ</td><td colspan="2">Identificação da rede (14 bits)</td><td colspan="2">Identificação da maquina (16 bits)</td></tr>
<tr><td>Classe C</td><td>1 1 θ</td><td colspan="3">Identificação da rede (21 bits)</td><td>Identificação da maquina (8 bits)</td></tr>
<tr><td>Classe D</td><td>1 1 1 θ</td><td colspan="4">Endereçamento Multicast</td></tr>
<tr><td>Classe E</td><td>1 1 1 1</td><td colspan="4">Reservador para o uso futuro</td></tr>
</table>

Quadro 2 - Classes de endereço IPv4, especificando a função de cada classe
Fonte: [2]

Classe	Endereço mais baixo	Endereço mais alto
A	0.0.0.0	127.255.255.255
B	128.1.0.0	191.255.255.255
C	192.0.1.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Quadro 3 - Classes de endereços IPv4, especificando a faixa de cada classe
FONTE: [2]

Alguns desses endereços possuem significado especial e desta lista abaixo existe alguns que são determinados como “Endereços Privados” que são os mais usados em redes locais, pois não são válidos na internet, porque para ficar conectado na internet seja permanente ou temporariamente é necessário um “Endereço Público” que são os endereços válidos e únicos, já os privados se repetem nas redes locais.

Endereços	Uso
0.0.0.0 a 0.255.255.255	Não podem ser usados
10.0.0.0 a 10.255.255.255	Endereçamento privado
127.0.0.0 a 127.255.255.255	Realimentação indica a própria maquina
169.254.0.0 a 169.254.255.255	*Zeroconf* (*Zero Configuration Networking*)
172.16.0.0 a 172.31.255.255	Endereçamento privado
192.0.2.0 a 192.0.2.255	Documentação e exemplos
192.88.99.0 a 192.168.88.99	Conversão IPv6 em IPv4
192.168.0.0 a 192.168.255.255	Endereçamento Privado
198.18.0.0 a 198.19.255.255	Dispositivo para teste da rede

Quadro 4 - Endereços IP
FONTE: [2]

Por padrão, em redes IP, é definido um endereço que serve para identificar a rede, sendo sempre o primeiro e geralmente é colocado como “.0”, um exemplo de rede classe C é o endereço IP 192.168.70.0, sendo que, se houver alguma máquina com endereço IP 192.168.70.w (o “w” pode variar de 1 até 254) e tiver um datagrama com destino para ela, o datagrama será enviado para essa rede (IP 192.168.70.0) a qual a máquina pertence, e depois o dispositivo de rede (roteador, *switch*, *hub*, etc.) entregará o datagrama, afinal o ultimo endereço é padronizado para entregar o datagrama para todas as maquinas da rede, geralmente é usado o “.255” como o exemplo IP 192.168.70.255 sendo o endereço de *broadcast*.

Classe	Endereço de rede	Endereço de *broadcast*
A	10.0.0.0	10.255.255.255
B	172.16.0.0 até 172.31.0.0	172.16.255.255 172.31.255.255
C	192.168.0.0	192.168.255.255

Quadro 5 - Exemplos de redes
FONTE: [2]

3.2 MÁSCARA DE REDE E SUB-REDE

Como observado no quadro 5, pode-se ter redes enormes e ter um grande problema de entrega de datagramas devido ao tráfego e vários endereços IP não sendo utilizado, então para poder gerenciar melhor o tamanho da rede e poder mostrar a qual rede o datagrama está destinado é usada a máscara de rede ou mascara de sub-rede.

A mascara de rede tem o mesmo tamanho do endereço IP, 32bits separado em octetos, o esquema usado é o seguinte: os bits da mascara sempre terão o valor 1 para designar uma rede e 0 para as máquinas dessa mesma rede, o valor decimal 255 é representado em binário com 8 bits com valor 1 o quadro 6 abaixo mostra as máscaras padrões:

Classes	Máscaras de rede em decimal	Máscaras de rede em binário
A	255.0.0.0	1111.1111.0000.0000.0000.0000.0000.0000
B	255.255.0.0	1111.1111.1111.1111.0000.0000.0000.0000
C	255.255.255.0	1111.1111.1111.1111.1111.1111.0000.0000

Quadro 6 - Classes de máscaras em binário
FONTE: [2]

Outra maneira de representar a mascara é usando o sistema CIDR (*Classess Inter-Domain Routing*), mostrado no quadro 7 que usa uma "/" depois do endereço IP da rede e logo após ela colocar o número (em decimal) de bits em 1 da máscara usada.

Classes	Máscaras de rede em decimal	Máscaras de rede com CIDR
A	255.0.0.0	x. 0. 0. 0 /8
B	255.255.0.0	x. y. 0. 0 /16
C	255.255.255.0	x. y. z. 0 /24

Quadro 7 - Classes de máscara com CIDR
FONTE: [2]

Obs.: x, y, z, são alguns endereços de rede.

Além das mascaras padrões /8 /16 /24 pode-se utilizar outras para dividir a rede como /26 que é uma rede de 64 computadores, pois 26 bits dos 32 bits do IP estão colocados em 1 assim sobrando 6 bits, logo com 6 bits pode-se representar 64 números, em ordem, de 0 a 63 ou de 64 a 127, 128 a 191 , 192 a 255, as figuras 4 e

5 abaixo mostram dividindo um endereço /24 em 4 redes e a outra só com 1 rede com 32 máquinas ou /27.

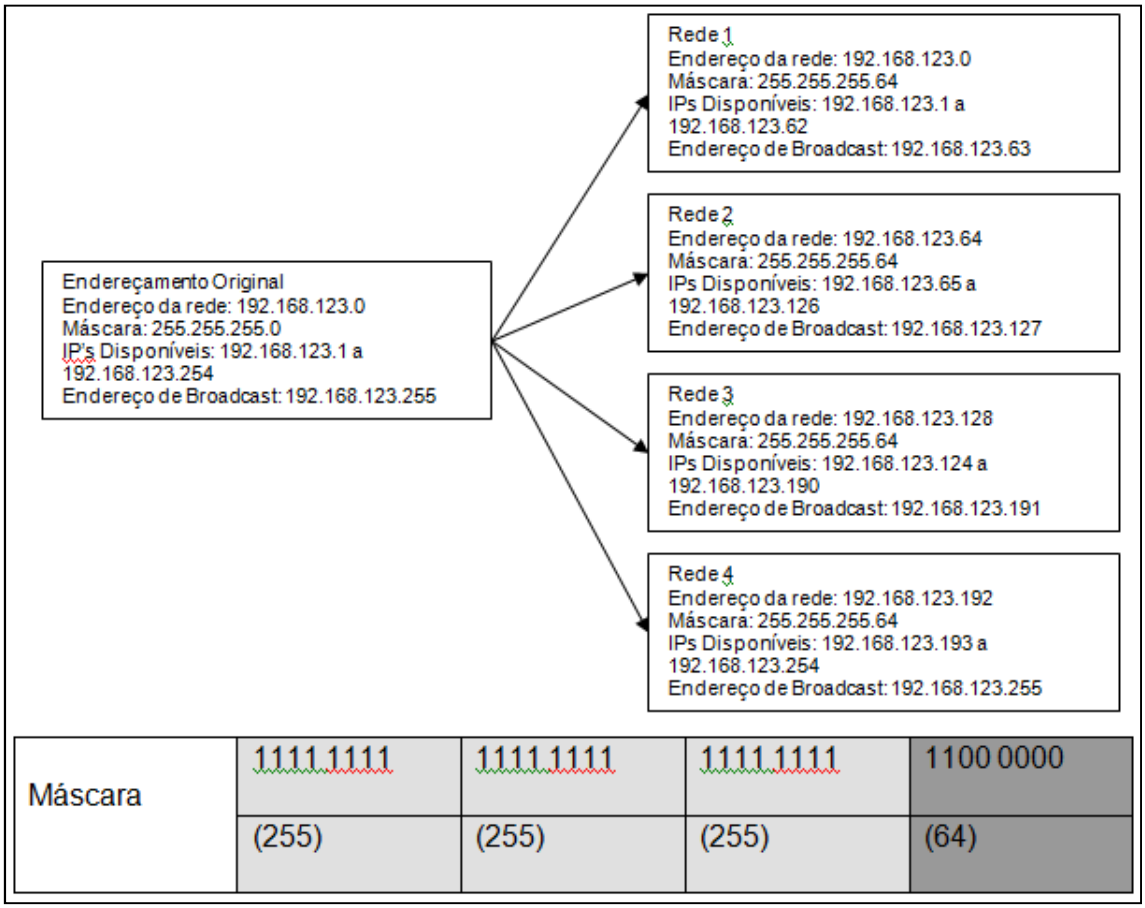

Figura 4 - Exemplos de redes, dividindo uma rede em sub-redes
FONTE: [2]

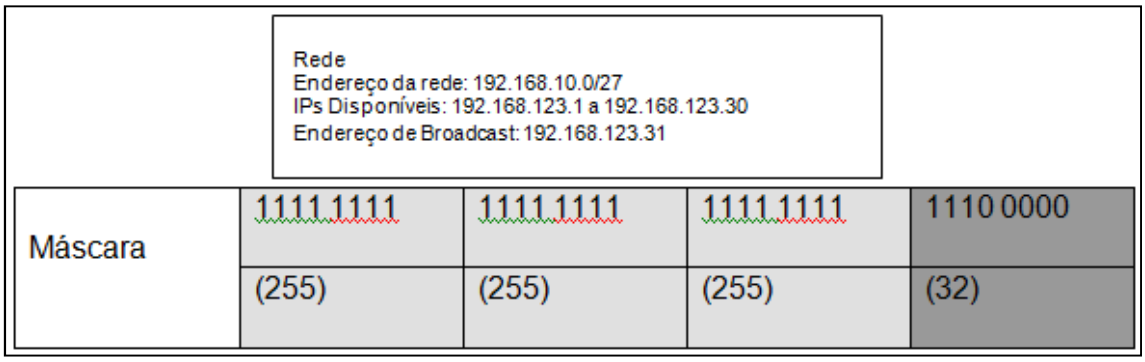

Figura 5 - Exemplos de redes, criando uma sub-rede
FONTE: [2]

3.3 DATAGRAMA IP

“É a unidade básica de dados no nível IP. Um datagrama está dividido em duas áreas, uma área de cabeçalho e outra de dados.” [23]

“O cabeçalho contém toda a informação necessária que identificam o conteúdo do datagrama.” [23]

Como disse TANENBAUM, 2002, p. 334:

> O cabeçalho tem uma parte fixa de 20 bytes e uma parte opcional de tamanho variável. Ele é transmitido em uma ordem big endian: da esquerda para a direita, com o bit de mais alta ordem do campo Version aparecendo primeiro. O campo Version controla a versão do protocolo à qual o datagrama pertence. Incluindo-se a versão em cada datagrama, é possível verificar a transição entre as versões, o que pode levar meses ou até mesmo anos, com algumas máquinas executando a versão antiga e outras executando a nova versão. [4]

“Na área de dados está encapsulado o pacote do nível superior, ou seja, um pacote TCP ou UDP.” [23]

Com isso temos o formato do datagrama IP:

<table>
<tr><td>Versão
(4 bits)</td><td>Comprimento
de Cabeçalho
(4 bits)</td><td>Tipo de Serviço
(8 bits)</td><td colspan="2">Comprimento Total (16 bits)</td></tr>
<tr><td colspan="3">Identificação (16 bits)</td><td>Bandeira
(3 bits)</td><td>Deslocamento do
Fragmento (13 bits)</td></tr>
<tr><td colspan="2">Duração de Vida (8 bits)
(TTL)</td><td>Protocolo
(8 bits)</td><td colspan="2">Soma de Controle do
Cabeçalho (16 bits)</td></tr>
<tr><td colspan="5">Endereço IP de Origem</td></tr>
<tr><td colspan="5">Endereço IP de Destino</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Dados</td></tr>
</table>

Figura 6 - Estrutura do Cabeçalho do Datagrama IP
FONTE: [24]

Dessa forma, têm-se os seguintes campos, de acordo com a referência [24]:

- Versão: trata-se da versão do protocolo IP que se está utilizando (atualmente essa versão é a IPv4, IP versão 4) para verificar a validade do datagrama, sendo codificada em 4 bits.

- Comprimento de Cabeçalho ou IHL (*Internet Header Length*): trata-se do número de palavras de 32 bits que constituem o cabeçalho (nota: o valor mínimo é 5), sendo codificado em 4 bits.
- Tipo de Serviço: indica a maneira segundo a qual o datagrama deve ser tratado.
- Comprimento Total: indica a dimensão total do datagrama em bytes. Sendo que a dimensão total do datagrama não pode exceder 65.536 bytes. Este campo, utilizado em conjunto com a dimensão do cabeçalho, permite determinar onde estão situados os dados.
- Identificação, Bandeira e Deslocamento do fragmento: são campos que permitem a fragmentação dos datagramas.
- Duração de Vida (TTL): este campo indica o número máximo de roteadores através dos quais o datagrama pode passar. Assim este campo é reduzido a cada passagem em roteador, quando este atinge o valor crítico de 0, o roteador destrói o datagrama. Isto evita o congestionamento da rede pelos datagramas perdidos.
- Protocolo: este campo, em notação decimal, permite saber de que protocolo procede ao datagrama.
- Soma de Controle do Cabeçalho: este campo contém um valor codificado de 16 bits, que permite controlar a integridade do cabeçalho a fim de determinar se este não foi alterado durante a transmissão. A soma de controle é o complemento de todas as palavras de 16 bits do cabeçalho (campo soma de controle excluído). Isto é para que, quando se faz a soma dos campos do cabeçalho (soma de controle incluída), se obtenha um número com todos os bits posicionados a 1.
- Endereço IP de Origem: este campo representa o endereço IP da máquina emissora, permitindo a resposta do destinatário.
- Endereço IP de Destino: este campo representa o endereço IP do destinatário da mensagem.
- Opções + Padding: esse campo é opcional e possui tamanho variável. Se for usado, ele precisa ter um comprimento múltiplo de 32 bits. Caso não seja, são adicionados zeros (senão houver mais opções a serem transmitidas no mesmo cabeçalho) ou uns (se houver mais opções a serem transmitidas no

mesmo cabeçalho) até que o tamanho desse campo seja múltiplo de 32 bits.

- Dados: o tamanho desse campo não é fixo, podendo ter até 65.535 bytes (64 KB). O tamanho da área de dados é chamado MSS (*Maximum Segment Size*), que especifica a maior quantidade de dados que um computador ou dispositivo de comunicação pode receber em um datagrama IP.

“Os dados circulam na Internet sob forma de datagramas (ou pacotes). ’ ‘Os datagrama são dados encapsulados, isto é, são dados aos quais se acrescentam cabeçalhos que correspondem a informações sobre o seu transporte, como por exemplo, o endereço IP.” [24]

“Os dados contidos nos datagramas são analisados e eventualmente alterados pelos roteadores que permitem o seu trânsito.” [24]

3.4 ICMP

“É um protocolo de mensagens de controle usado para informar outros dispositivos de importantes situações das quais podemos citar, por exemplo: fluxo de mensagens maior que a capacidade de processamento de um dispositivo, parâmetro TTL, e mensagens de redirecionamento. ’ ‘Eventualmente um roteador pode estar recebendo mais informação do que pode processar, sendo assim ele passa a contar com controle de fluxo, enviando uma mensagem source quench, para o dispositivo de origem para que ele pare ou diminua o fluxo de dados. ’ ‘Esta mensagem é enviada pelo protocolo ICMP.” [17]

“O segundo caso evolve o parâmetro TTL que basicamente é o número de hops (roteadores) total que uma informação pode percorrer. ‘ ‘Ele é decrementado a cada hop e quando chega à zero, o roteador descarta o datagrama e envia uma mensagem à fonte informando que a informação não chegou ao seu destino, utilizando o ICMP.” [17]

“O terceiro caso é a mensagem de redirecionamento ICMP, que é utilizada quando o roteador determina que um caminho melhor exista para o pacote que acabou de ser enviado assim mesmo. ’ ‘Neste caso, a implementação do protocolo de roteamento pode definir um novo caminho de acordo com este melhor caminho. ‘ ‘Alguns

sistemas operacionais de roteamento não consideram esta mensagem e continuam enviando dados pelo pior caminho.” [17]

O ICMP faz parte da pilha TCP/IP, localizando-se na camada de rede (camada 3), a mesma camada do protocolo IP. “Ele também é similar ao protocolo UDP, pois suas mensagens cabem num só datagrama, mais não é considerável um protocolo de alto nível como o UDP ou o TCP, sendo, no entanto ainda mais simples uma vez que possui a indicação no seu cabeçalho das portas; utilizando o IP para o transporte de mensagem, não oferecendo garantia de entrega podendo acontecer de a própria mensagem ICMP ser perdida no meio do caminho.” [7] Assim na figura 7 mostra como uma mensagem ICMP é encapsulada em um datagrama IP.

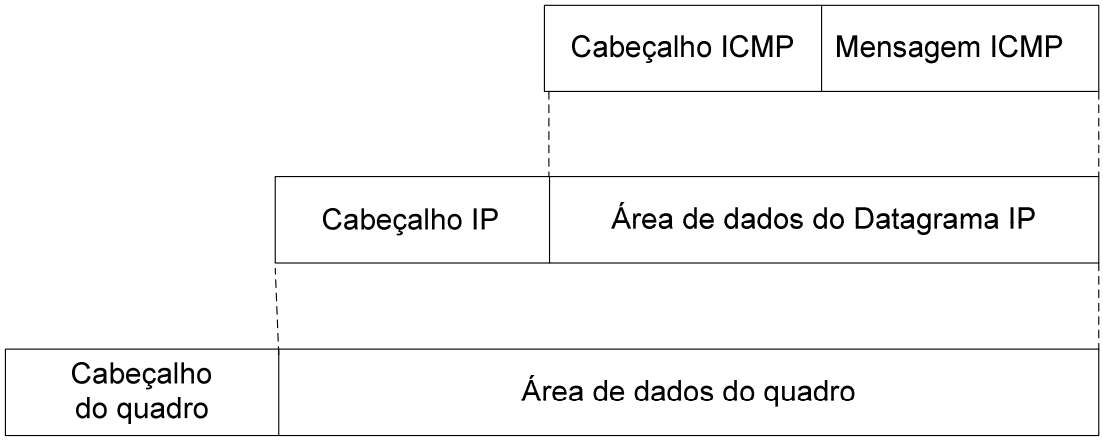

Figura 7 - Mensagem ICMP
FONTE: [2]

“Ocorrendo algum problema previsto por esse protocolo, uma mensagem ICMP descrevendo a situação é preparada e entregue à camada IP, que a adiciona ao seu cabeçalho e envia ao emissor do datagrama com o qual ocorreu o problema.” [7]

O formato geral de uma mensagem ICMP é apresentado na figura 8. “O campo TIPO identifica a mensagem ICMP particular, o campo CÓDIGO é usado na especificação dos parâmetros da mensagem e o campo CHECKSUM corresponde ao código verificador de erro, calculado a partir da mensagem ICMP completa;” [7] sendo que os campos, IDENTIFICADOR e NÚMERO DE SEQÜÊNCIA nem sempre estarão presentes.

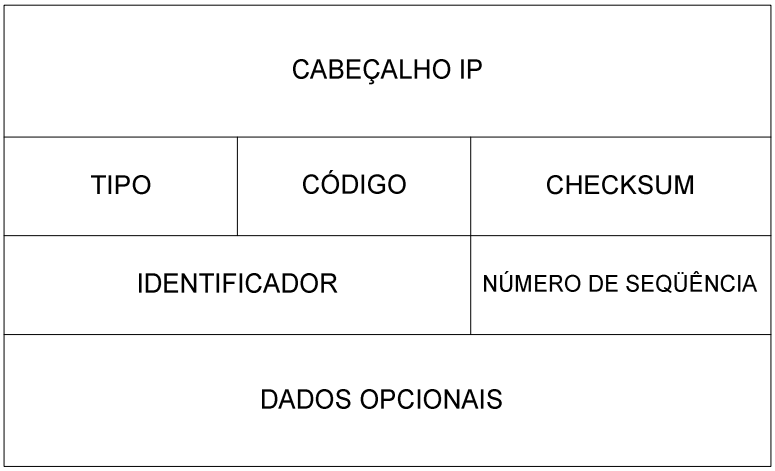

Figura 8 - Pacote ICMP
FONTE: [7]

Esse protocolo possui os seguintes tipos de mensagens:

- *Destination unreachable*: não foi possível entregar o pacote;
- *Time exceeded*: o campo *Time To Live* chegou a 0;
- *Parameter problem*: campo de cabeçalho inválido;
- *Source quench*: pacote regulador;
- *Redirect*: ensina geografia a um roteador;
- *Echo*: pergunta a uma máquina se ela está ativa;
- *Echo reply*: sim, estou ativa;
- *Timestamp request*: igual à *Echo*, mas com timbre de hora;
- *Timestamp reply*: igual à *Echo reply*, mas com o timbre de hora.

O uso mais comum do ICMP é feito pelos utilitários *Ping* e *Traceroute*. A principal diferença entre esses comandos é que o *Ping* é uma forma rápida e fácil de dizer se o servidor de destino está online e estimativas de quanto tempo leva para enviar ands e receber dados para o destino. Já o *Traceroute* diz-lhe a rota exata que se deve tomar para alcançar o servidor de seu computador (ISP, *Internet Service Provider*) e quanto tempo leva cada salto.

3.4.1 *Ping*

Conhecido de *PING* (*Packet Internet Grouper*) ou *Ping* é um comando utilizado para testar se existe um endereço IP acessível ou não.

Assim, pela descrição de MARQUES, 2000, p. 138:

> É um dos utilitários mais conhecidos. Um de seus maiores objetivos é testar se um endereço está ativo, enviando pacotes de teste ao mesmo e esperando resposta (vide ICMP) tendo outras diversas aplicações. [3]

"Para utilizá-lo, basta executá-lo através de um *Prompt* de Comando ou terminal que pode ser em *Windows*, *Linux* ou *Macintosh*;" [28] utilizando o *Windows* digita-se no *Prompt Ping* espaço nome do domínio, como um site ou endereço IP, e Enter para confirmar.

Esse utilitário permite que se realize um simples teste com a finalidade de se descobrir se um determinado equipamento de rede está funcionando e se o mesmo está acessível via rede, e quanto tempo está levando para os pacotes de informações "viajarem" a partir do seu computador para o servidor de destino, com um tempo de resposta (TTL). Esses pacotes chamados ICMP são pequenos blocos de dados, geralmente 32 bytes de informação. Com isso, digitando o endereço *www.google.com*, tem-se a figura 9 com o funcionamento do *Ping*.

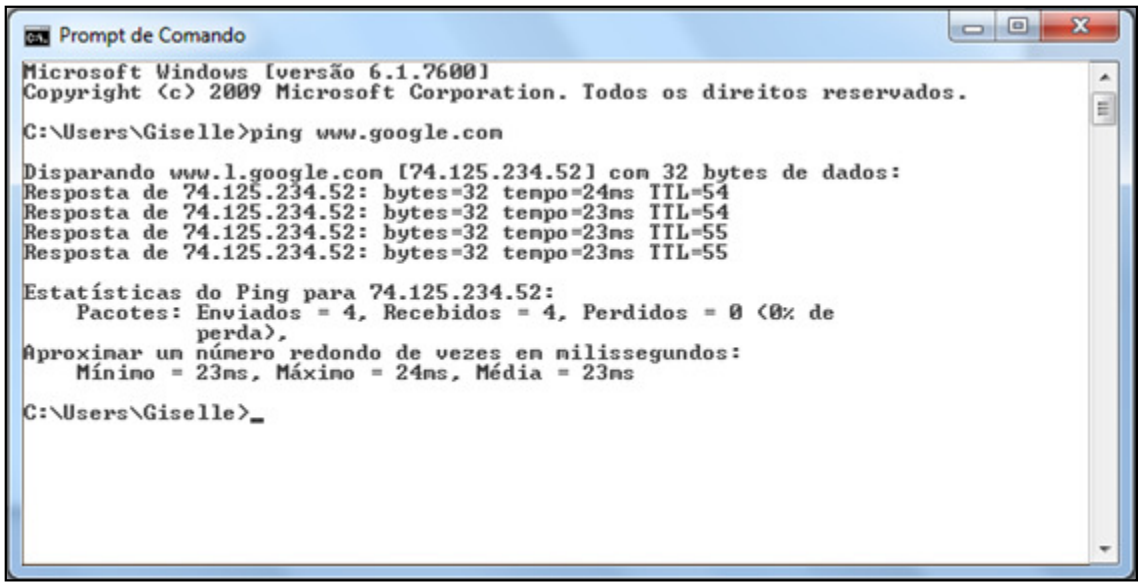

Figura 9 - *Prompt* de Comando, utilizando o comando *Ping*

Esse comando possui as seguintes opções mostradas na figura 10.

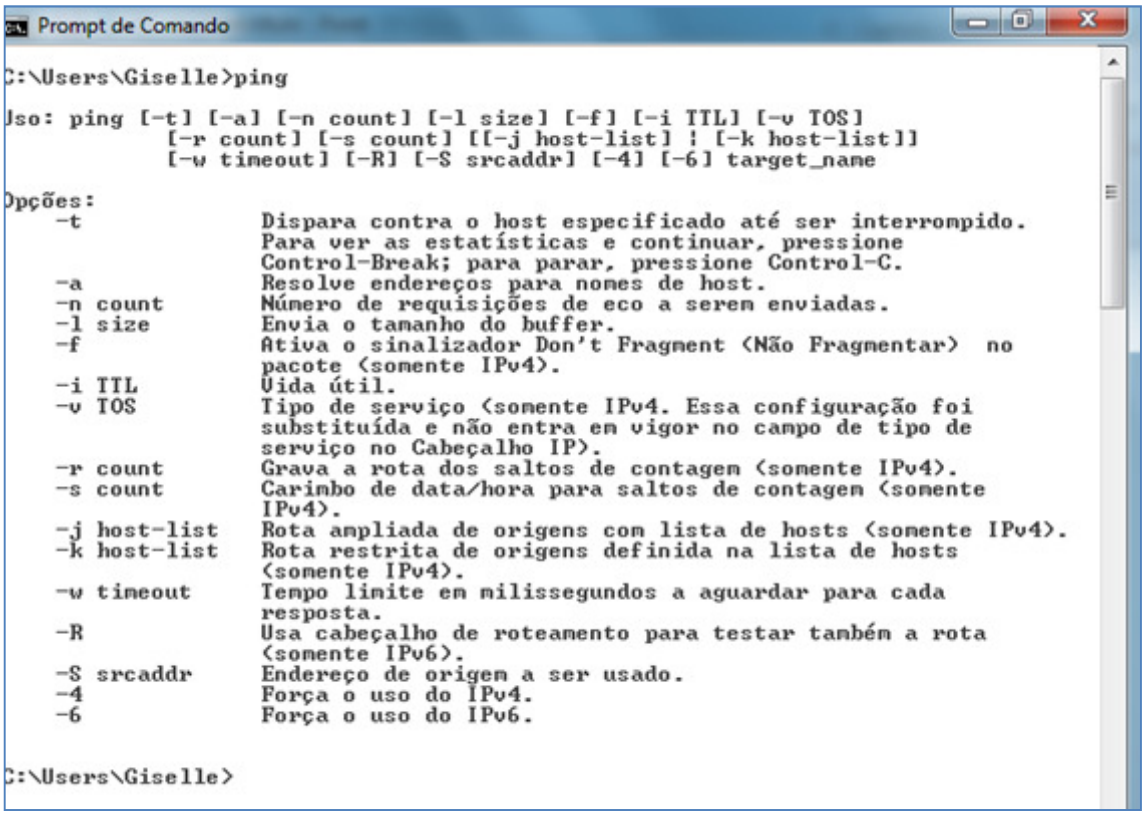

Figura 10 - *Prompt* de Comando, mostrando as opções do *Ping*

3.4.2 *Traceroute*

É um utilitário *UNIX*, mas quase todas as plataformas têm algo semelhante. O Windows inclui um utilitário chamado *Traceroute tracert*. Como exemplo, em um computador com *Windows*, pode-se executá-lo através de um *Prompt* de Comando, assim abrindo a sua janela: digite *tracert* espaço nome do servidor de destino, endereço de internet ou um endereço IP, como por exemplo *www.google.com* e Enter pra confirmar; dessa forma, será visualizada a quantidade de saltos que o computador leva até chegar ao seu destino, mostrando que qualquer salto que aparecer com o * significa Esgotado o tempo limite do pedido, sendo que este congestionamento da rede representa um motivo de carregamento lento de páginas web e quedas de conexão.

“Este comando obtém os endereços IP dos roteadores intermediários entre a origem e o destino, isto é, traça a rota entre ambos, acompanhando o caminho que o pacote leva de seu computador até o endereço de destino. ‘ ‘Sua operação é baseada na manipulação do campo TTL de datagrama IP e tratamento das mensagens ICMP *Time Exceeded* geradas a partir desta manipulação.” [28]

Abaixo a figura 11 mostra o exemplo proposto no texto do funcionamento do comando *tracert*.

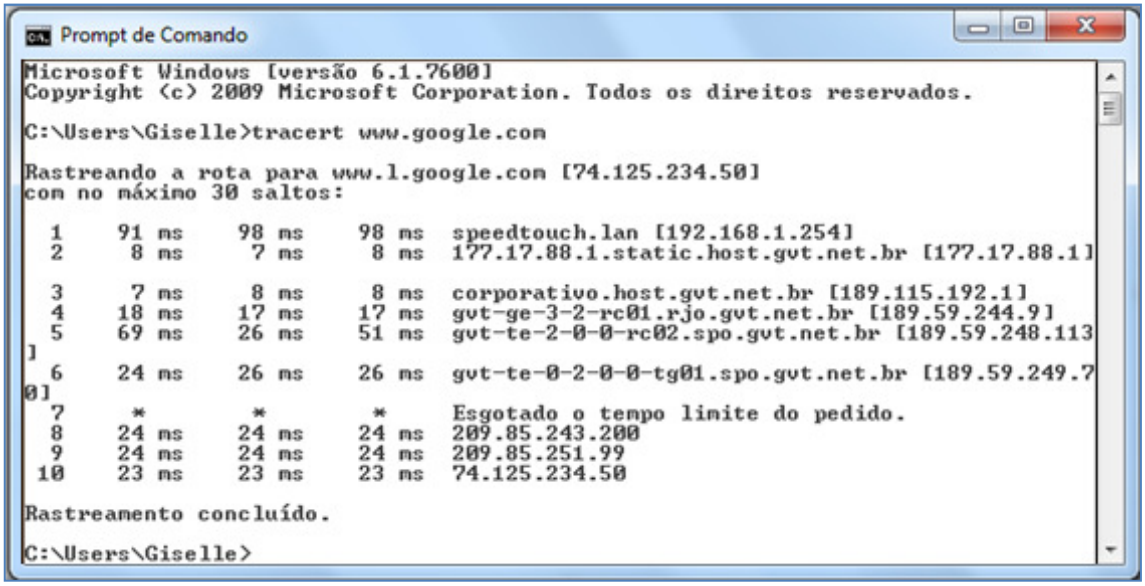

Figura 11 - *Prompt* de Comando, utilizando o comando tracert

Esse comando *tracert* tem várias opções quando utilizado, como por exemplo, mostrado na figura 12, digitando apenas o nome do mesmo no *Prompt*.

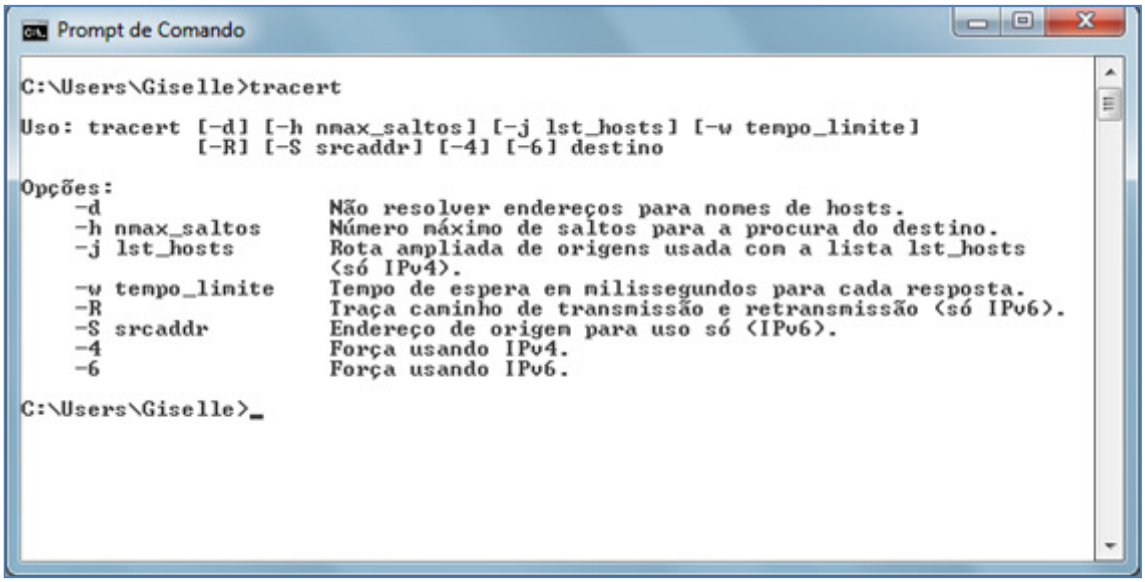

Figura 12 - *Prompt* de Comando, mostrando as opções do tracert

3.5 *IPCONFIG*

É um comando utilizado para controle de conexões de rede. Para executá-lo, utiliza-se o *Prompt* de Comando, digitando *ipconfig* e Enter pra confirmar, em sua interface aparecem algumas informações, tais como mostra a figura 13.

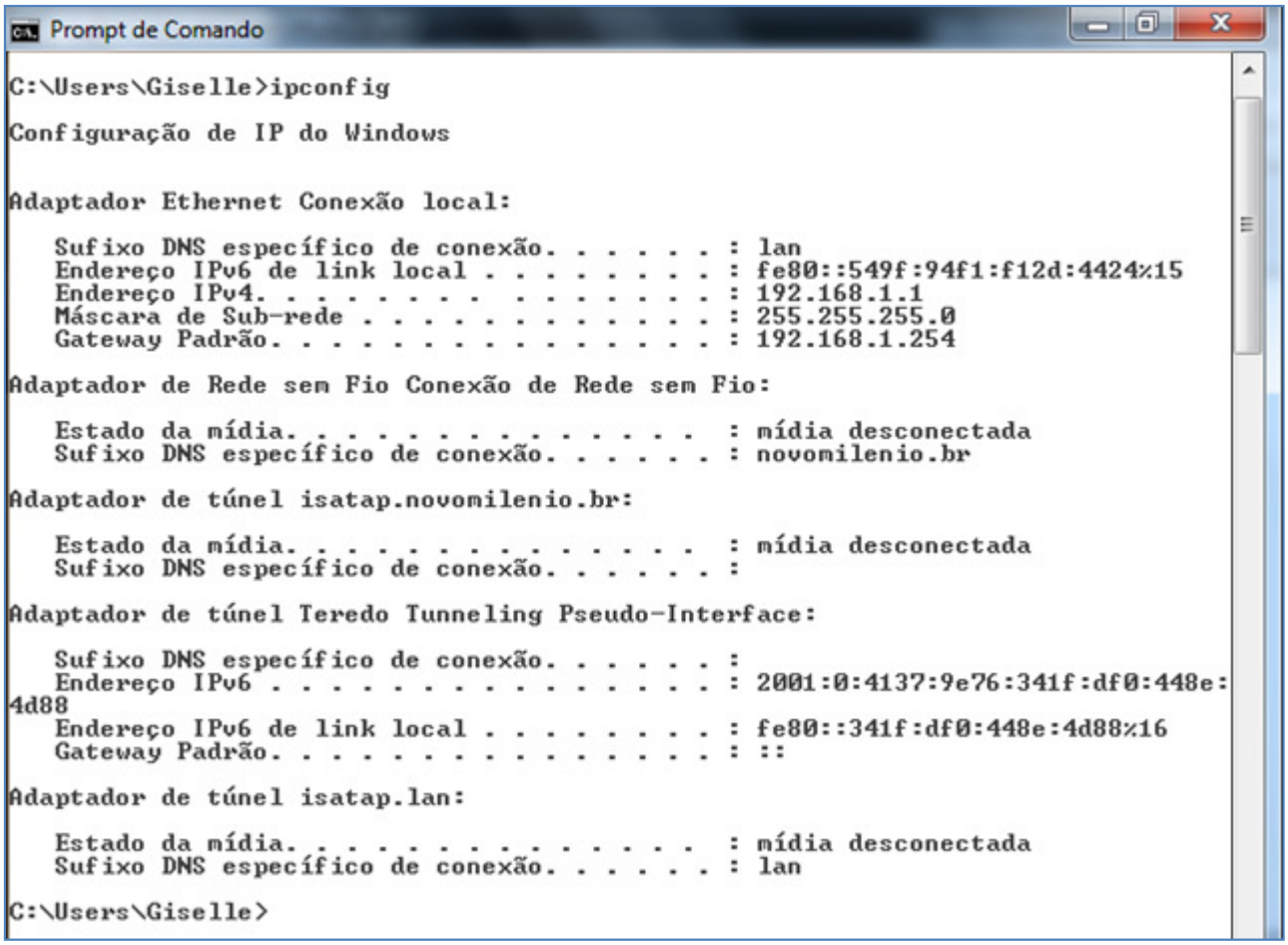

Figura 13 - *Prompt* de Comando, utilizando o comando *ipconfig*

Esse aplicativo fornece algumas opções de comando, tais como:

- “Ipconfig /all” - Exibe todas as informações de configuração das interfaces de redes instaladas.
- “Ipconfig /release” - Libera o endereço IP do adaptador especificado.
- “Ipconfig /renew” - Renova o endereço IP para o adaptador especificado.
- “Ipconfig /flushdns” - Limpa o cache de resolução DNS.
- “Ipconfig /registerdns” - Atualiza todas as concessões DHCP e torna a registrar os nomes DNS.
- “Ipconfig /displaydns” - Exibe o conteúdo de cache de resolução de DNS.

A figura 14 mostra todas as opções deste comando, utilizando o “ipconfig ()” ou um comando *ipconfig* inválido. Onde digitando este comando e Enter pra confirmar aparecem as opções possíveis para utilizar o *ipconfig*.

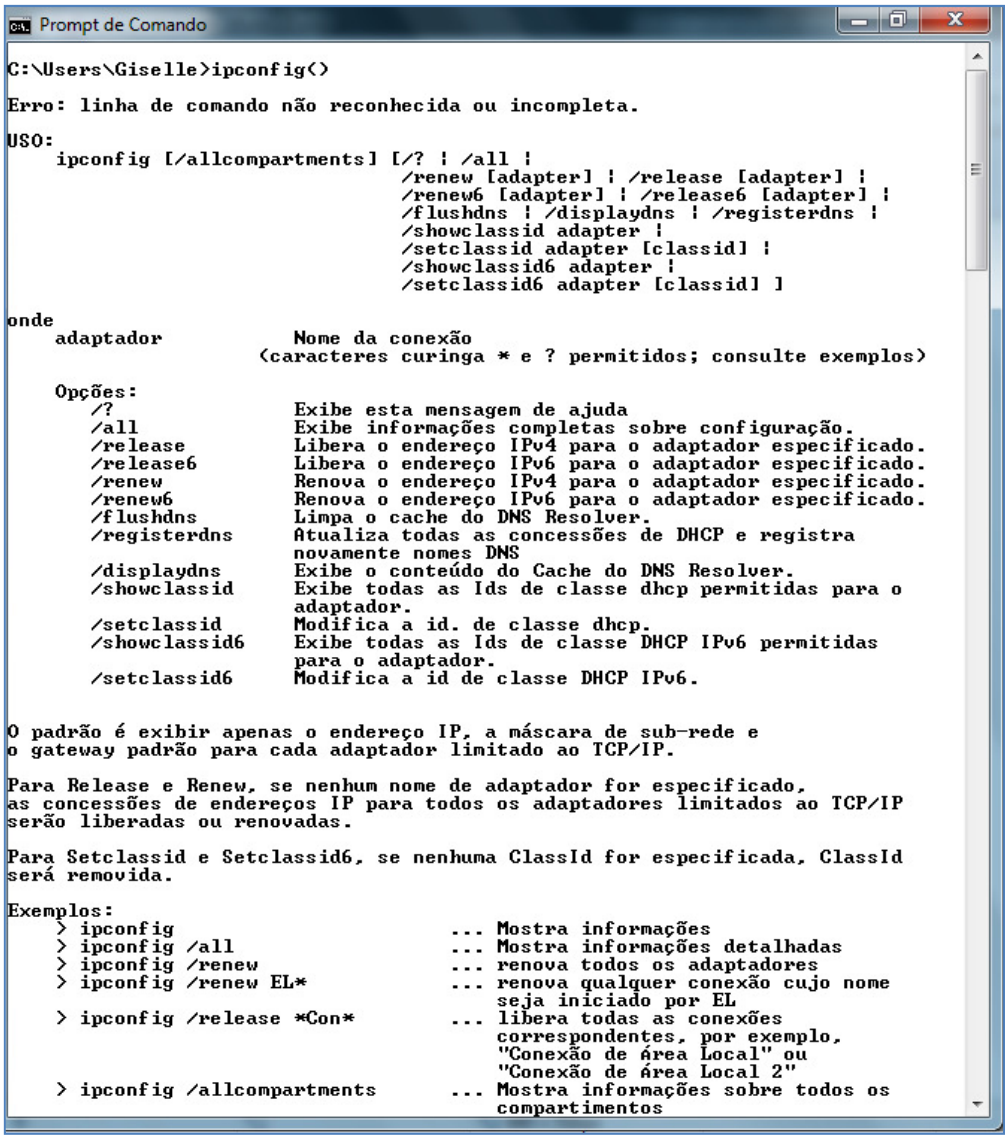

Figura 14 - *Prompt* de Comando, mostrando as opções do comando *ipconfig*, utilizando o comando "ipconfig ()"

3.6 IPV6

A Internet nos últimos anos tem aumentado o seu número de usuários, assim os números de endereços IPs disponíveis estão se esgotando e a previsão de termino do último lote do IPv4 foi no primeiro semestre de 2011, dessa forma implementando o IPv6 (Internet Protocol versão 6), protocolo mais atual do protocolo IP, trazendo um espaço de endereçamento capaz de suportar o crescimento da rede indefinidamente e avanços em áreas como segurança, mobilidade e desempenho.

O endereçamento IPv6 tem o tamanho de 128 bits separados em grupos de 16 bits, e cada grupo de 16 bits usa quatro algarismos hexadecimais, tendo um total de 32 caracteres, organizados em oito quartetos e separados por dois pontos, com isso cada caractere representa 4 bits (16 combinações). “O número de endereços disponíveis no IPV6 é simplesmente absurdo; seria o número 340.282.366.920 seguido por mais 27 casas decimais. ’ ‘Devido a isso forma além dos números de 0 a 9, tem-se os caracteres A, B, C, D, E e F, que representariam os números 10, 11, 12, 13, 14 e 15;” [22] um exemplo desse endereço é o 1234:AFE4:0000:0000:18A4:000A:0000:18CD, admitindo dois tipos de abreviações: uma é esconder os zeros à esquerda 1234:AFE4:0:0:18A4:A:0:18CD podendo ser repetido e a outra é substituir o intervalo de um grupo de zeros por “::”, 1234:AFE4::18A4:000A:0000:18CD não podendo repeti-lo.

Ao configurar endereços dentro de uma mesma rede, existem duas opções. A primeira seria simplesmente usar endereços seqüenciais, como "2001:bce4::1", "2001:bce4::2", "2001:bce4::3" e assim por diante; e, a segunda seria seguir a sugestão do IETF (*Internet Engineering Task Force*) e usar os endereços MAC das placas de rede para atribuir os endereços dos *host*s, sendo justamente o que acontece ao utilizar a atribuição automática de endereços no IPV6.

De acordo com TORRES, 2009, p. 261:

> Em redes operando como IPv4 e o IPv6 ao mesmo tempo, endereços IPv4 podem ser facilmente convertidos em IPv6 usando a notação x:x:x:x:x:x:a.b.c.d, onde x:x:x:x:x:x são os seis primeiros grupos do endereço IPv6 e a.b.c.d é o endereço IPv4. Por exemplo, o endereço 192.168.1.2 seria representado como 0:0:0:0:0:0:192.168.1.2 ou simplesmente ::192.168.1.2.
>
> É interessante notar que esse endereços mistos possuem um equivalente puramente IPv6, bastando para isso converter cada numero usado no IPv4

> de decimal para hexadecimal e separá-los com um sinal de dois pontos. O endereço ::192.168.1.2 é equivalente a ::C0A8:0102 (192=C0, 168=A8, 1=01, 2=02), ou simplesmente ::C0A8:102. [2]

É possível também adicionar um endereço IPv6 a um computador já configurado com endereço IPv4, sem precisar derrubar a rede. Neste caso, ele continua respondendo normalmente no endereço IPv4 antigo, sendo este o principal de seus objetivos que é manterem a compatibilidade, já que muitos sistemas provavelmente não serão atualizados, mas responde também no endereço IPv6. A maior parte da internet já utiliza o novo sistema, mas seu provedor de acesso ainda oferece suporte apenas a endereços IPv4. Para se entender as diferenças entre o IPv6 e o IPv4 temos o quadro 8 a seguir:

	IPv6	IPv4
Espaço de endereçamento	128bits	32bits
Suporte para o IP móvel	Bom suporte para o IP Móvel	Suporte precário
Segurança	Oferece cabeçalhos para inserir segurança	Nenhuma Segurança
Autoconfiguração	Padrão da versão	Não existe

Quadro 8 - Comparação do IPv6 com o IPv4
FONTE: [21]

O suporte a IPV6 está presente nas distribuições atuais do *Linux* e do *Windows* e a definição do formato de endereços IPv6 encontra-se na RFC 2373.

As máscaras de rede do IPv6 são feitas no formato CIDR e por padrão os 64 primeiros bits são reservados para endereço de rede e a outra metade é para endereço de máquina chamada de IID (*Interface IDentifier*). Esta parte IID que identifica a maquina é criada usando o endereço MAC, mas o endereço MAC tem 48 bits e a parte IID tem 64 bits, a conversão é feita adicionando o valor “FFFE” no meio do endereço MAC, como por exemplo, temos o MAC 0080AD0ACDDC para o IDD 02:80:AD:FF:FE:0A:CD:DC, nota-se que no começo do IID não esta igual ao começo do número MAC isso acontece porque o bit “Universal/Local” (bit 41 do endereço MAC e 57 no IID) passa do valor 0 para o valor 1 fazendo a mudança da representação em hexadecimal, mostrado na figura 15.

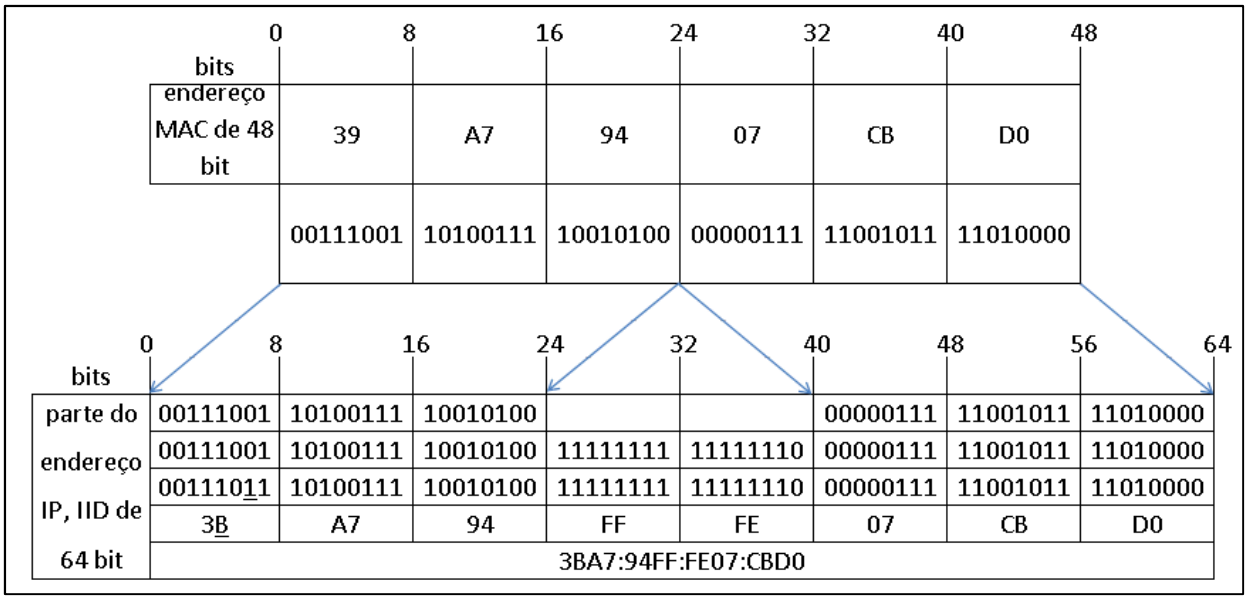

Figura 15 - Conversão do endereço MAC em IID
FONTE: [25]

Existem três tipos básicos de endereço IPv6:

*Unicas*t: usado para identificar uma única interface (placa de rede).

Anycast: utilizado para identificar um grupo de placas de rede que tipicamente pertencem a nós (máquinas) diferentes. O pacote é entregue somente a interface mais próxima definida pelo protocolo de roteamento.

Multicast: usado para identificar um grupo de placas de rede que pertencem a máquinas diferentes. O datagrama é entregue a todas as maquinas do grupo. O IPv6 não usa o endereço de *broadcast*, pois o pacote só irá para as máquinas da rede que tiverem o mesmo endereço de *multicast* configurado.

4 ROTEAMENTO

É o mecanismo utilizado para a entrega de pacote de dados entre *host*s (equipamentos de rede, como computadores e roteadores). “Seu modelo é do *hop-by-hop* (salto-por-salto), onde cada roteador que recebe um pacote de dados abre e verifica o endereço de destino no cabeçalho IP, calcula o próximo salto para deixar o pacote mais próximo de seu destino e o entrega neste próximo salto. ‘ ‘Este processo se repete e assim segue até a entrega do pacote ao seu destinatário, sendo que, para isso funcionar, é necessário dois elementos: protocolos de roteamento e tabelas de roteamento.” [6]

Existem vários tipos de roteamento, assim de acordo com a referência [8], temos:

- Roteamento Direto: comunicação entre dois *hosts* (roteadores) alocados em uma mesma rede física;
- Roteamento Indireto: conexão entre dois *hosts* alocados em redes distintas, sendo necessário o uso de *Gateways* para efetuar o encaminhamento dos pacotes a rede destino;
- Roteamento Interno: são roteadores utilizados para a troca de informações dentro do mesmo Sistema Autônomo (AS), considerados vizinhos interiores, utilizando-se o protocolo IGP (*Interior Gateway Protocol*), como por exemplo, o RIP e o OSPF;
- Roteamento Externo: São roteadores que trocam dados entre Sistemas Autônomos que não pertencem ao mesmo sistema, considerados vizinhos exteriores, utilizando-se o protocolo EGP (*Exterior Gateway Protocol*) para se comunicarem. Esse protocolo é um exemplo do BGP, que tem as características de suportarem mecanismos de aquisição de vizinhos, os testando continuamente para ver se estão respondendo e divulgando informações entre os mesmos utilizando mensagens de atualização de rotas.
- Roteamento Hierárquico: é realizado em áreas chamadas regiões, sendo que cada roteador só conhece apenas a sua região, assim para grande regiões são necessárias algumas subdivisões (zonas de *clusters*, *clusters* de regiões, etc.) para que os roteadores possam trabalhar com eficiência;
- Roteamento por *Broadcast*: os pacotes são enviados para todos os roteadores simultaneamente, abordagem por difusão;

- Roteamento por *Multicast*: os pacotes são enviados para um grupo seleto de roteadores existindo a necessidade da figura de gerência de grupos.

Roteadores por operarem na Camada de Rede, usam o sistema de endereçamento lógico dessa camada chamado endereço IP. E também por operarem na camada de Rede do Modelo OSI são capazes de fragmentar (dividir) os datagramas recebidos. Para uma melhor visualização deste equipamento (roteador) são mostrados vários tipos na figura 16.

Figura 16 - Tipos de Roteadores
FONTE: [14]

"Cada roteador é um dispositivo responsável pelo recebimento e redirecionamento dos pacotes na rede", [8] tendo as funções básicas: permitir a conexão de duas redes diferentes isolando cada rede, mantendo separados seus domínios de *broadcast*; e, escolher um caminho a ser usado para o datagrama chegar ao seu destino, assim é necessário a configuração de rotas em uma tabela de roteamento para um "conversar" com o outro, dessa forma, utilizando os protocolos de roteamento acontece à comunicação com os roteadores vizinhos.

4.1 TABELA DE ROTEAMENTO

“São registros de endereços de destino associados ao número de saltos até ele, podendo conter várias outras informações [6]”, como por exemplo, rotas criadas entre roteadores e computadores. “Esta tabela possui uma entrada informando o que fazer quando chegar um datagrama com um endereço desconhecido.” [5] Dessa forma visualizamos a seguir a figura 17:

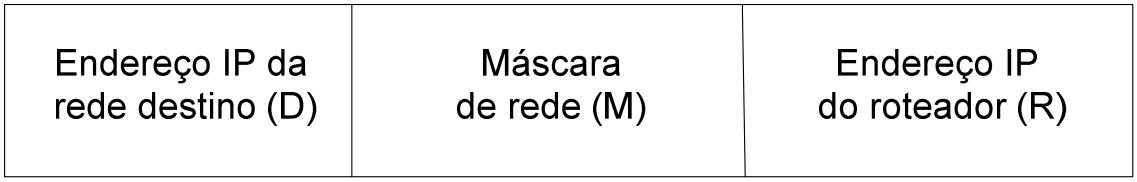

Figura 17 - Estrutura da entrada da Tabela de Roteamento
FONTE: [9]

“De acordo com a figura, cada entrada especifica uma rede destino, a sua máscara de rede e o próximo roteador a ser usado para se chegar a esta rede.” [9]
“Essas tabelas podem ser classificadas em estáticas e dinâmicas. ’ ‘As estáticas são conhecidas como rotas diretas e estáticas, e são inseridas informações de maneira direta não existindo a possibilidade de mudança. ’ ‘Já as dinâmicas são montadas e atualizadas constantemente, visando possibilitar a comunicação entre roteadores de forma dinâmica, através de protocolos de comunicação roteador-roteador. ’ ‘Esta é a forma mais tradicional de operação de protocolos de comunicação, pois em redes grandes como a Internet os roteadores se reconfiguram quando as condições da rede são alteradas, sem a necessidade de intervenção de um indivíduo.” [8]

4.2 ROTEAMENTO ESTÁTICO

É o roteamento predefinido, parado, estacionado, as rotas serão sempre as mesmas, definidas manualmente através de tabelas de roteamento do roteador que usa o mesmo caminho para enviar um datagrama ao destino, por isso é sujeito a falhas de configuração.

4.3 ROTEAMENTO DINÂMICO

É o roteamento que permite aos próprios roteadores mudarem a rota de acordo com as novas necessidades da rede, decidindo dinamicamente com a troca de informação entre roteadores para qual caminho deve-se seguir através de dois critérios: o caminho mais curto ou o menos congestionado. Os protocolos dinâmicos podem ser divididos também entre protocolos internos (IGP) e os externos (EGP).

4.4 PROTOCOLOS DE ROTEAMENTO

São responsáveis pela divulgação de rotas, atualização das informações das tabelas de roteamento.

Esses protocolos são baseados em algoritmos de roteamento, aos quais adotam diferentes abordagens, que de acordo com a referência [8] são:

- Protocolos de roteamento adaptativo: baseados em algoritmos adaptativos, as decisões que são tomadas constituem um reflexo da carga da rede e de possíveis trocas na topologia da rede;
- Protocolos de roteamento não-adaptativo: baseados em algoritmos não-adaptativos (ou estáticos), não consideram suas decisões medidas (ou estimativas de tráfico) e a topologia da rede.

O *algoritmo* de roteamento é o *software* responsável por decidir sobre qual linha de saída o pacote recebido deverá ser transmitido, “tem-se a função de montar uma tabela para que o roteamento dos pacotes seja efetuado de forma precisa”. [8]

“Protocolos de roteamento são projetados para serem ferramentas capazes de realizar várias tarefas como: *throughput* (velocidade de transmissão); qualidade dos circuitos entre os roteadores; status operacional de roteadores específicos; número de pontos intermediários (ou *hops*) que um pacote irá passar; caminhos alternativos disponíveis em caso de falha na rede;” [8] retardos de propagação; retardos de enfileiramento, custo do *link* e etc.

“Estes protocolos podem operar de duas formas: informando o menor caminho para atingir uma rede (protocolos baseados na distância) ou então informando o melhor

caminho, que nem sempre é o menor caminho, em geral é o caminho menos congestionado (protocolos baseados em estado de *link*).” [2]

“Os baseados na distância mais conhecidos são o RIP (usado pelo IP e pelo IPX, *Internetwork Packet Exchange*), o EIGRP (*Enhanced Interior Gateway Routing Protocol*) e o IGRP (*Interior Gateway Routing Protocol*, usados por roteadores *Ciscos*) e o RTMP (*Real Time Messaging Protocol*, usado pelo *AppleTalk*). Já os baseados em estado de *link* mais conhecidos são o OSPF (usado pelo IP), o NLSP (*Netware Link Service Protocol*, usado pelo IPX) o PNNI (*Private Network-to-Network Interface*, usado pelo ATM, *Asynchronous Transfer Mode*) e o IS-IS. ’ ‘E tem-se o BGP sendo o protocolo por vetor de caminho, que funciona baseado na distância caso nenhum parâmetro adicional seja especificado, isto é, parâmetros adicionais podem fazer este protocolo escolher outro caminho que não necessariamente é o mais curto.” [2]

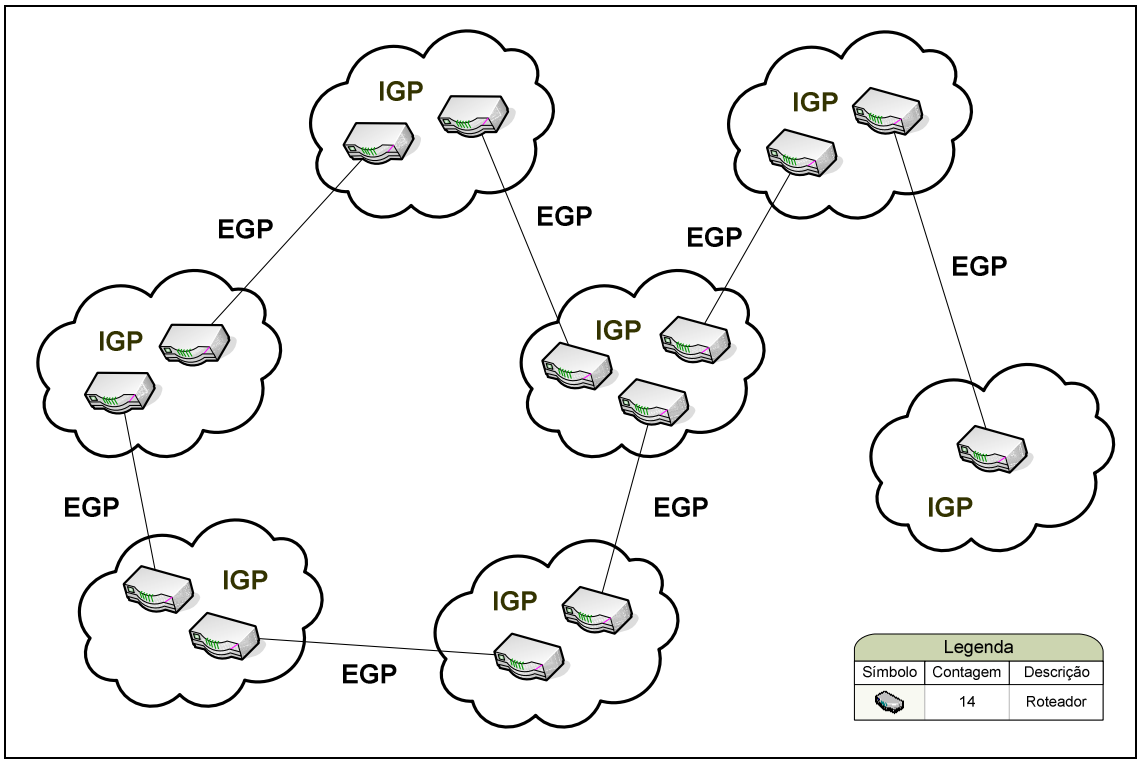

Figura 18 - Exemplo de Funcionamento da Internet
FONTE: [2]

Assim, abordaremos a seguir os seguintes protocolos RIP, o OSPF (IGP) e o BGP (EGP).

4.4.1 Protocolos RIP

Este protocolo foi um dos primeiros utilizados em TCP/IP e também tem sido o mais popular protocolo de roteamento interior. Pois é um dos protocolos mais fáceis de configurar e menos exigente em recursos de todos os protocolos de roteamento.

"É um protocolo que tenta descobrir o caminho mais curto entre as redes, ele envia sua tabela de roteamento para os outros roteadores da rede de 30 em 30 segundos, nessa tabela consta as redes conhecidas e a distância entre elas que é dada em saltos, ou seja, o número de roteadores que o datagrama (pacote) tem que passar para chegar ao seu destino." [5]

As vantagens desse protocolo são: em redes pequenas não depende de muita largura de banda e tempo de configuração e gerenciamento e, também de fácil implementação. Já as desvantagens: convergência lenta para redes de tamanho médio ou grande, existência de loops e contagem ao infinito, e também limitações de métrica: número máximo de saltos por caminho (15).

O protocolo RIP tem várias versões como o RIPv1 (*Routing Information Protocol version 1*) que não permite usar máscaras de sub-rede, RIPv2 (*Routing Information Protocol version 2*) que possibilita a autenticação (senha), e RIPng que suporta o IPv6 ou IPng que não usa autenticação, mas usa o protocolo IPsec (*IP Security Protocol*), que é um protocolo para transportar a mensagem RIPng (*Routing Information Protocol next generation*).

Nas mensagens de RIPv1 as informações de rota são trocadas em RIP através do envio de dois tipos diferentes de mensagens RIP: Pedido de RIP e RIP resposta. Essas mensagens possuem vários campos que variam de acordo com a quantidade dependendo da versão, e os campos que mostram a rota a ser seguida podem ser repetidos até no máximo 25 vezes, isto significa que podem passar por 25 roteadores, porém o RIP considera o número de saltos maior que 15 como "infinito". Caso o roteador seguinte estiver congestionado ele manda uma mensagem ICMP para o roteador anterior dizendo para reduzir a velocidade. Estes tipos são transmitidos como TCP regular/ IP mensagens usando o UDP.

Como o RIPv1 tem vários problemas e limitações devido à evolução de funcionalidades IP, pois o protocolo TCP/IP evoluiu e mudou, criou-se o RIPv2 que foi desenvolvido e publicado em 1993 inicialmente na RFC 1388, sendo o

documento que descreve os padrões desse protocolo. Agora é definido na RFC 2453 o RIP versão 2, publicada em novembro de 1998.

RIPv2 é a versão mais recente do RIP usado em IPv4, incluindo uma série de melhorias em relação ao original RIPv1, como suporte para máscaras e sem classe de endereçamento, especificação do próximo salto, marcação de percurso, autenticação e, *multicast* que entrega a informação para vários destinos ao mesmo tempo e a mensagem passa por um caminho (*link*) uma única vez. Para compatibilidade, ele usa o formato da mensagem básica, a mesma do RIPv1, colocando a informação extra, necessária para as suas novas funcionalidades em alguns dos campos não utilizados da uma mensagem de formato RIP. Nas suas mensagens são trocadas usando o mesmo mecanismo básico RIPv1 mensagem. Dois diferentes tipos de mensagens existentes, solicitação RIP e RIP resposta. Eles são enviados usando UDP número de porta reservada. A semântica para o uso desta porta é o mesmo que para o RIPv1.

O futuro do TCP/IP é o novo protocolo Internet versão 6 (IPv6), que faz algumas mudanças muito importantes para o IP, especialmente com relação à resolução. Como os endereços IPv6 são diferentes de endereços IPv4, tudo o que funciona com endereços de IP deve mudar para funcionar em IPv6. Isto inclui os protocolos de roteamento, que troca informações de endereçamento.

Para garantir um futuro para o *Routing Information Protocol*, um IPv6 compatível com a nova versão tinha que ser desenvolvido. Esta nova versão foi publicada em 1997 no RFC 2080, RIPng para o IPv6, onde o ng representa a próxima geração (IPv6 também é às vezes chamado de “próxima geração de IP”).

RIP, que também é ocasionalmente vista como RIPv6 (*Routing Information Protocol version* 6) por razões óbvias, foi projetado para ser o mais semelhante possível com a versão atual do RIP para IPv4, o que é RIP versão 2 (PIRv2). Na verdade, RFC 2080 descreve RIPng como "a mudança mínimo" possível RIP para permitir que ele funcione em IPv6. Apesar deste esforço, não foi possível definir RIPng como apenas uma nova versão do protocolo RIP mais antigos, como foi o RIPv2. RIPng é um novo protocolo, que foi necessário devido à importância das alterações entre IPv4 e IPv6, especialmente a mudança de 32 bits para endereços de 128 bits no IPv6, o que implicou um novo formato de mensagem.

4.4.2 Protocolos OSPF

É um protocolo de roteamento baseado no estado do *link* que pode ser traduzido como protocolo aberto de roteamento baseado no estado do *link*, no protocolo RIP os roteadores demoram muito tempo para descobrir que há algo de errado na conexão com outro roteador ou rede, o RIP também fica enviando suas tabelas de roteamento a cada 30 segundos, já o OSPF testa a conexão periodicamente de 10 em 10 segundos, cada roteador testa o estado do *link* com os roteadores que ele estiver conectado diretamente, essas chamadas são as LSA (*Link-State Announcement*), com essa descoberta cada roteador monta um Banco de Dados Baseado no Estado do *Link* (LSDB, *Link-State Database*) e periodicamente os roteadores mandam seu banco de dados para os outros roteadores, depois de um tempo todos os roteadores terão o mesmo LSDB, conhecendo todos os caminhos que os interligam e poderão não só escolher o menor caminho, mas sim o de melhor desempenho.

O OSPF permite o balanceamento de carga caso houver mais de uma rota para um mesmo destino, também inclui roteamento baseado na qualidade do serviço (QoS): atraso máximo e confiabilidade. Cada roteador cria um banco de dados separado para cada métrica isso faz com que dependendo do serviço requerido o caminho mude e também como no RIPv2 o OSPF pode usar autenticação. Esta versão do OSPF é a segunda, a primeira não se usa mais desde 1991, a terceira versão é usada para o IPv6.

Existem duas topologias de rede que o OSPF consegue trabalhar: a básica (roteadores ligados ponto-a-ponto) que serve para redes básicas e a topologia hierárquica utilizada para redes grandes que divide o sistema autônomo em varias áreas que funcionam como se fossem sistemas autônomos separados. Cada área é numerada e gerenciada pelos roteadores daquela área que funciona como se fosse uma rede básica. Do lado de fora dessas várias áreas ficam os roteadores que se interligam as outras áreas, esses roteadores recebem, coletivamente, o nome de "área 0" ou roteadores de Backbone.

Os roteadores da estrutura hierárquica são divididos dessa maneira:

- Internos: ficam dentro de cada área e não se conectam com a área 0;
- De Fronteira: aparecem dentro de cada área fazendo conexão com a área 0;

- De *Backbone*: presentes somente na área 0. Os roteadores de Fronteira também são de *Backbone*, mas o inverso não acontece.

As mensagens OSPF são enviadas dentro de datagramas IP. Nestes datagramas, o campo protocolo é colocado como valor 89, de forma a identificar que o datagrama esta carregando uma mensagem OSPF. As mensagens são dividas em dois campos: cabeçalho que usa a mesma estrutura para todas as mensagens OSPF, e mensagem em si, cuja estrutura varia de acordo com o tipo de mensagem que está sendo transmitida.

Tipos de mensagem do OSPF:

- *Hello*: testa a comunicação entre dois roteadores e verifica se os mesmos estão presentes.
- Descrição do Banco de Dados (DD ou DBD, *DataBase Description*): busca informações resumidas sobre os caminhos (*links*), geralmente usada na comunicação inicial, depois da troca de mensagem hello, para que os roteadores adquiram o conhecimento dos seus respectivos caminhos (*links*).
- Requisição do Estado do *Link* (LSR, *Link-State Request*): pede informações completas sobre o estado de um determinado caminho (*link*).
- Atualização do Estado do *Link* (LSU, *Link-State Update*): datagrama que contém informações detalhadas do estado de um determinado caminho. São enviadas em resposta a uma Requisição do Estado do *Link* (LSR).
- Confirmação do Estado do *Link* (LSAck, *Link-State Acknowledge*): confirma o recebimento de uma mensagem de Descrição do Banco de Dados (DBD) e de atualização do Estado do *Link* (LSU).

4.4.3 Protocolos BGP

É um protocolo de roteamento externo usado na internet, utilizado no processo de roteamento entre sistemas autônomos (grandes redes, redes de empresas gigantes, etc.), o BGP também é usado dentro do sistema autônomo, somente quando precisa trocar informações com outro roteador externo. As mensagens BGP são enviadas através do protocolo TCP (porta 179) e logo o destinatário confirma o recebimento dela, diferente do RIP e OSPF que usam datagrama IP, as mensagens BGP também usam autenticação, e suas mensagens basicamente dizem o caminho dos sistemas autônomos que os datagramas precisam percorrer, por isso, o BGP é classificado como protocolo de vetor de caminho. Se houver mais de um caminho para atingir outro sistema autônomo e nenhum atributo adicional tiver especificado o BGP escolherá o caminho mais curto.

Os sistemas autônomos são numerados e sua numeração é controlada pela IANA a mesma que distribui os endereços IP e que também repassa a tarefa para órgãos regionais, no Brasil eles são atribuídos pela LACNIC.

Tipos de Mensagem do BGP:

- Abertura: tem função de estabelecer uma relação de vizinhança e troca de parâmetros básicos.
- *Keepalive*: utilizada para manter a conexão e verificar se o roteador da outra ponta está funcionando, essas mensagens tem o padrão de serem enviadas a cada 60 segundos e se o roteador da outra ponta não responder em no máximo 180 segundos ele é considerado como fora de alcance.
- Atualização: tem a função de enviar informações de roteamento.
- Notificação: utilizada na ocorrência de um erro. Anula a relação de vizinhança entre roteadores.

5 *ROUTERBOARD MIKROTIK*

5.1 *MIKROTIK*

É uma empresa de desenvolvimento, instalação e venda de roteadores e *wireless*. Fundada em 1995, começou desenvolvendo roteadores e sistemas provedores de internet (ISP) *wireless* para conectividade com a Internet. Em 1997 criaram seu próprio sistema operacional para roteadores baseado no *Linux* o *RouterOS*, "sistema esse que provê grande controle, flexibilidade e estabilidade para todos os tipos de interfaces de dados e roteamento". [26] Em 2002, essa empresa criou a marca *Routerboard*, fazendo seu próprio *hardware* para roteamento e sistemas ISP (Provedor de Serviço de Internet).

A *MikroTik Routerboard* possui diversos equipamentos desde roteadores a antenas para *wireless*, alguns roteadores podem até possui *upgrade*, que poderia fazer uma mudanças de *hardware* e *software* para uma versão melhor ou mais recentes, todos os roteadores vem com o *RouterOS* instalado, sendo que nesse sistema existe também ferramentas para ajudar a configurar roteadores (*Winbox* e *Webfig*) e gerência de redes (*The Dude*). Afinal roteadores são configurados em *MS-DOS*, mais o *Routerboard MikroTik* possui uma interface gráfica sendo acessada tanto pelo *Winbox* quanto pelo *Webfig*.

5.2 *ROUTEROS*

É o Sistema Operacional desenvolvido pela empresa *MikroTik* para roteadores, pode ser instalado de duas formas: utilizando um CD *Iso bootável* (gravado como imagem) e também via rede com o utilitário *Netinstall*. Sendo que para acessá-lo, deve-se utilizar a ferramenta *Winbox* ou usando qualquer navegador de internet para acessar a ferramenta *Webfig*. Esse sistema suporta dois tipos de roteamento: dinâmico e estático. No estático as rotas são criadas pelo usuário através de inserção de rotas pré definidas em função da topologia da rede; Já no dinâmico as rotas são geradas automaticamente através de algum agregado de endereçamento

IP ou por protocolos de roteamento como, no caso do *MikroTik RouterOS* pode ser utilizados o RIPv1, RIPv2, OSPF versão 2 e o BGP versão 4. O uso deste tipo de roteamento permite implementar redundância e balanceamento de cargas de forma automática sendo a forma de se fazer uma rede semelhante às redes conhecidas como *Mesh* (Malha), porém de forma estática. Este sistema suporta o ECMP (*Equal Cost Multipath Routing*) que é um mecanismo que permite rotear pacotes através de vários caminhos (*links*) e permite balanceamento de carga.

Esse sistema pode desempenhar as seguintes funções:

- Roteador Dedicado;
- *Bridge* (ponte);
- *Firewall* (segurança de rede);
- Controlador de Bandas e QoS;
- APs (*Access Point*) *Wireless* modo 802.11 e proprietário;
- Concentrador PPPoE (*Point-to-Point Protocol over Ethernet*), PPtP (*Point-to-Point tunneling Protocol*), IPSeC, L2TP (*Layer 2 Tunneling Protocol*), etc;
- Roteador de Borda;
- Servidor *Dial-in* e *Dial-out*;
- *Hotspot* e gerenciador de usuários;
- *WEB Proxy* (Servidor *WEB*);
- Recursos de *Bonding*, VRRP (*Virtual Router Redundancy Protocol*), dentre muitas outras, etc.

5.2.1 *Winbox*

Ferramenta para poder configurar todos os roteadores da *MikroTik*. Abaixo na figura 19, segue a interface para entrar na janela de configuração desse programa.

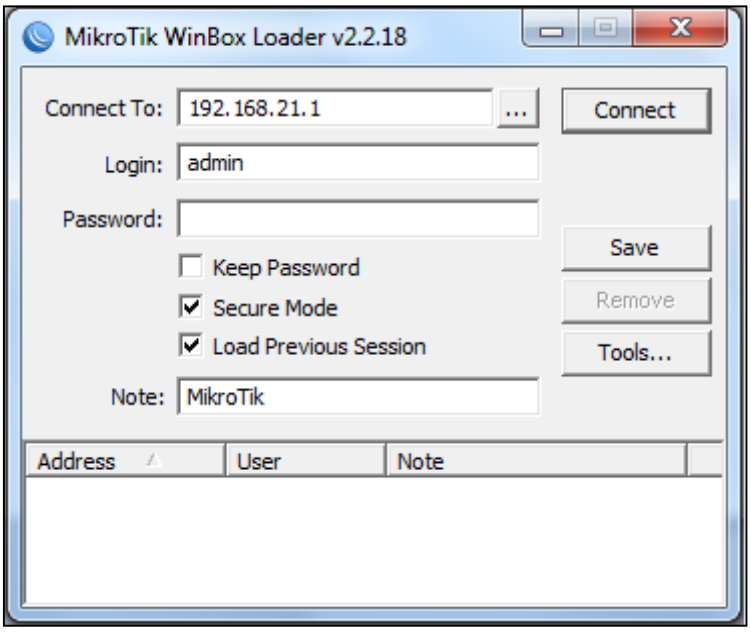

Figura 19 - Interface para o acesso ao Winbox

Dessa forma, de acordo com a figura 19, as funções dos botões são:

- Botão para descobrir o IP do equipamento (roteador) conectado.

  

- Botão para conectar o *winbox* ao roteador da *MikroTlk*.

  

Assim utilizando o botão 

clica-se no endereço que vai aparecer, sendo este do roteador que está conectado e depois clica em 

para entrar na interface do *winbox* (o computador utilizado para acessar este programa deve estar na mesma rede do roteador que está conectado). Com isso aparecerá à figura 20 a seguir.

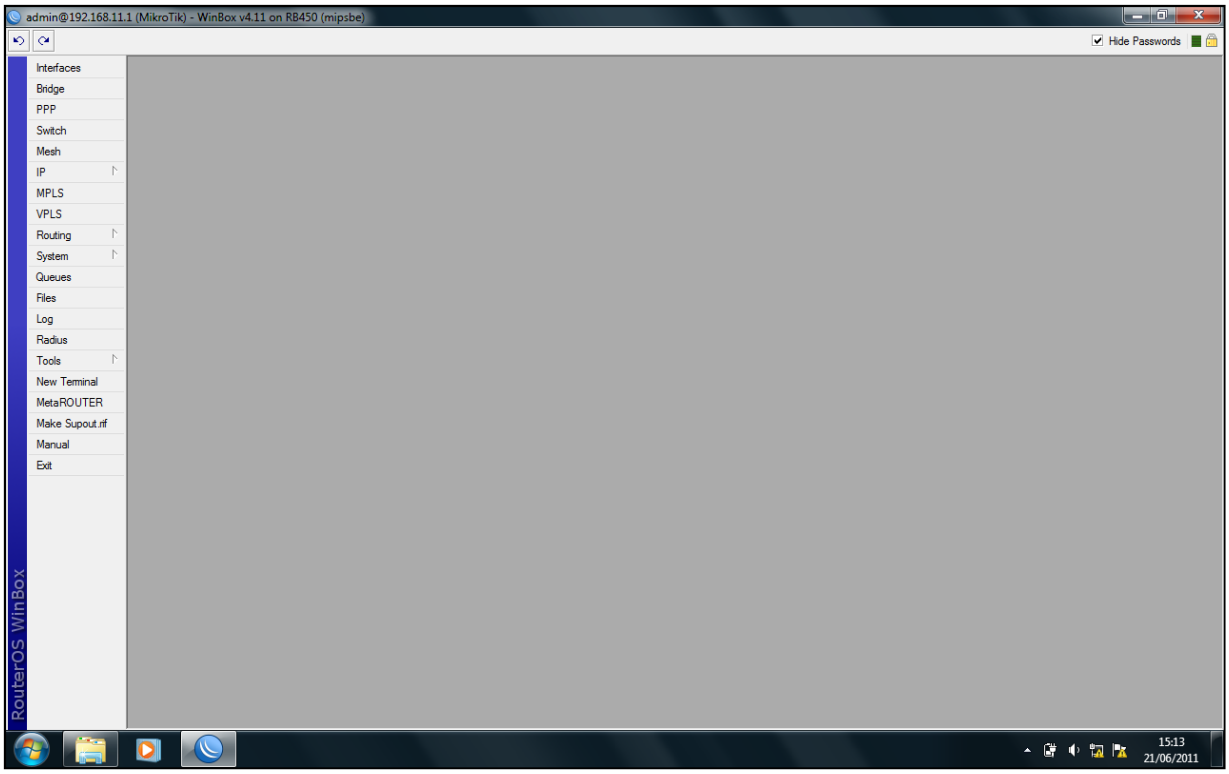

Figura 20 - Interface do Winbox

Depois que aberta à janela do *winbox*, configura-se o roteador conectado utilizando as opções que aparecem na barra de menus à esquerda da tela.

Assim para se configurar cada roteador, tem-se esta barra com várias sub-barras com muitas outras opções. Sendo que cada opção desta possui funções diferentes, mas para nossas experiências serão utilizadas as opções “IP” (*Address* e *Routes*) e “Routing” (RIP) para as devidas configurações.

5.2.1.1 IP

Logo ao abrir o *Winbox* aparece do lado esquerdo uma barra de menus com vários itens, aparecendo à opção IP com muitos subitens.

Dentre estes subitens tem a opção *Address* (endereço) aonde se configura endereços das portas do roteador que se está usando, criando-se novos endereços ou alterando os já criados clicando no ícone “+” abrindo outra janela chamada *New Address* (novo endereço).

Tem-se também a opção *Routes* para se configurar rotas, e visualizando as rotas

que aparecem automáticas quando criados os endereços das portas do *Routerboard MikroTik*, podendo-se alterar as rotas que foram criadas manualmente.

5.2.1.2 *Routing*

Essa opção esta na barra de menus da interface do *winbox*, utilizada para a configuração de rotas dinâmica definindo-se o protocolo que será utilizado. Afinal quando se clica nessa opção aparece a sub-barra de menus com os protocolos que podem ser utilizados como o RIP, BGP, OSPF e outros.

5.2.2 *Webfig*

É uma ferramenta de configuração do *RouterOS*, acessada diretamente do roteador e não precisando de *software* adicional e sim de um navegador de internet; como o *Webfig* é independente da plataforma, pode ser usado até por dispositivos móveis para fazer as configurações do roteador; ele foi projetado para ser uma alternativa do *Winbox*, tendo um *layout* bastante parecido, e também há suporte ao IPv6. Para abrir sua interface tem-se que executar qualquer navegador de internet, digitando o endereço IP do roteador que está conectado, no campo de endereços do navegador, abrindo sua janela principal.

5.3 *ROUTERBOARD*

É a marca de equipamentos que foi desenvolvida pela empresa *MikroTik* para roteamento e sistemas ISP (Provedores de internet).
Os roteadores dessa marca possuem cinco portas, configuradas para serem usadas como LAN (*Local Area Network*) ou WAN (*Wide Area Network*).

Figura 21 - *Routerboard MikroTik*
FONTE: [27]

5.4 DESCRIÇÃO DA CONFIGURAÇÃO DO *ROUTERBOARD MIKROTIK*

Para começar a descrição desta configuração tem-se que mostrar alguns botões que serão necessários durante esse processo:

- Botão para adicionar novos parâmetros.

- Botão para remover parâmetros existentes.

- Botão para ativar novos parâmetros.

- Botão para desativar parâmetros existentes sem removê-los.

5.4.1 Configuração de portas e roteamento estático

Assim começando a configuração desse dispositivo, tem-se:

1) Primeiro deve-se clicar: no “Iniciar” – “Painel de Controle” – “Rede e Internet” – “Central de Rede e Compartilhamento”;

2) Continuando clica-se em “Conexão Local” – “Propriedades” – “Protocolo TCP/IP Versão 4 (TCP/IPv4)” aparecerá a janela com o “Obter um endereço IP automaticamente” selecionado, dessa forma seleciona-se o “Usar o seguinte endereço IP:”, observando este passo 2 nas figuras 22, 23, 24 e 25:

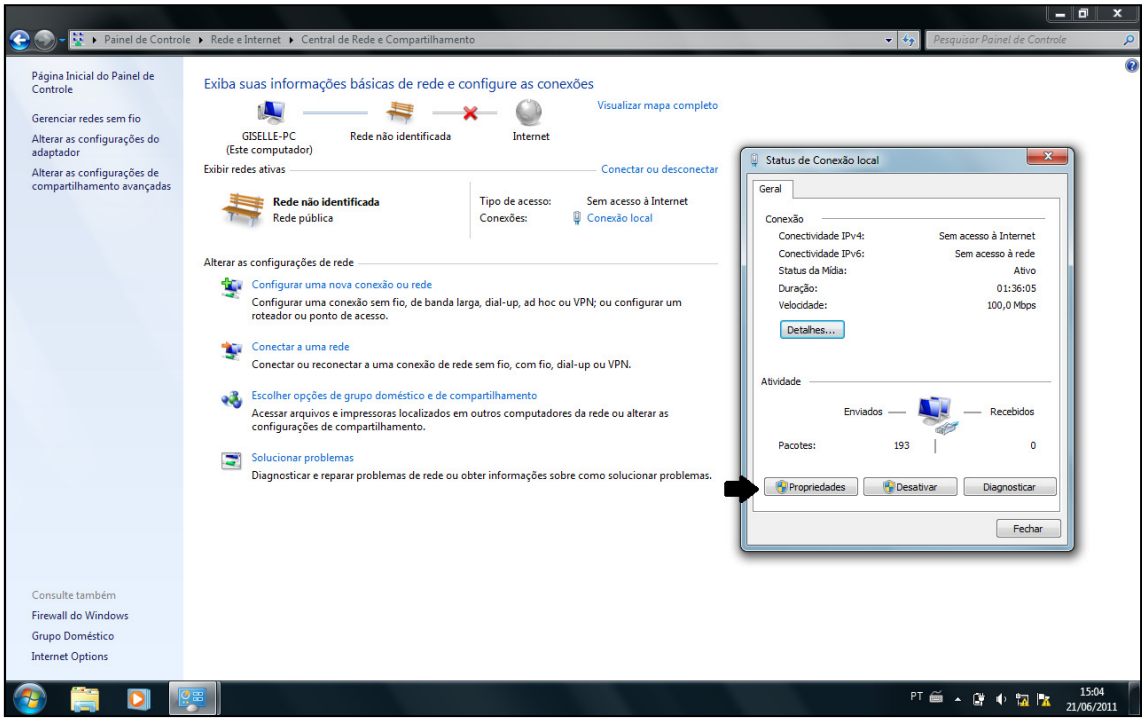

Figura 22 - Configurando IP da máquina utilizando a opção propriedades

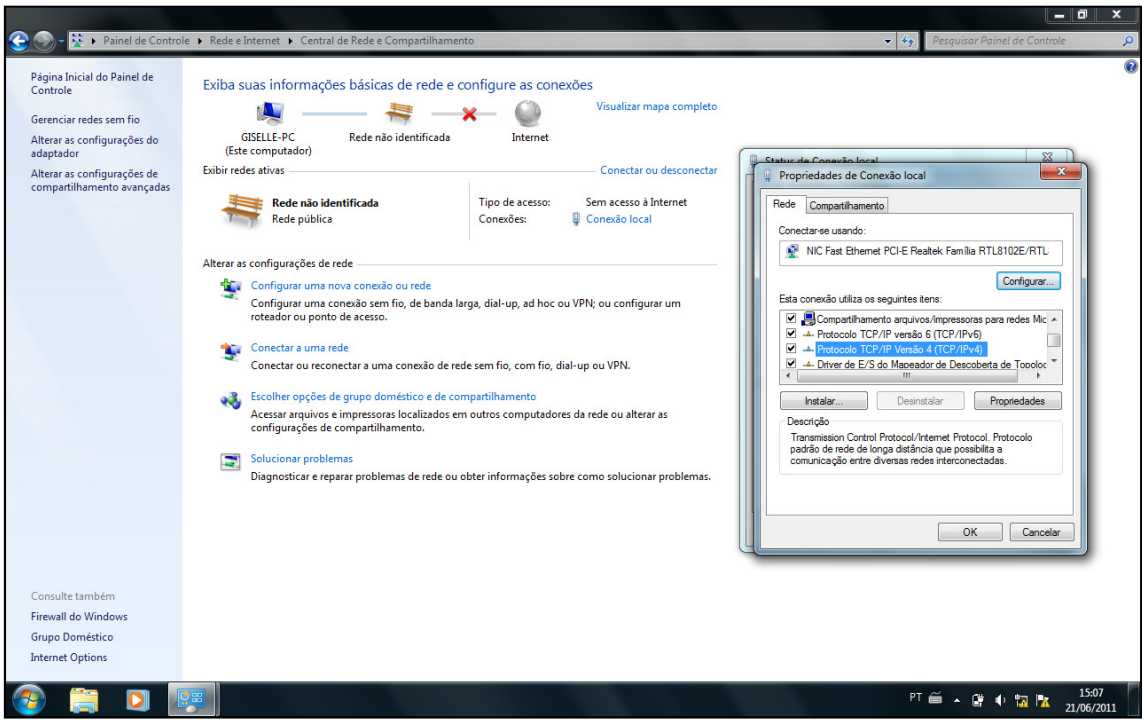

Figura 23 - Configurando IP da máquina utilizando propriedades da conexão local

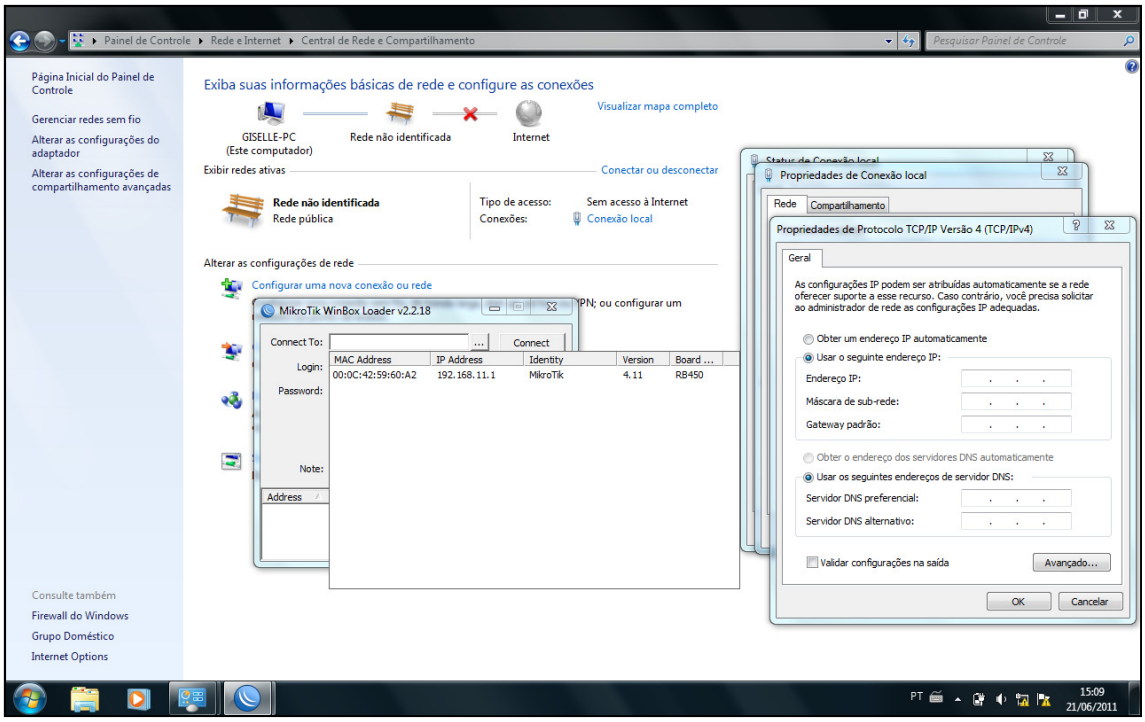

Figura 24 - Configurando IP da máquina utilizando propriedades do TCP/IP versão 4

Utilizando a figura 24 acima e analisando o endereço mostrado na janela do *winbox*, preenchem-se os seguintes campos:

- Endereço IP: 192.168.11.2 (endereço do computador utilizado);
- Máscara de sub-rede: que ao clicar aparece automaticamente, mas senão aparecer, digita-se o número 255.255.255.0; e,
- *Gateway*: 192.168.11.1.

Obs.: Endereços esses que serão utilizados no estudo de caso, simulação 1.

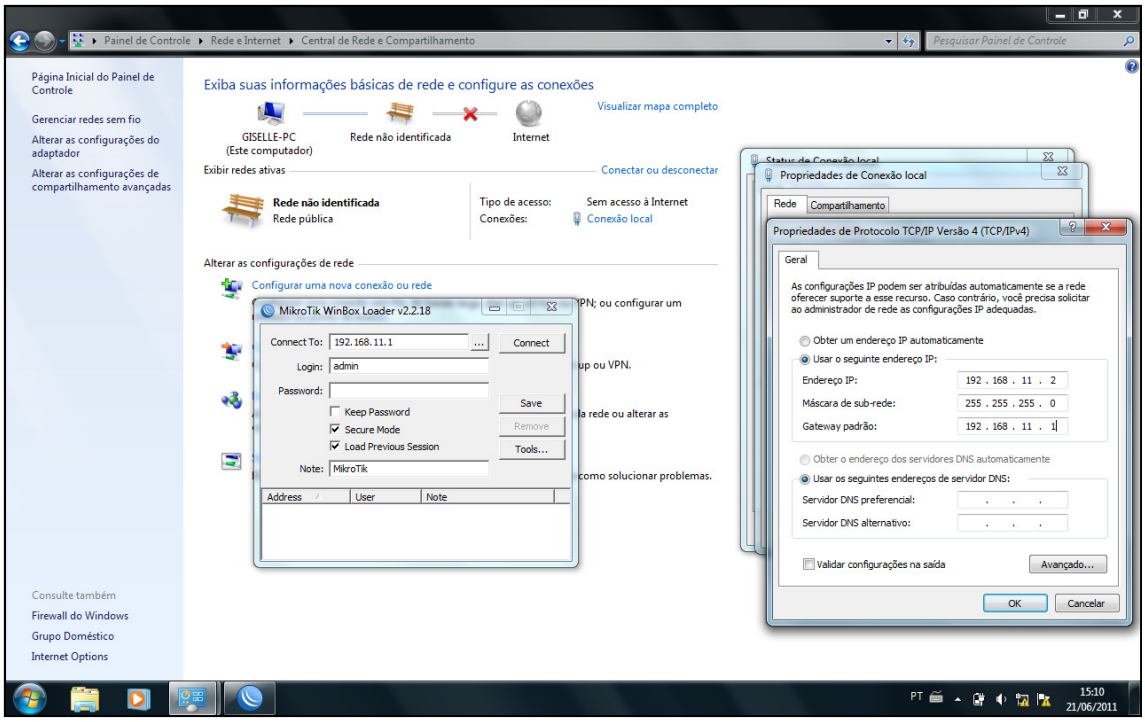

Figura 25 - Inserindo o endereço IP da máquina, máscara de rede, endereço IP do Gateway

3) Seguindo o passo 2, clica-se em “OK” na primeira e segunda janela e depois em “Fechar”, com isso execute o programa *winbox*, depois clicando no botão “...” e seleciona-se o endereço que irá aparecer, em seguida clica-se no botão “Connect”, como demonstrado na figura 25 acima, e assim abre-se a *interface* do *winbox*;

4) Para iniciar a configuração das portas do roteador, clica-se no IP da barra de menus na *interface* desse programa; abrindo uma sub-barra de menus têm-se as opções *Address* e *Routes*; utilizando-se a primeira opção *Address* pode-se configurar o endereço de todas as portas e a segunda opção *Routes* configura-se as rotas para fazer a comunicação entre a porta de um roteador com a porta de outro roteador. Dessa forma, após clicar na opção *Address* abre-se a janela *Address List* clicando no botão “+” para adicionar um novo endereço IP em uma porta, com isso abrirá uma nova janela “New Address”; analisando assim essas opções na figura 26.

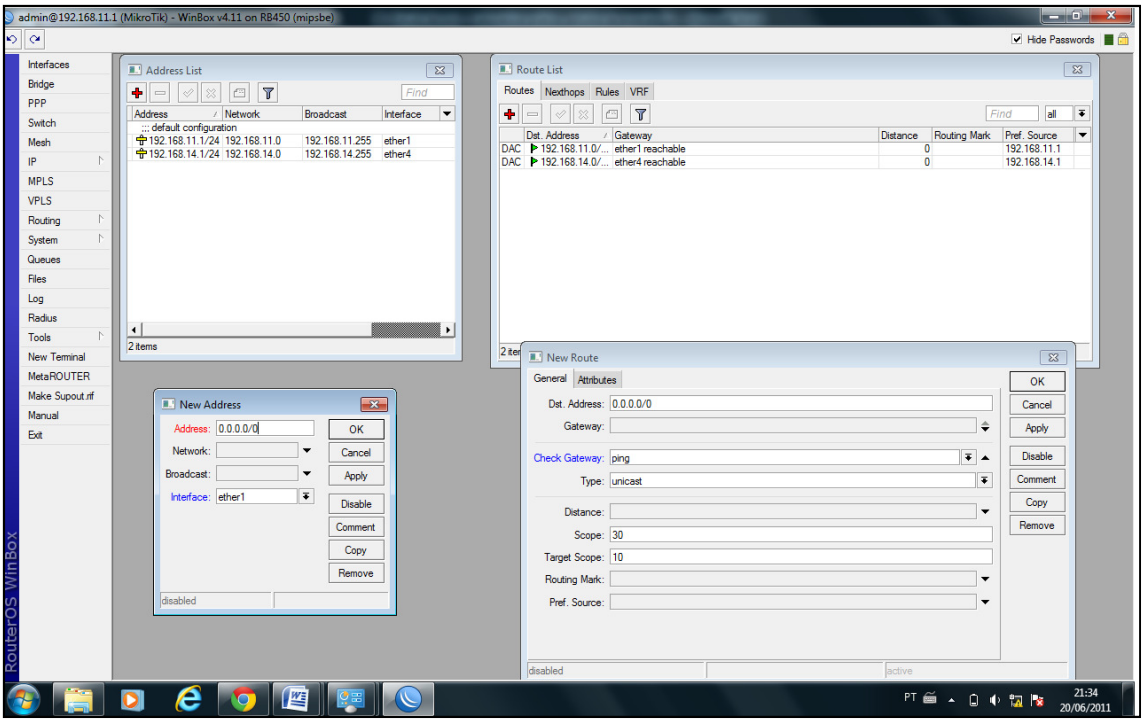

Figura 26 - Janelas de configurações de Address (endereço) e Routes (rotas)

Tendo que preencher os campos: *Address* (endereço da porta do roteador), *Network* (endereço da rede), *Broadcast* (último endereço da rede) e a *Interface* (clicando-se no botão ao lado seleciona-se a porta "*ether*1").

5) De acordo com a figura 26, configura-se também a opção "Routes", que ao ser clicado abre-se a janela "Route List" onde ao clicar no botão "+" adiciona-se uma nova rota; sendo que quando se cria um endereço automaticamente aparece uma rota padrão na "Route List" referente ao endereço criado, e depois se configura as rotas entre os roteadores. Com isso clicando no botão "+" preenchendo-se os seguintes endereços: *Dst. Address* (endereço da rede de destino), *Gateway* (endereço IP da porta do outro roteador, no caso o roteador 2) e a *Distance* (a quantidade de hops que se irá passar), pois digita-se 1 para passar por um hop (roteador), 2 para passar por dois hops e assim sucessivamente.

5.4.2 Configuração de roteamento dinâmico com RIP

Para este tipo de configuração devem-se ter as portas já configuradas, pois o começo da configuração na parte de endereços é igual ao item 5.4.1, no caso, repetindo os passos 1, 2, 3 e parte do passo 4, afinal as rotas não são configuradas. Com isso seguimos os passos a seguir:

1) Depois de utilizar os passos acima para se configurar os endereços das portas, utiliza-se a opção “Routing” da barra de menus na *interface* do *winbox* para se configurar o RIP, dessa forma clica-se na opção “RIP” da sub-barra de menus para este protocolo criar as rotas dinâmicas. Com isso, abre-se a janela “New RIP Interface” para selecionar as portas que serão utilizadas, clicando-se no botão do campo “Interface” para selecioná-las, de acordo com a figura 27;

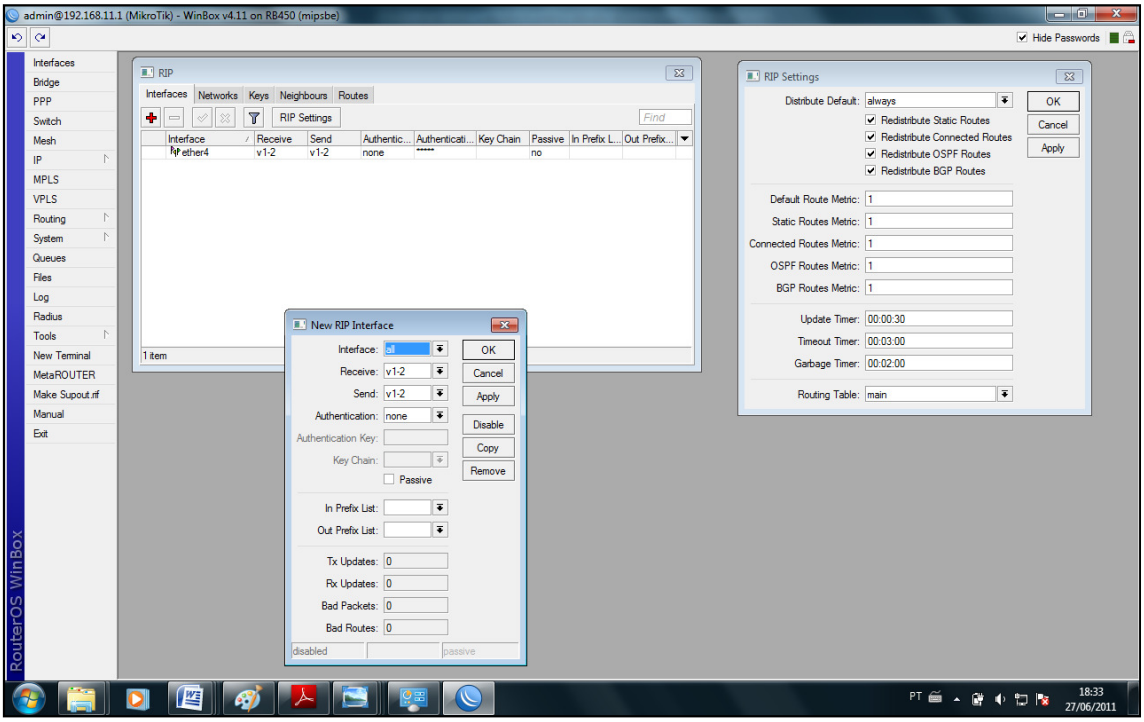

Figura 27 - Janelas de configuração do RIP adicionando interface

2) Continuando na aba “Interface” tem-se o botão “RIP Settings”, configurando-se os seguintes campos: “Distribute Default” escolhendo a opção “always” e selecionando as opções “Resdistribute Static Routes” e “Resdistribute

Connected Routes” e depois se clica em “OK”, como se mostra na figura 28;

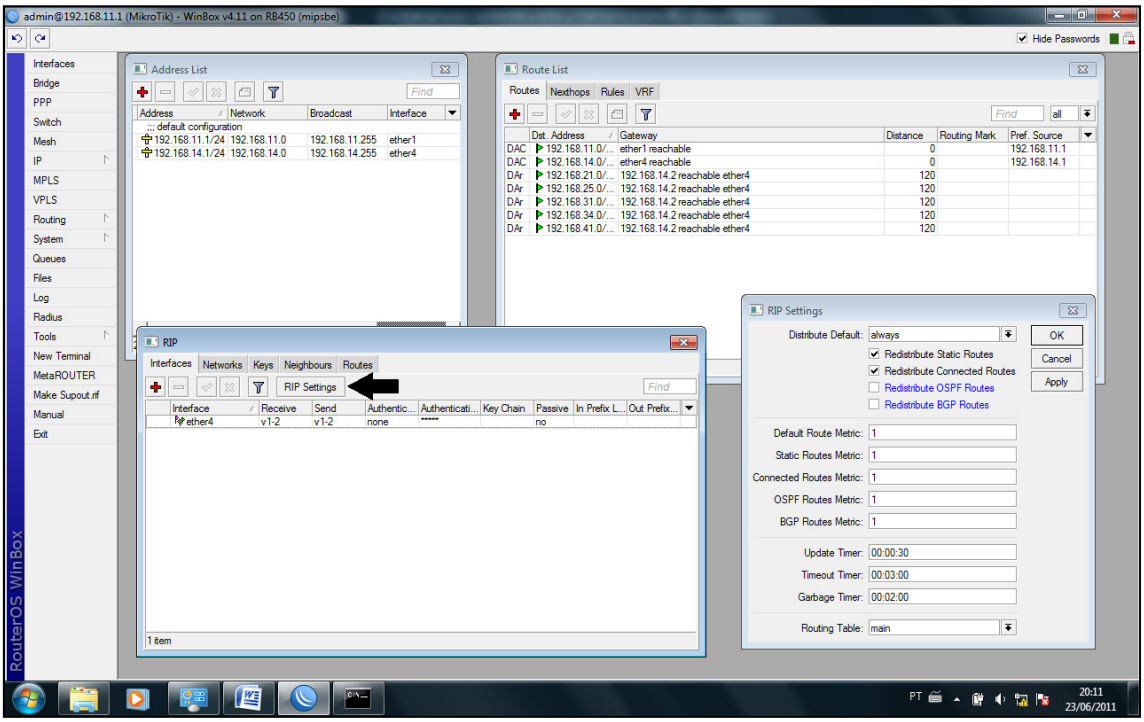

Figura 28 - Janela para configuração do “RIP Settings”

3) Assim o último parâmetro a ser configurado é o endereço IP do roteador vizinho, para isso clica-se na aba “Neighbours” e depois no botão “+” abrindo-se a janela “New RIP Neighbours”, clicando-se em “OK” para adicionar um novo vizinho. Onde um roteador pode ter mais de um vizinho, dessa forma tendo que inserir todos os vizinhos existentes. Sendo mostrado esse procedimento na figura 29 abaixo;

4) Agora nota-se que as rotas criadas pelo RIP aparecem de duas formas:
   - Na aba “Routes” da janela RIP da opção “Routing” da barra de menus; e
   - Na aba “Routes” da janela *Route List* na sub-barra de menus “Routes” encontrado na opção “IP” da barra de menus.

   Observando-se assim na figura 30 abaixo os dois lugares que são mostradas as rotas criadas.

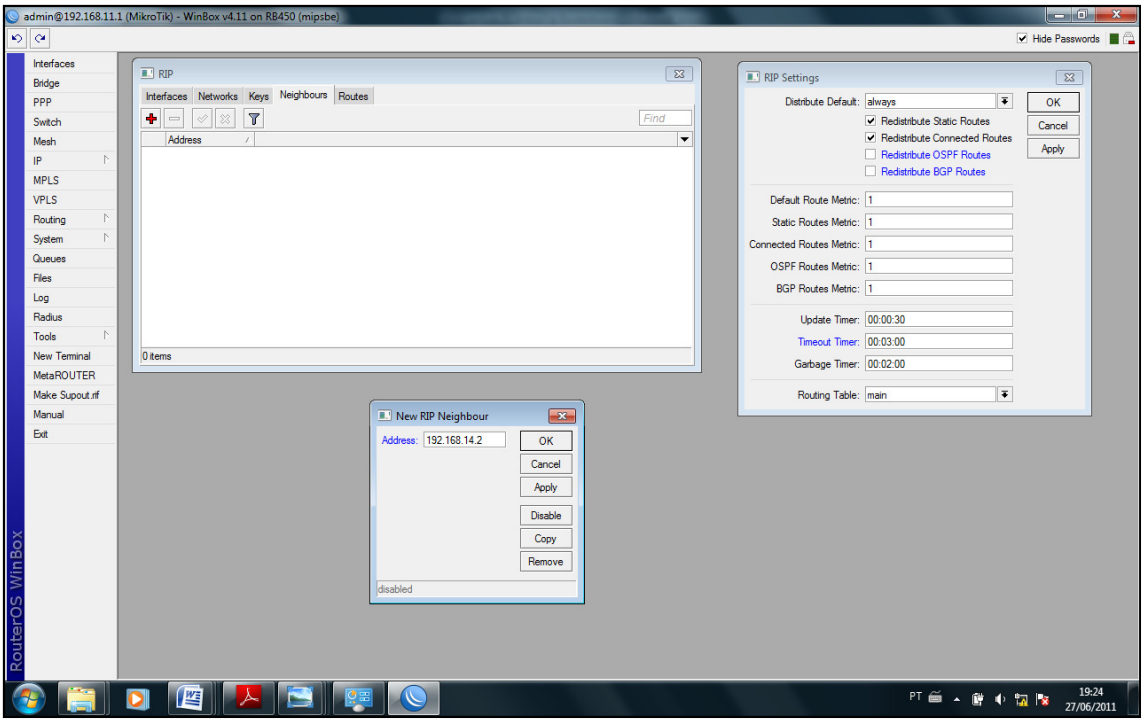

Figura 29 - Janelas de configuração do RIP adicionando vizinhos (*Neighbours*)

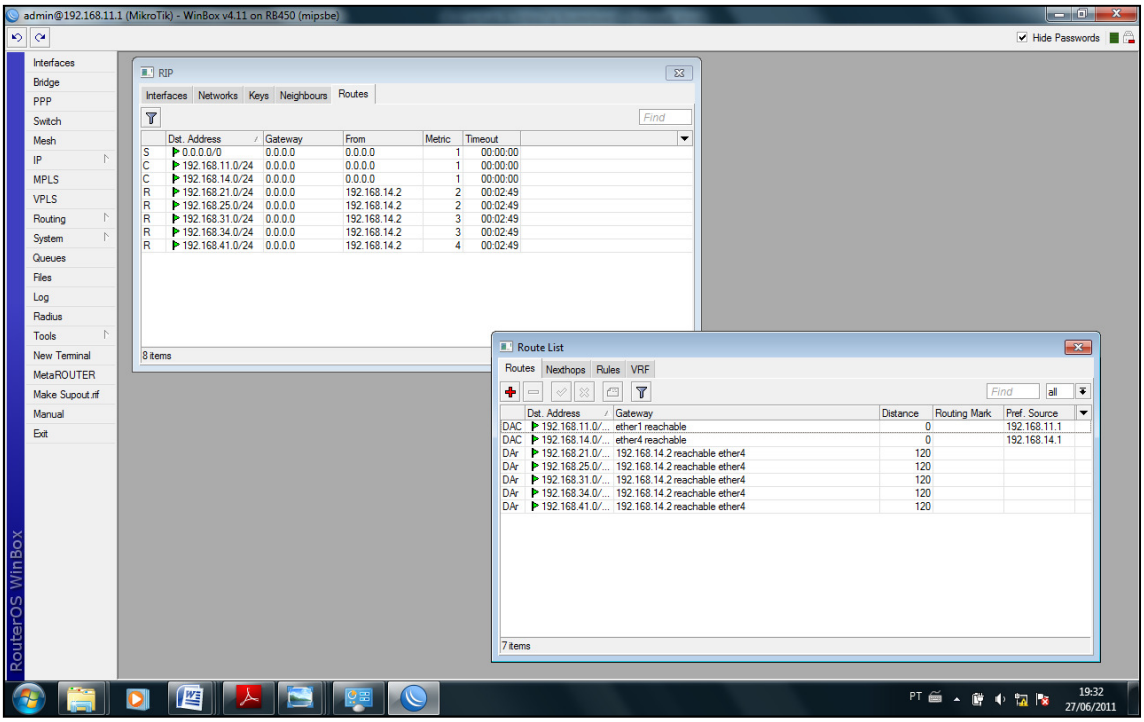

Figura 30 - Rotas criadas pelo RIP

6 ESTUDO DE CASO: LABORATÓRIO PRÁTICO, ESTUDO DE EXPERIÊNCIAS

Foram estudadas as topologias de rede descritas anteriormente nesse trabalho usando o roteador *MikroTik Routerboard*, que possui cinco portas *Ethernet* (Eth1, Eth2, Eth3, Eth4, Eth5) pode-se configurar cada porta e também acessar o roteador por qualquer uma das portas, todas as redes destas portas comunicam-se entre si, isso quer dizer que, se na porta Eth1 houver uma rede e na Eth2 outra, estas portas automaticamente estarão ligadas, então qualquer rede estabelecida nas portas se comunicarão, porém ao conectar um outro roteador, este precisa estar na mesma rede (sendo que a parte de rede do endereço IP tem que ser a mesma) para que os roteadores possam se comunicar, a rota para esse novo roteador pode ser estabelecida criando a tabela manualmente ou utilizando um protocolo de roteamento dinâmico como RIP.

Dessa forma, serão realizadas as simulações a seguir, que em todas as experiências começará a montagem da rede de acordo com a topologia utilizada, onde primeiro os roteadores serão conectados entre si com cabos UTP CAT5e, depois utilizando mais um cabo UTP, será conectado o *Notebook* (*Laptop)* em cada roteador separadamente para configurá-los, colocando o cabo preferencialmente na porta Eth1 de cada roteador, mas qualquer uma das cinco portas serve para tais ajustes de configuração, tendo nesta a possibilidade de definir o endereço IP.

Assim, no final de cada experiência será testado o funcionamento da rede, para mostrar a comunicação entre os roteadores, o *Notebook* (*Laptop*) e o Computador (PC, Personal Computer), e também como será configurado cada parâmetro necessário dos roteadores, utilizando o programa *winbox* da empresa *MikroTik*.

6.1 EXPERIÊNCIAS COM TOPOLOGIA LINEAR

Simulação 1:

Experiência 1 com Roteamento Estático:

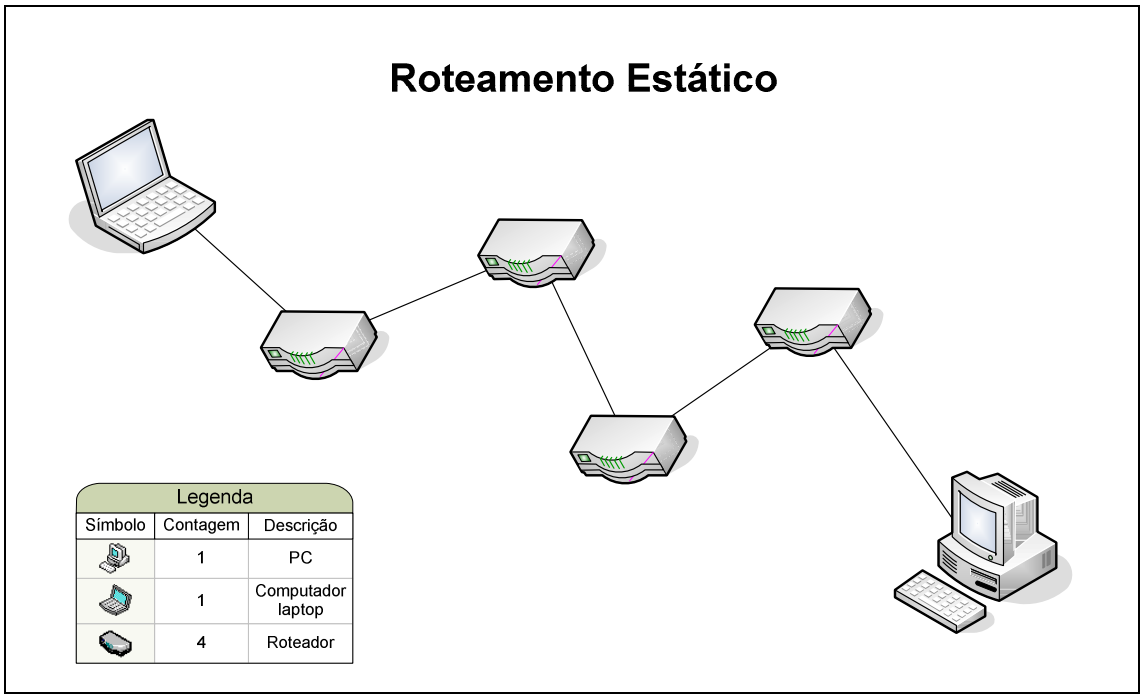

Figura 31 - Experiência 1 realizada em laboratório

De acordo com a figura 31, foi realizada essa experiência em laboratório para a configuração do *Routerboard MikroTik*. Assim descreve-se a seguir esta configuração:

1) Antes de começar a configuração foram utilizados os equipamentos:
   - 1 *Notebook* (*Laptop*);
   - 1 Computador (PC);
   - 4 Roteadores da marca *Routerboard MikroTik*;
   - 5 Cabos UTP CAT5e (cabos de rede);

2) Em seguida foi considerado o seguinte endereço de porta do *Notebook* (*Laptop*): 192.168.11.2 e o endereço do Computador (PC): 192.168.41.2;

3) Primeiro deve-se clicar: no “Iniciar” em seguida no “Painel de Controle” e em “Rede e Internet” depois na “Central de Rede e Compartilhamento” e após isso seguir o passo 4;

4) Clica-se em “Conexão Local”, seguido de “Propriedades”, clicando em “Protocolo TCP/IP Versão 4 (TCP/IPv4)” aparecerá a janela com o “Obter um endereço IP automaticamente” selecionado, dessa forma seleciona-se o “Usar o seguinte endereço IP:” e em seguida configura-se:
    - Endereço IP: 192.168.11.2 (endereço do computador utilizado);
    - Máscara de sub-rede: que ao clicar aparece automaticamente, mas senão aparecer, digita-se o número 255.255.255.0; e,
    - *Gateway*: 192.168.11.1;

5) Seguindo o passo 2, clica-se em “OK” na primeira e segunda janela e depois em “Fechar”, com isso execute o programa *winbox*, depois clicando no botão “...” e seleciona-se o endereço que irá aparecer, em seguida clica-se no botão “Connect”, abrindo assim a interface do *winbox*;

6) Para iniciar a configuração das portas do roteador, clica-se no IP da barra de menus na interface desse programa; abrindo a opção IP têm-se várias opções dentre elas, *Address* e *Routes*; utilizando-se a primeira opção *Address* pode-se configurar o endereço de todas as portas e a segunda opção *Routes* configura-se as rotas para fazer a comunicação entre a porta de um roteador com a porta de outro roteador. Dessa forma ao abrir a janela *Address List* clica-se no botão “+” para adicionar um novo endereço IP em uma porta, com isso abrirá uma nova janela “New Address” onde se deve inserir:
    - *Address*: 192.168.11.1/24 (endereço da porta do roteador);
    - *Network*: 192.168.11.0 (endereço da rede);
    - *Broadcast*: 192.168.11.255 (último endereço da rede);
    - *Interface*: clicando-se no botão ao lado seleciona-se a porta “ether1”, dessa forma seguindo os mesmos passos para as demais portas tem-se o quadro 9;

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.168.11.1	IP 192.168.21.1	IP 192.168.31.1	IP 192.168.41.1
Eth 2				
Eth 3		IP 192.168.14.2	IP 192.168.25.2	IP 192.168.34.2
Eth 4	IP 192.168.14.1		IP 192.168.34.1	
Eth 5		IP 192.168.25.1		

Quadro 9 - Endereços IPs configurados para a experiência 1

7) Continuando a parte de configuração tem-se a opção “Routes”, que ao ser clicado abre-se a janela “Route List” onde ao clicar no botão “+” adiciona-se uma nova rota; sendo que quando se cria um endereço automaticamente aparece uma rota padrão na “Route List” referente ao endereço criado, e depois se configura as rotas entre os roteadores. Com isso clicando no botão “+” inserem-se os seguintes endereços:
   - *Dst. Address*: 192.168.41.0/24 (endereço da rede de destino);
   - *Gateway*: 192.168.14.2 (endereço IP da porta do outro roteador, no caso o roteador 2)
   - *Distance*: 4 (a quantidade de hops que se irá passar), pois digita-se 1 para passar por um hop (roteador), 2 para passar por dois hops e assim sucessivamente.

   Depois de configurar todas as rotas, obtém a tabela 1 com as rotas criadas;

Tabela 1 - Rotas criadas inseridas em cada roteador, experiência 1

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.41.0/24	192.168.14.2	3
	192.168.34.0/24	192.168.14.2	2
	192.168.25.0/24	192.168.14.2	1
Roteador 2	192.168.41.0/24	192.168.25.2	2
	192.168.34.0/24	192.168.25.2	1
	192.168.11.0/24	192.168.14.1	1
Roteador 3	192.168.41.0/24	192.168.34.2	1
	192.168.14.0/24	192.168.25.1	1
	192.168.11.0/24	192.168.25.1	2
Roteador 4	192.168.25.0/24	192.168.34.1	1
	192.168.14.0/24	192.168.34.1	2
	192.168.11.0/24	192.168.34.1	3

Obs.: porta de saída (G*ateway*) é a porta que está conectada o cabo de rede do próximo roteador, um roteador pode ter mais de um *Gateway*.

8) Depois de configurar todos os endereços e todas as rotas tem-se uma rede com roteamento estático, abaixo se mostram como foram testadas as rotas “pingando” cada porta do *host* (Computador) ao ultimo roteador. Analisando as figuras 32, 33 e 34 em seqüência, tiradas do *Prompt* de Comando; observa-se a rede do *Notebook* (*Laptop*) se comunicando até a rede do Computador (PC);

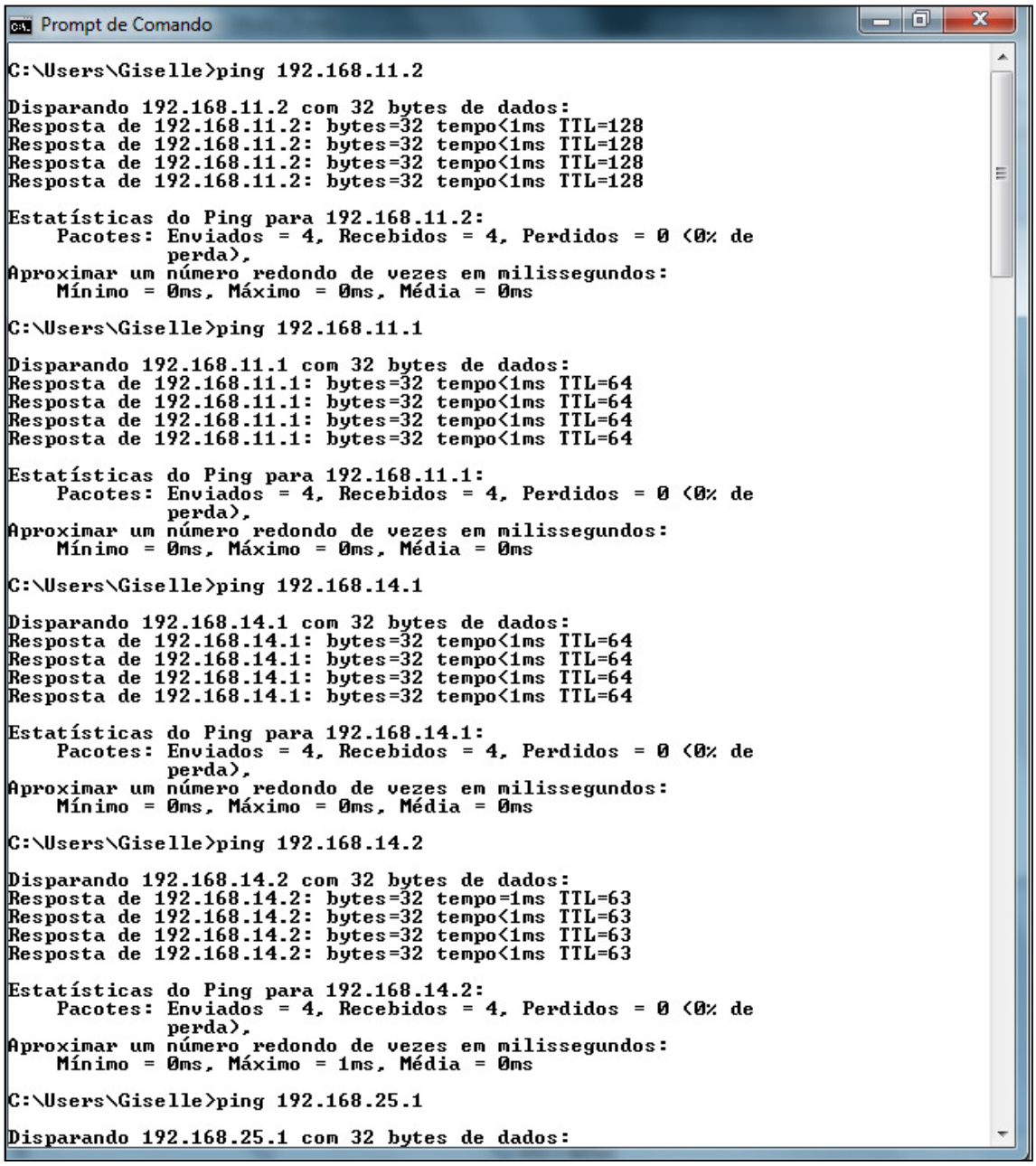

Figura 32 - Teste de conexão do *Notebook* (*Laptop*) até o endereço 192.168.14.2

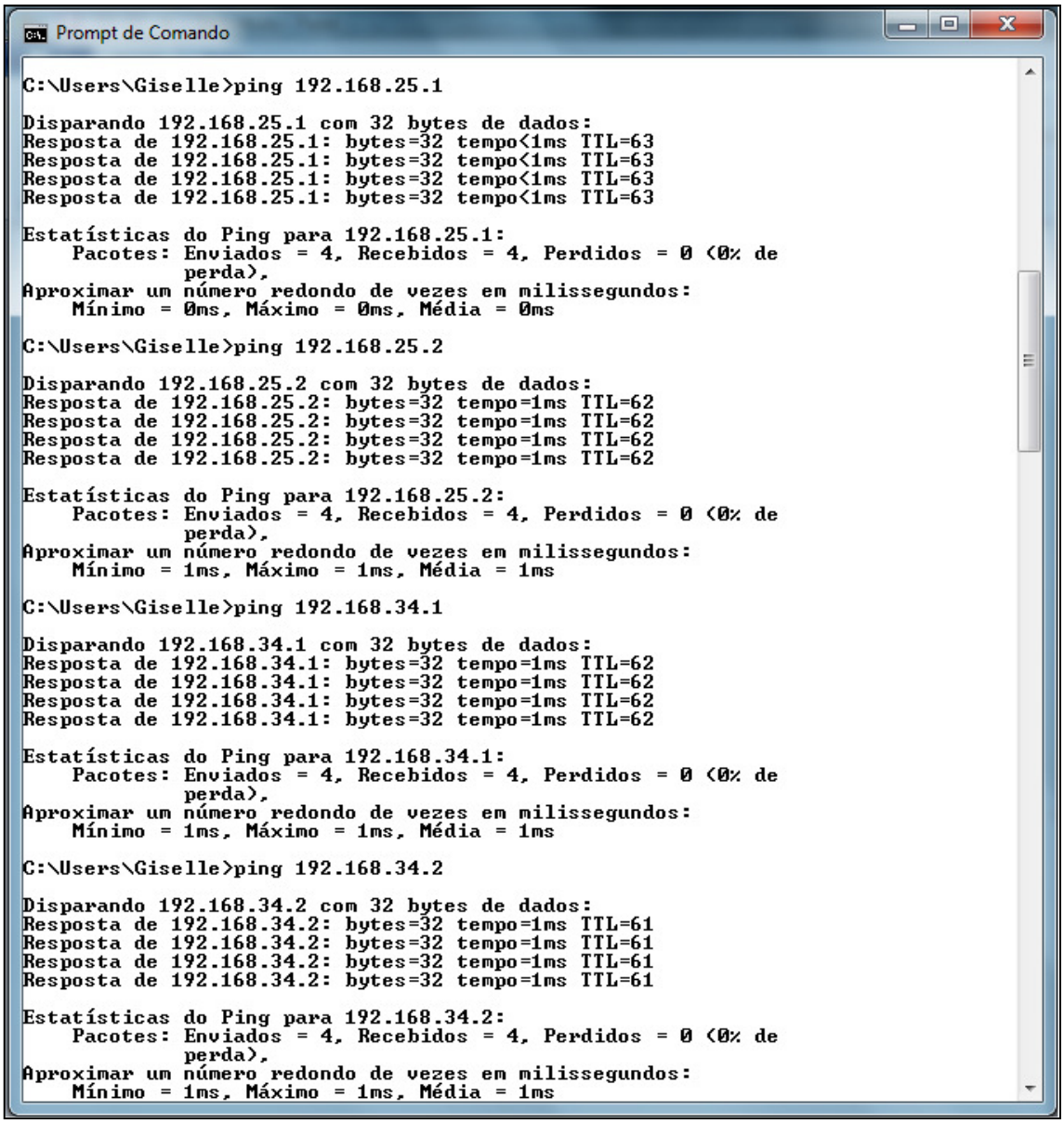

Figura 33 - Teste de conexão do endereço 192.168.25.1 até o endereço 192.169.34.2

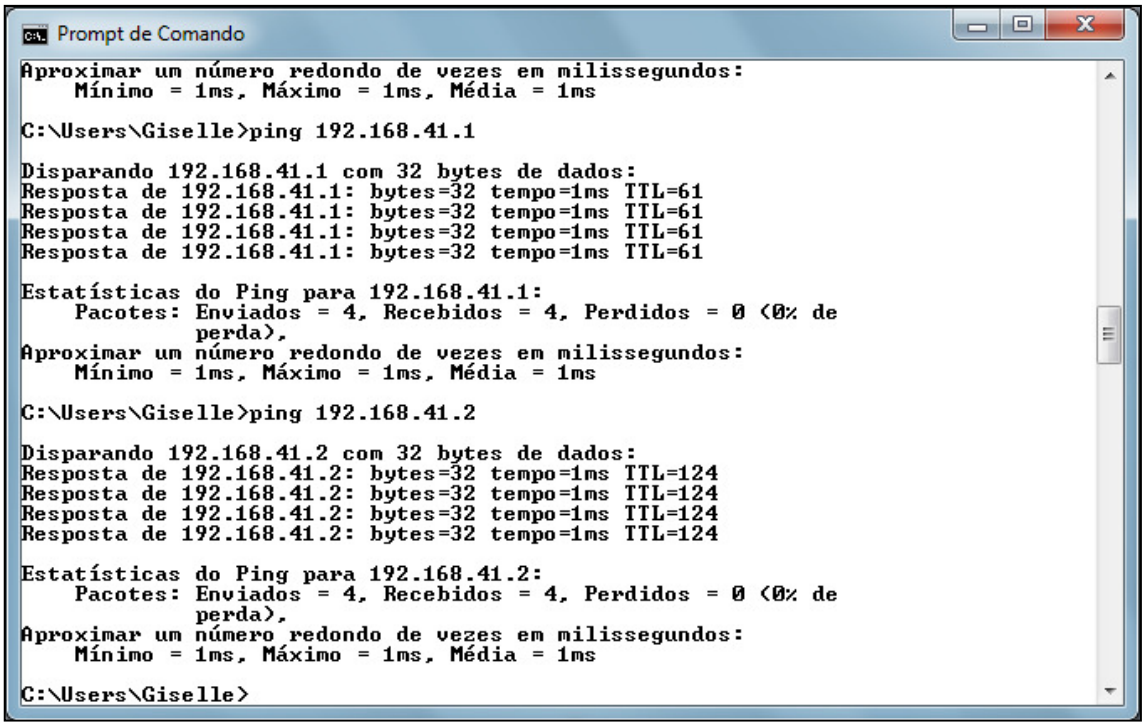

Figura 34 - Teste de conexão do endereço 192.168.41.1 até o Computador (PC)

9) E analisando também as figuras 35, 36 e 37 em seqüência, tiradas do *Prompt* de Comando; observa-se a rede do Computador (PC) se comunicando até a rede do *Notebook* (*Laptop*), assim tem-se a volta da rede do passo 8;

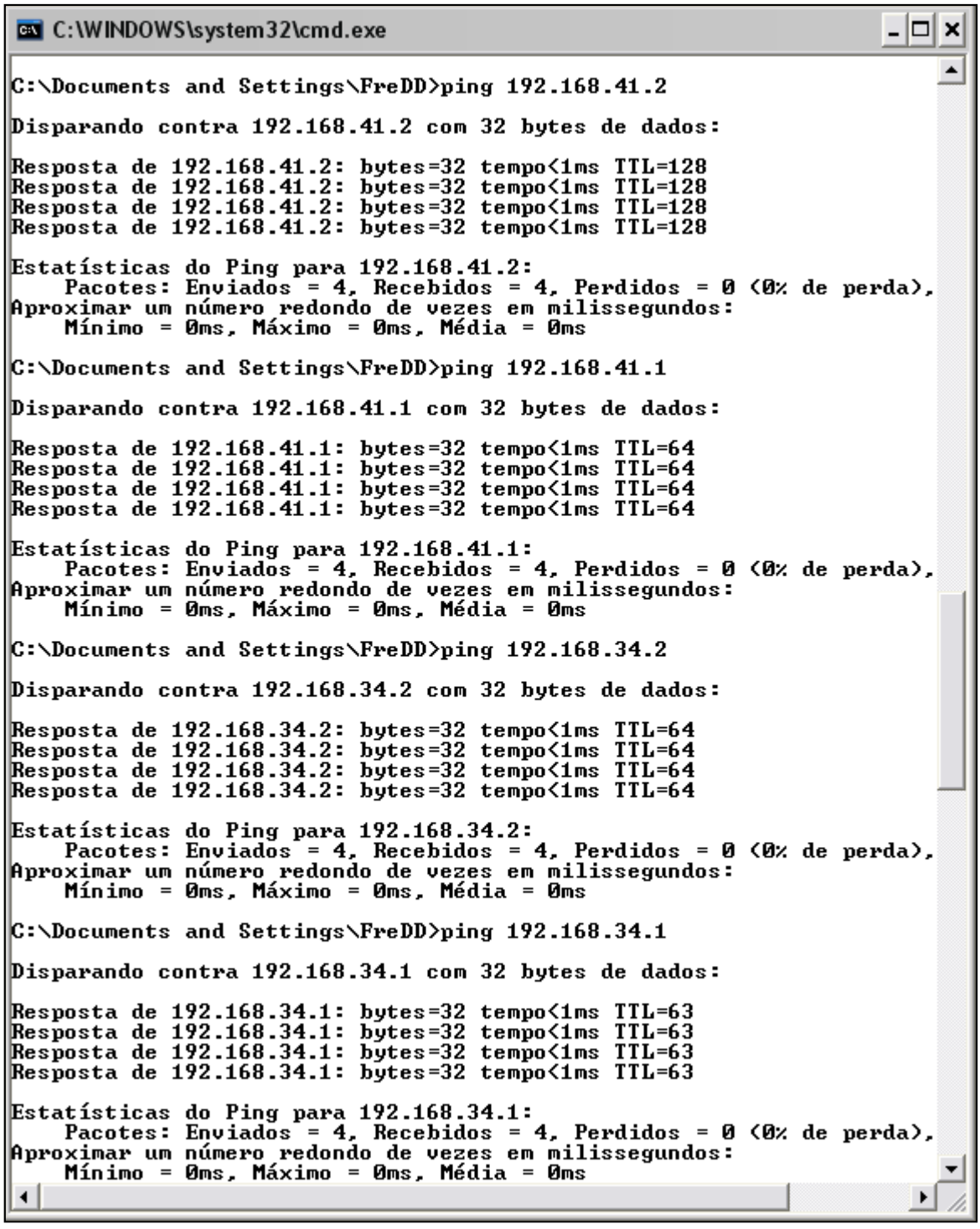

Figura 35 - Teste de conexão do Computador (PC) até o endereço 192.168.34.1

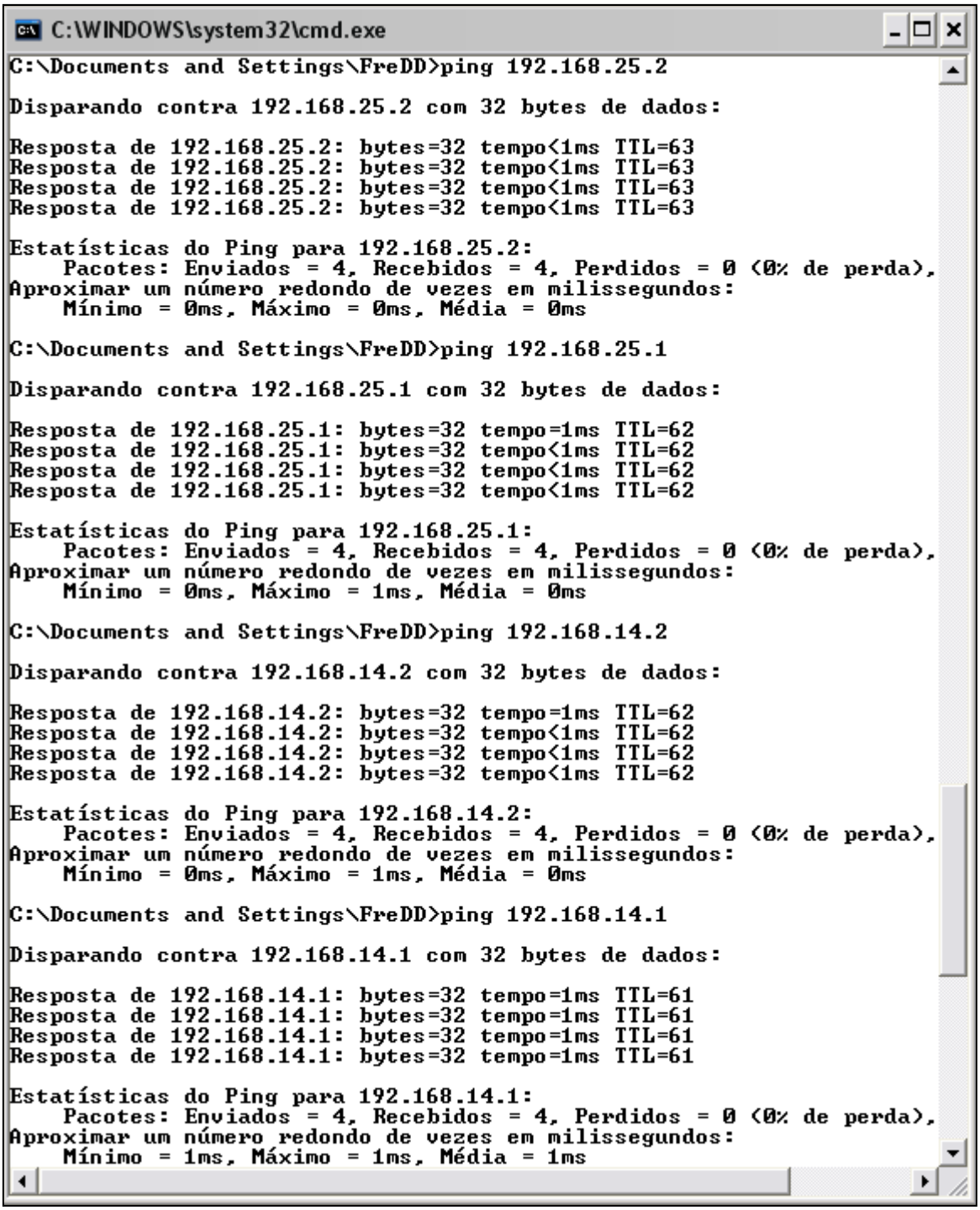

Figura 36 - Teste de conexão do endereço 192.168.25.2 até o endereço 192.168.14.1

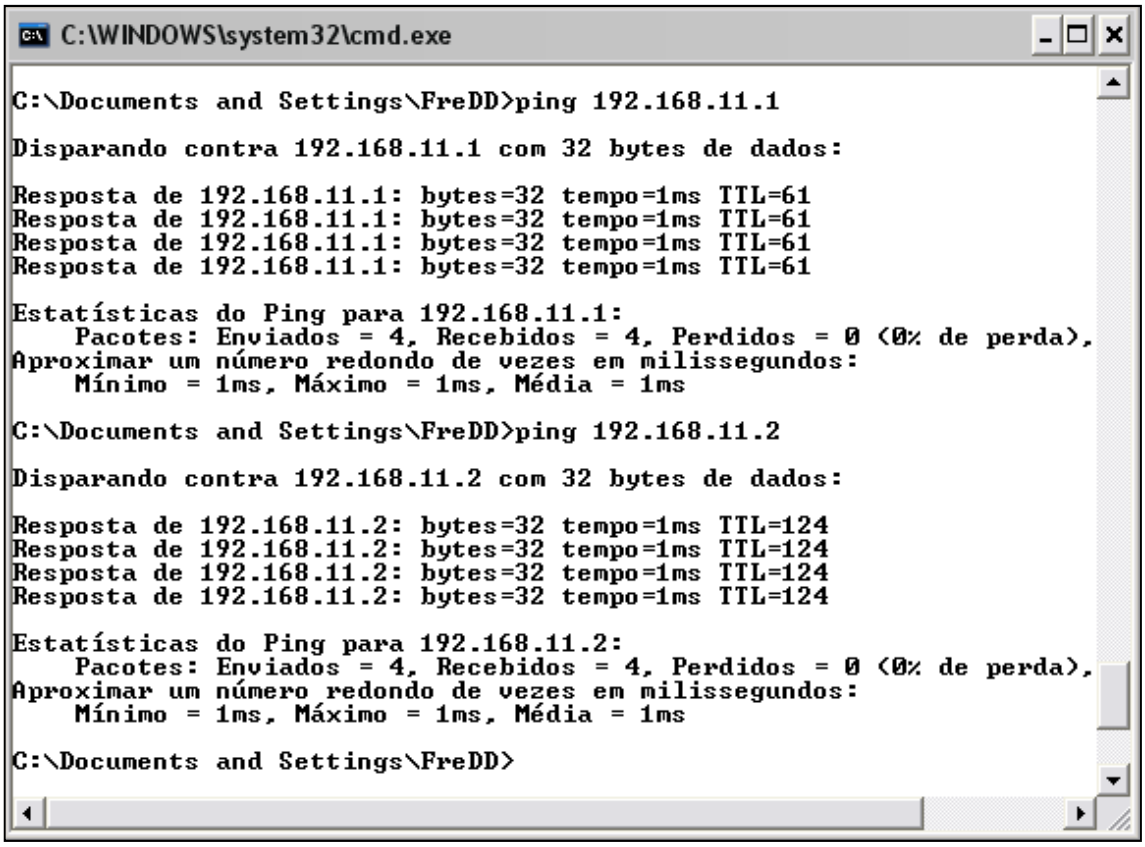

Figura 37 - Teste de conexão do endereço 192.168.11.1 até o *Notebook*

10) Com isso pode-se observar o funcionamento dessa rede. Sendo que esta rede foi realizada para a comunicação entre as redes 192.168.11.0 e 192.168.41.0, no caso, a rede do *Notebook* (*Laptop*) até a rede do Computador (PC);

11) Utilizando o comando *tracert* foram contados os saltos até chegar o destino, sendo que na figura 38 este destino é o Computador (PC) e na figura 39 é o *Notebook* (*Laptop*).

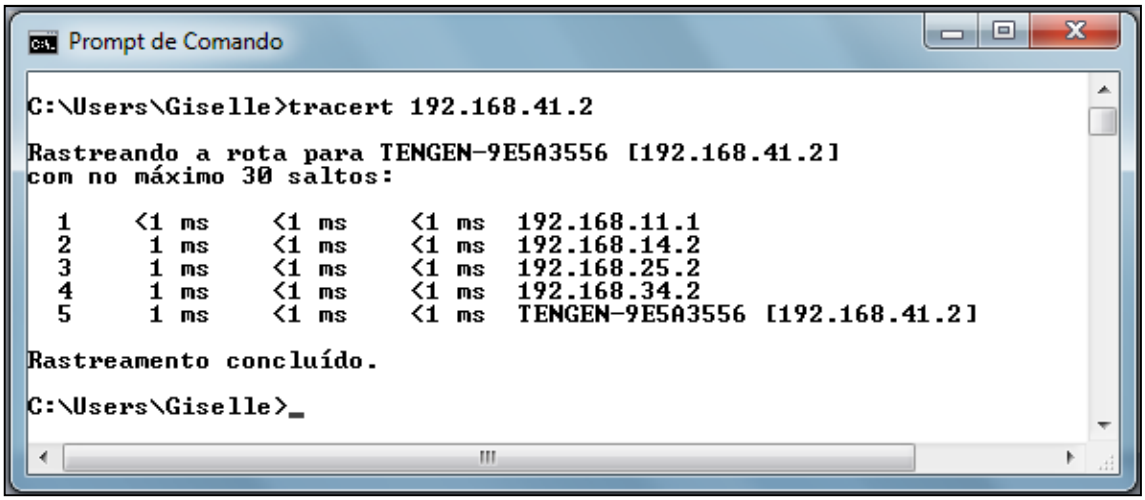

Figura 38 - Comando tracert para verificar as rotas do *Notebook* (*Laptop*) para o Computador (PC)

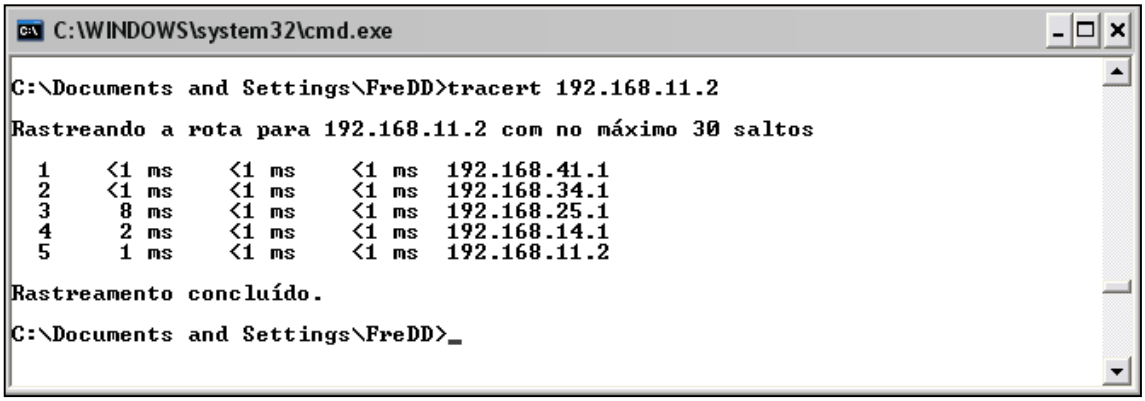

Figura 39 - Comando tracert para verificar as rotas do Computador (PC) para o *Notebook* (*Laptop*)

Experiência 2 com Roteamento Dinâmico:

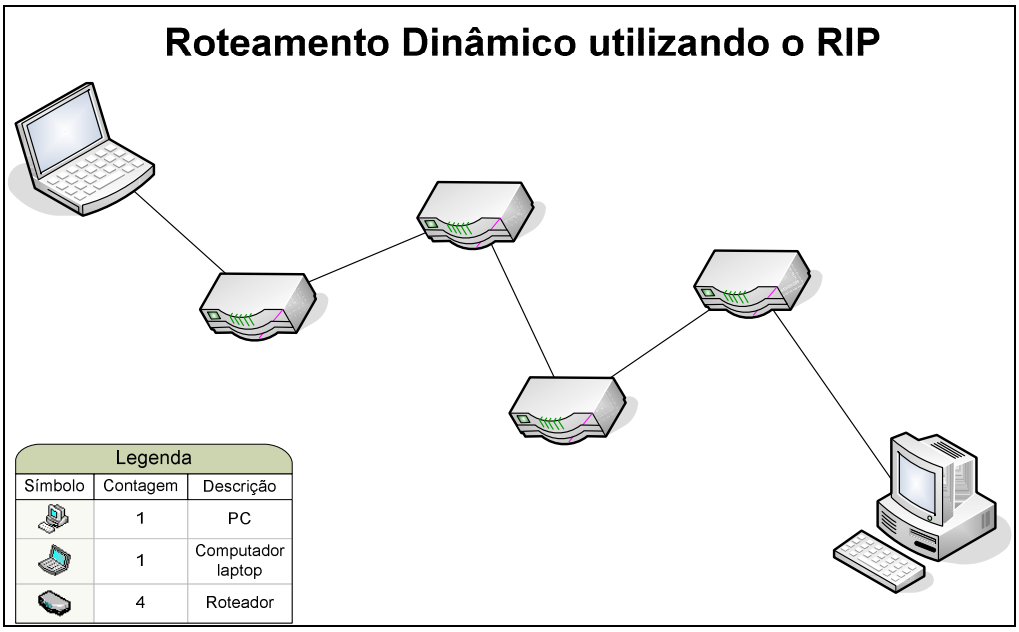

Figura 40 - Experiência 2 realizada em laboratório utilizando o RIP

De acordo com a figura 40, foi realizada essa experiência em laboratório para a configuração do *Routerboard Mikrotik*. Assim descreve-se a seguir esta configuração:

1) Antes de começar a configuração foram utilizados os equipamentos:
   - 1 *Notebook* (*Laptop*);
   - 1 Computador (PC);
   - 4 Roteadores da marca *Routerboard MikroTik*;
   - 5 Cabos UTP CAT5e (cabos de rede);

2) Em seguida foi considerado o seguinte endereço de porta do *Notebook* (*Laptop*): 192.168.11.2 e o endereço do Computador (PC): 192.168.41.2;

3) Repetindo os passos 3, 4, 5 e 6 da experiência 1, tem-se a configuração dos endereços de cada porta no quadro 10, utilizando os mesmo números da experiência anterior;

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.168.11.1	IP 192.168.21.1	IP 192.168.31.1	IP 192.168.41.1
Eth 2				
Eth 3		IP 192.168.14.2	IP 192.168.25.2	IP 192.168.34.2
Eth 4	IP 192.168.14.1		IP 192.168.34.1	
Eth 5		IP 192.168.25.1		

Quadro 10 - Endereços IPs utilizados da experiência 1 para a experiência 2

4) Continuando a parte de configuração tem-se a opção “Routing”, que ao ser clicado abre-se uma sub-barra de menus, utilizando a opção “RIP” que abre uma janela na aba “Interfaces”, onde se clicou no botão “RIP Settings” configuram-se os seguintes campos: “Distribute Default” escolhendo a opção “always” e selecionando as opções “Resdistribute Static Routes” e “Resdistribute Connected Routes” e depois se clica em “OK”; e no botão “+” onde abrirá a janela “New RIP Interface” selecionando a porta [*ether*1, 2, 3, 4, 5 ou *all* (todas)] no botão do campo “Interface” para se configurar as portas que estão conectadas aos roteadores vizinhos, mais que no caso do roteador 1 é somente a porta *ether*4; Assim abaixo segue a tabela 2.

Tabela 2 - Portas / Interfaces configuradas em cada roteador, experiência 2

Roteador 1	Roteador 2	Roteador 3	Roteador 4
Ether 4	*Ether* 3	*Ether* 3	*Ether* 3
	Ether 5	*Ether* 4	

5) Assim seleciona-se a aba “Neighbours” para se inserir, clicando no botão “+”, o endereço IP dos roteadores vizinhos, no caso, como se esta utilizando o roteador 1 tem-se somente o vizinho 192.168.14.2; Dessa forma tem-se a tabela 3 de vizinhos configurados em cada roteador;

Tabela 3 - Portas dos vizinhos de cada roteador, experiência 2

	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Endereço IP do Roteador vizinho	192.168.14.2	192.168.14.1	192.168.25.1	192.168.34.1
		192.168.25.2	192.168.34.2	

6) Depois de configurar todos os endereços e todos os vizinhos, simula-se a rede de roteamento dinâmico utilizando o RIP. Sendo que esta simulação fica

igual a das figuras 32, 33, 34, 35, 36 e 37 na seqüência. Afinal o número de endereços é o mesmo, assim quando se “pinga” essa rede visualiza as mesmas figuras da experiência 1 anterior, pois o tipo de configuração que foi realizada desta parte é a mesma. Mas o RIP configura as rotas de forma dinâmica e não como na experiência 1 que foi de forma estática;

7) Para mostrar que a simulação das duas experiências é a mesma, utilizou-se o utilitário *tracert* para se comparar as figuras 38 e 39 com as 41 e 42, assim quando for analisado não restará duvidas dessa igualdade. Afinal foram utilizados os mesmo endereços IPs das portas.

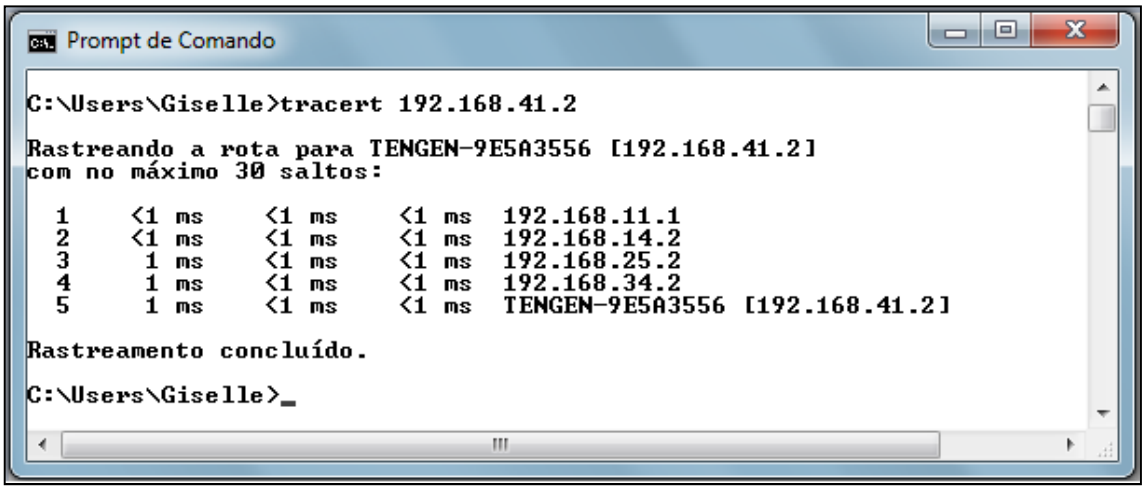

Figura 41 - Comando tracert para verificar as rotas do *Notebook* (*Laptop*) para o Computador (PC)

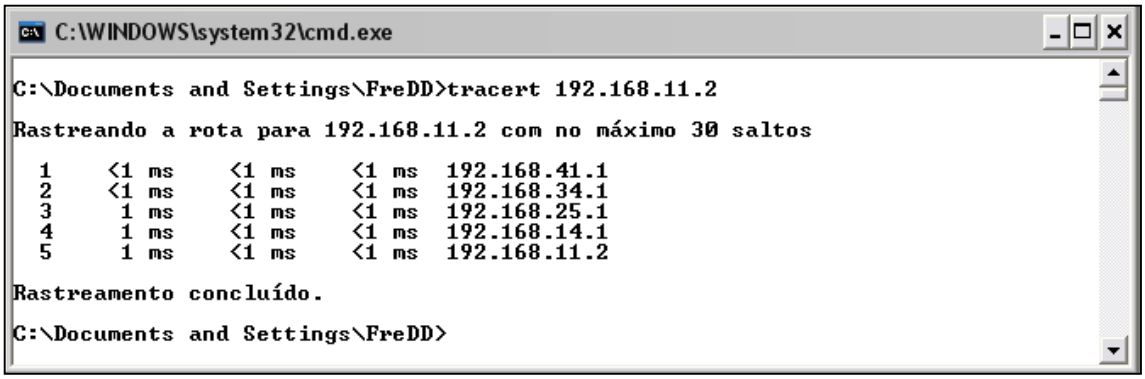

Figura 42 - Comando tracert para verificar as rotas do computador (PC) para o *Notebook* (*Laptop*)

Concluindo as experiências 1 e 2 foi observado que quando utilizado o roteamento

estático (experiência 1), as portas correspondentes aos IPs 192.168.21.1 e 192.168.31.1 configuradas não se consegue alcançá-las por não possuírem rotas para elas, pois qualquer endereço que não tiver rota definida não será encontrado, assim observado na figura 43 a mensagem: "*Host* de destino inacessível".

Já no roteamento dinâmico (experiência 2), que não precisa configurar rotas e sim vizinho (*Neighbours*), os endereços IPs 192.168.21.1 e 192.168.31.1 das portas criadas serão acessados, pois o RIP cria rotas automaticamente ao ser configurada uma nova porta, analisando-se na figura 44 o acesso ao destino final.

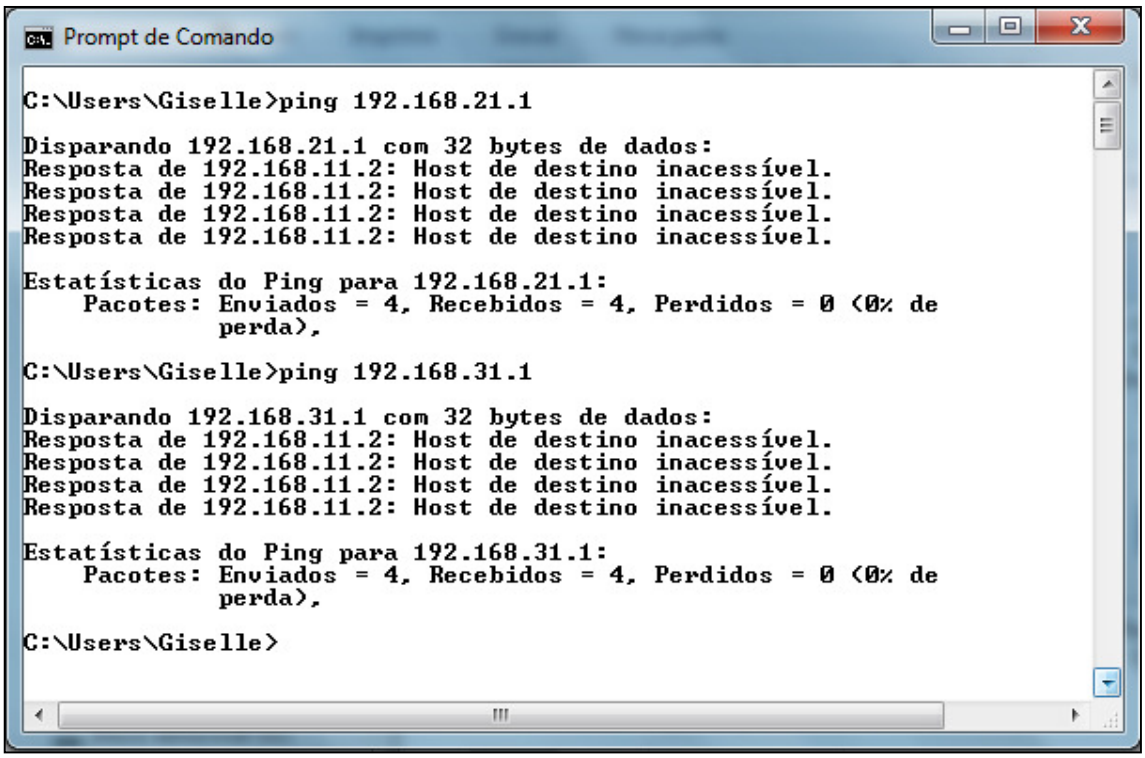

Figura 43 - Roteamento estático sem rotas criadas

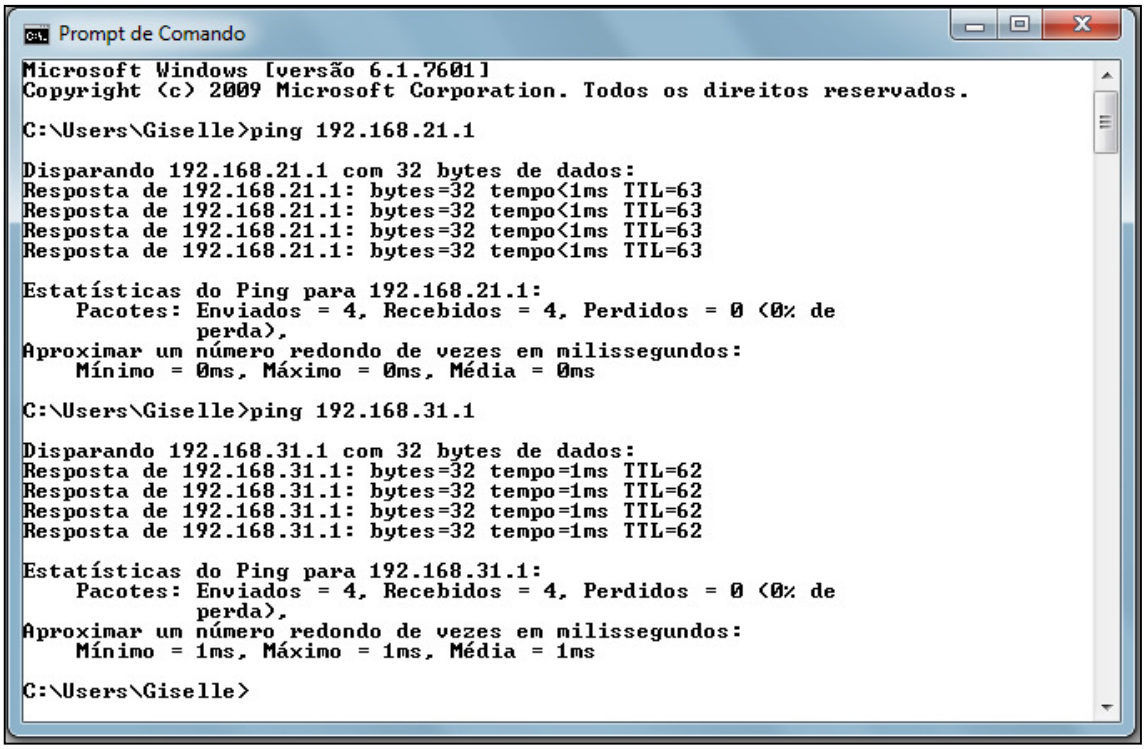

Figura 44 - Roteamento dinâmico com rotas definidas pelo RIP

Depois de testar a simulação 1, temos na seqüência as simulações 2, 3, 4, 5 e 6 que mostrarão as figuras com o seu tipo de topologia, os quadros de endereços criados e as tabelas de rotas criadas de cada experiência realizada; Já a parte de configuração pode-se basear em todo o procedimento da experiência 1 (Simulação 1), com isso seguindo os passos referentes a endereços e rotas que são: passos 3, 4, 5, 6 e 7 anteriormente realizados. Pois a parte de configuração do Routerboard MikroTik é a mesma para qualquer tipo de experiência realizada com roteamento estático, sendo que a diferença entre estas é a quantidade de equipamentos utilizados, onde quanto mais portas usadas maior serão os números de endereços e rotas criados.

Assim seguem-se abaixo as simulações com as experiências testadas em laboratório.

6.2 EXPERIÊNCIAS COM TOPOLOGIA ESTRELA

Simulação 2:

Na experiência 3 (figura 45), utilizaram-se quatro roteadores, e nestes definiu-se os endereços IPs das portas que estão dispostos no quadro 11:

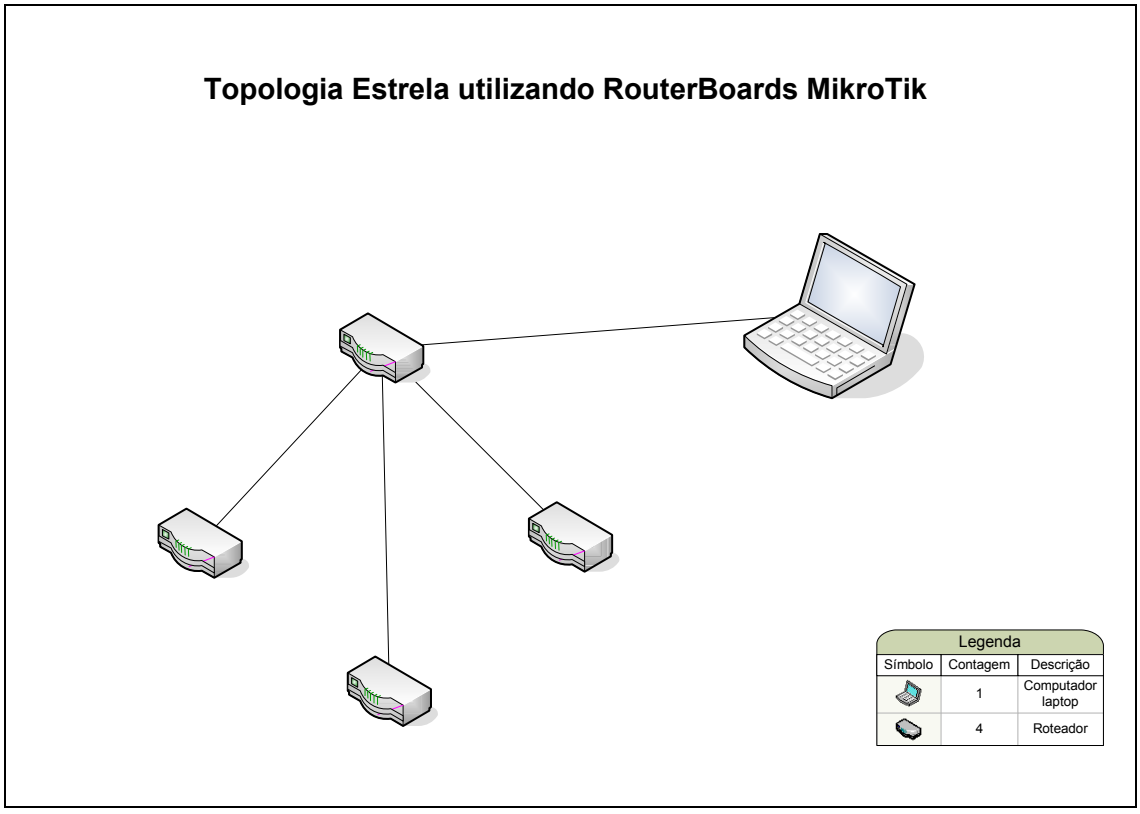

Figura 45 - Experiência 3 realizada em laboratório

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.162.11.1	IP 192.162.21.1	IP 192.162.31.1	IP 192.162.15.2
Eth 2	IP 192.162.12.1			
Eth 3	IP 192.162.13.1	IP 192.162.13.2	IP 192.162.12.2	
Eth 4				IP 192.162.44.2
Eth 5	IP 192.162.15.1			

Quadro 11 - Endereços IPs configurados para a experiência 3

Tabela 4 - Rotas criadas para a experiência 3

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.44.0/24	192.168.15.2	1
	192.168.31.0/24	192.168.12.2	1
	192.168.21.0/24	192.168.13.2	1
Roteador 2	192.168.11.0/24	192.168.13.1	1
Roteador 3	192.168.11.0/24	192.168.12.1	1
Roteador 4	192.168.11.0/24	192.168.15.1	1

Simulação 3:

Foram usados 3 roteadores nesta experiência 4 (figura 46) , e nestes definiu-se os endereços IPs das portas que estão dispostos no quadro 12 e as rotas na tabela 5:

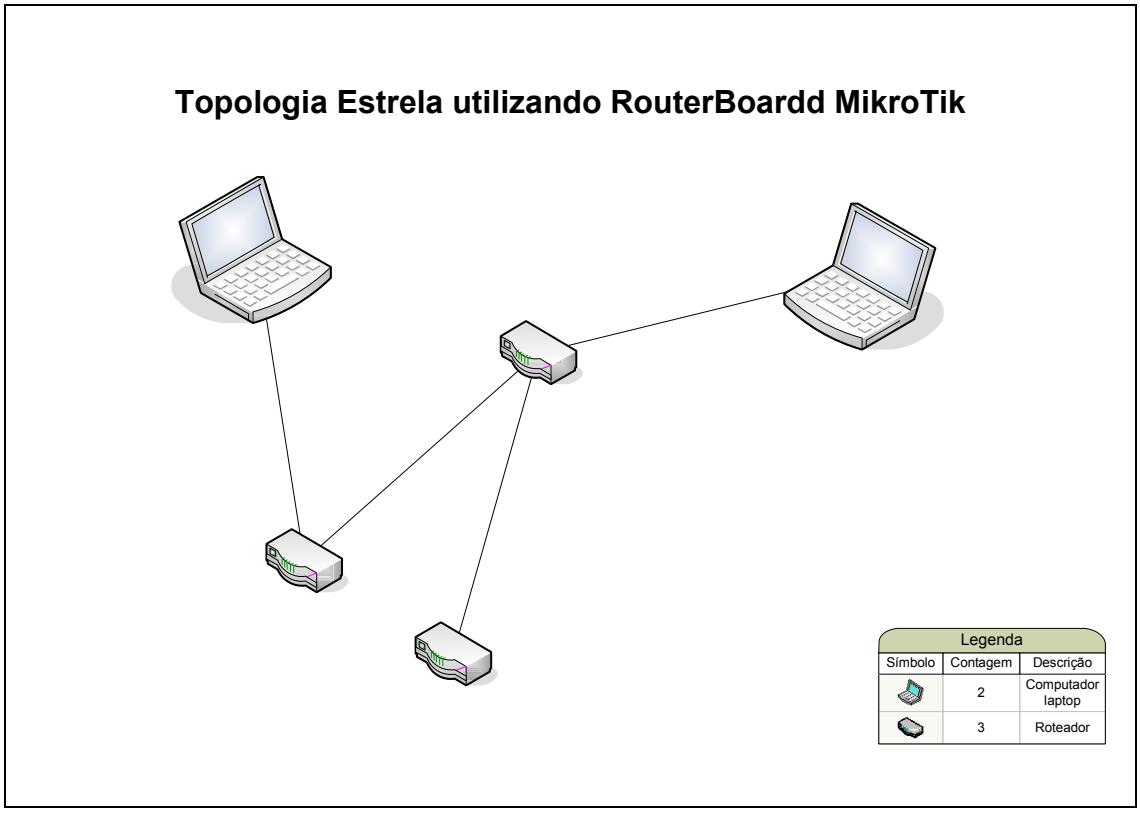

Figura 46 - Experiência 4 realizada em laboratório

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.162.11.1	IP 192.162.21.1		IP 192.162.41.1
Eth 2				
Eth 3				
Eth 4	IP 192.162.14.1			IP 192.162.14.2
Eth 5	IP 192.162.15.1	IP 192.162.15.2		

Quadro 12 - Endereços IPs configurados para a experiência 4

Tabela 5 - Rotas criadas para a experiência 4

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.21.0/24	192.168.15.2	1
	192.168.41.0/24	192.168.14.2	1
Roteador 2	192.168.11.0/24	192.168.14.1	1
Roteador 3	192.168.11.0/24	192.168.14.1	1

Simulação 4:

Foram usados 4 roteadores nesta experiência 5 (figura 47) , e nestes definiu-se os endereços IPs das portas que estão dispostos no quadro 13 e as rotas na tabela 6:

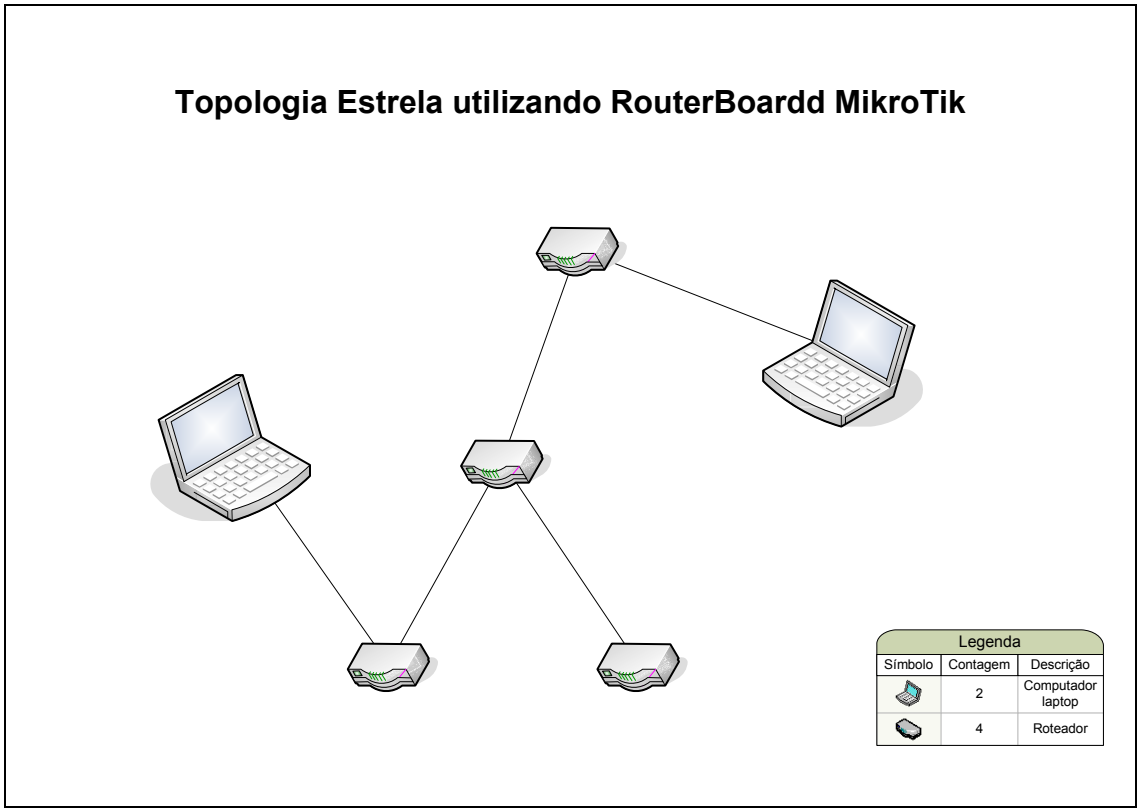

Figura 47 - Experiência 5 realizada em laboratório

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.168.11.1	IP 192.168.21.1	IP 192.168.31.1	IP 192.168.15.2
Eth 2	IP 192.168.12.1			IP 192.168.42.1
Eth 3	IP 192.168.13.1	IP 192.168.13.2	IP 192.168.12.2	
Eth 4				
Eth 5	IP 192.168.15.1			

Quadro 13 - Endereços IPs configurados para a experiência 5

Tabela 6 - Rotas criadas para a experiência 5

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.21.0/24	192.168.13.2	1
	192.168.31.0/24	192.168.12.2	1
	192.168.42.0/24	192.168.15.2	1
Roteador 2	192.168.42.0/24	192.168.13.1	2
	192.168.11.0/24	192.168.13.1	1
	192.168.31.0/24	192.168.13.1	2
	192.168.12.0/24	192.168.13.1	1
	192.168.15.0/24	192.168.13.1	1
Roteador 3	192.168.11.0/24	192.168.12.1	1
	192.168.21.0/24	192.168.12.1	1
	192.168.42.0/24	192.168.12.1	2
	192.168.13.0/24	192.168.12.1	1
	192.168.15.0/24	192.168.12.1	1
Roteador 4	192.168.11.0/24	192.168.15.1	1
	192.168.21.0/24	192.168.15.1	2
	192.168.31.0/24	192.168.15.1	2
	192.168.13.0/24	192.168.15.1	1
	192.168.12.0/24	192.168.15.1	1

Simulação 5:

Foram usados 4 roteadores nesta experiência 6 (figura 48), e nestes definiu-se os endereços IPs das portas que estão dispostos no quadro 14 e as rotas na tabela 7:

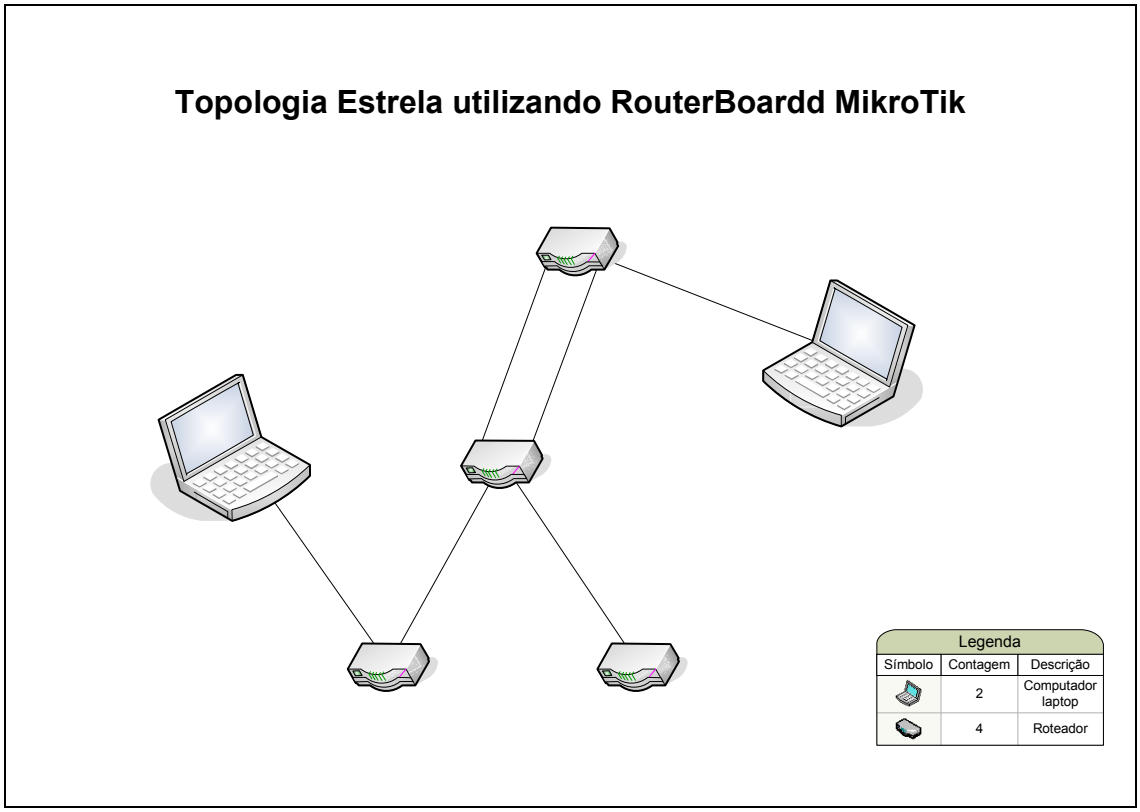

Figura 48 - Experiência 6 realizada em laboratório

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.168.11.1	IP 192.168.21.1	IP 192.168.31.1	IP 192.168.41.1
Eth 2		IP 192.168.22.1		
Eth 3	IP 192.168.23.2	IP 192.168.23.1		IP 192.168.22.2
Eth 4	IP 192.168.24.2	IP 192.168.24.1		
Eth 5		IP 192.168.25.1	IP 192.168.21.2	

Quadro 14 - Endereços IPs configurados para a experiência 6

Tabela 7 - Rotas criadas para a experiência 6

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.31.0/24	192.168.23.1	2
	192.168.31.0/24	192.168.24.1	2
	192.168.25.0/24	192.168.24.1	1
	192.168.21.0/24	192.168.24.1	1
	192.168.41.0/24	192.168.24.1	2
	192.168.41.0/24	192.168.23.1	2
	192.168.25.0/24	192.168.23.1	1
	192.168.22.0/24	192.168.23.1	1
Roteador 2	192.168.11.0/24	192.168.24.2	1
	192.168.31.0/24	192.168.21.2	1
	192.168.11.0/24	192.168.23.2	1
	192.168.41.0/24	192.168.22.2	1
Roteador 3	192.168.11.0/24	192.168.21.1	2
	192.168.24.0/24	192.168.21.1	1
	192.168.25.0/24	192.168.21.1	1
	192.168.23.0/24	192.168.21.1	1
Roteador 4	192.168.11.0/24	192.168.22.1	2
	192.168.23.0/24	192.168.22.1	1
	192.168.25.0/24	192.168.22.1	1
	192.168.24.0/24	192.168.22.1	1

6.3 EXPERIÊNCIA COM TOPOLOGIA ANEL

Simulação 6:

Foram usados 4 roteadores nesta experiência 7 (figura 49) , e nestes definiu-se os endereços IPs das portas que estão dispostos no quadro 15 e as rotas na tabela 8:

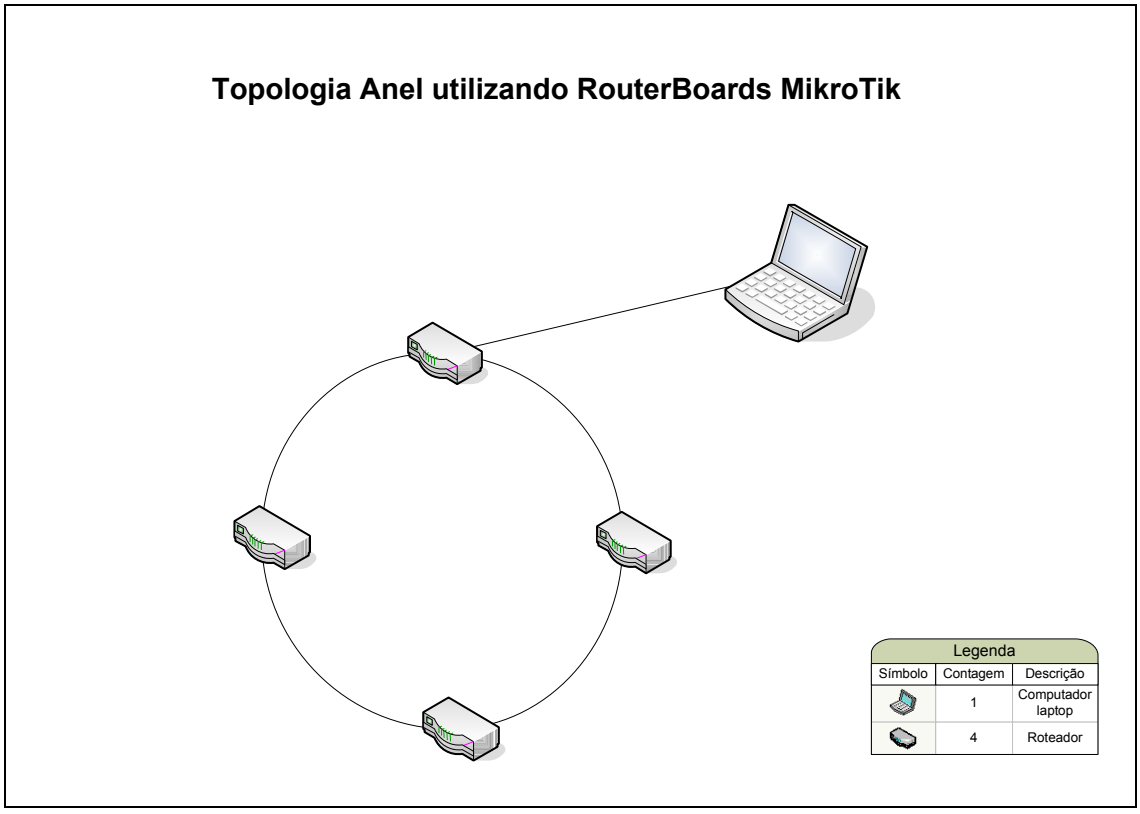

Figura 49 - Experiência 7 realizada em laboratório

Porta	Roteador 1	Roteador 2	Roteador 3	Roteador 4
Eth 1	IP 192.168.11.1	IP 192.168.21.1	IP 192.168.31.1	IP 192.168.41.1
Eth 2	IP 192.168.12.1	IP 192.168.22.2	IP 192.168.32.1	IP 192.168.13.2
Eth 3	IP 192.168.13.1	IP 192.168.12.2	IP 192.168.22.2	IP 192.168.32.2
Eth 4				
Eth 5				

Quadro 15 - Endereços IPs configurados para a experiência 7

Tabela 8 - Rotas criadas para a experiência 7

	Dst. Address (Endereços de rede)	*Gateway* (Endereços da porta de saída)	*Distance* (*Hops*)
Roteador 1	192.168.22.0/24	192.168.12.2	1
	192.168.22.0/24	192.168.13.2	2
	192.168.32.0/24	192.168.13.2	1
	192.168.32.0/24	192.168.12.2	2
Roteador 2	192.168.13.0/24	192.168.12.1	1
	192.168.13.0/24	192.168.22.2	2
	192.168.32.0/24	192.168.22.2	1
	192.168.32.0/24	192.168.12.1	2
	192.168.11.0/24	192.168.12.1	1
	192.168.11.0/24	192.168.22.2	3
Roteador 3	192.168.12.0/24	192.168.22.1	1
	192.168.12.0/24	192.168.32.2	2
	192.168.13.0/24	192.168.22.1	2
	192.168.13.0/24	192.168.32.2	1
	192.168.11.0/24	192.168.22.1	2
	192.168.11.0/24	192.168.32.2	2
Roteador 4	192.168.22.0/24	192.168.32.1	1
	192.168.22.0/24	192.168.13.1	2
	192.168.12.0/24	192.168.13.1	1
	192.168.12.0/24	192.168.32.1	2
	192.168.11.0/24	192.168.13.1	1
	192.168.11.0/24	192.168.32.1	3

CONSIDERAÇÕES FINAIS

Com a conclusão deste trabalho observou-se que cada capítulo estudado, foi importante para que na hora das experiências práticas entendesse as funções de cada utilidade de uma rede de computadores, no caso de uma rede de roteamento. Pois tudo que foi visto e lido é de extrema importância para o objetivo final que foi aprender sobre roteamento, poder ensinar instrutores para quem sabe a criação de um laboratório de roteamento na Faculdade Novo Milênio, e também pessoas capazes de aprender a desenvolver e repetir as experiências propostas. Possibilitando a configuração de outras funções desse roteador em trabalhos futuros, aprimorando essas experiências práticas realizadas ou em novas experiências com diferentes topologias. Assim o estudo de caso fica tranqüilo para ser desenvolvido com leitores já entendidos do assunto mostrado nos capítulos anteriores.

No capítulo do estudo de caso a proposta foi mostrar como com poucos roteadores podem-se criar várias topologias de redes e muitas experiências. Afinal todas estas foram simuladas e testadas utilizando roteadores, *Routerboard MikroTik*, por serem mais fáceis de configurar, ajudando no desenvolvimento dessas redes, onde todas as experiências com roteamento estático tem o mesmo tipo de configuração.

Por exemplo, nas experiências 1 e 2 (simulação 1) do estudo de caso, foi realizada uma comparação entre roteamento estático e dinâmico, onde ao concluir estas observou-se como é indiscutível o tempo perdido ao fazer as rotas estáticas, pois dependendo da topologia a tabela de cada roteador pode simplesmente ficar enorme, com isto o RIP poupa tempo, pois só é preciso definir 3 parâmetros em cada roteador e todos os roteadores estarão conectados e trocando tabelas. Porém o RIP, só aceita no máximo 15 hops (saltos), então não é aconselhado para redes com mais do que 15 roteadores, pois algumas sub-redes não alcançarão as outras.

A diferença na utilização do roteamento estático para o dinâmico utilizando o RIP foi mostrada nas figuras 43 (experiência 1) e 44 (experiência 2) da simulação 1. Onde nestas figuras quando não se criar rotas para o roteamento estático, mesmo tendo endereços criados não consegue se comunicar com as portas destes endereços. Já para o dinâmico só criando os vizinhos (*Neighbours*), as portas que estiverem com endereços criados serão encontradas e se comunicarão com as demais dentro

dessa rede. Observando-se que com o roteamento dinâmico tem uma vantagem enorme quando se tem que criar endereços e rotas, afinal às rotas nem precisarão ser criadas, pois são automáticas quando são criados os vizinhos (*Neighbours*).

As outras simulações foram para mostrar que mesmo utilizando outros tipos de topologias de rede, a configuração da rede de roteamento será a mesma, afinal a mudança de uma topologia para outra está nas vantagens, desvantagens e a forma de montar a sua estrutura. Assim pode-se observar que estas simulações obtiveram um resultado significativo.

REFERÊNCIAS

[1] TANENBAUM, Andrew S. Redes de Computadores. Tradução da Quarta Edição. Campus. 2003. 968 p.

[2] TORRES, Gabriel. Redes de Computadores. Versão Revisada e Atualizada. Nova Terra. 2009. 834 p.

[3] MARQUES, Wilson Soler. TCP/IP – Projetando Redes. Brasport. 2000. 332 p.

[4] TANENBAUM, Andrew S. Computer **Networks (Redes de Computadores)**. Fourth Edition (Quarta Edição). Campus. 2002. 632 p.

[5] TORRES, Gabriel. **Redes de Computadores Curso Completo**. Axcel Books. 2001. 688 p.

[6] <http://www.rnp.br/newsgen/9705/n1-1.html>, acesso em 02 jun. 2011.

[7] CBPF-NT-010/0. INTRODUÇÃO AO *PING* E *TRACEROUTE*. 26/11/02. <http://www.rederio.br/downloads/pdf/nt01002.pdf>, acesso em 02 jun. 2011, ref. Figura 8 – Pacote ICMP.

[8] <http://www.ee.pucrs.br/~decastro/pdf/Redes_Comutadas_Cap2_1.pdf>, acesso em 02 jun. 2011.

[9] <http://walfredo.dsc.ufcg.edu.br/cursos/2003/redes20031/p4c.pdf>, acesso em 02 jun. 2011, ref. Figura 17 – Tabela de Roteamento.

[10] <http://www.artigonal.com/ti-artigos/topologias-de-rede-991863.html>, acesso em 07 jun. 2011.

[11] UNICENTRO NEWTON PAIVA, Tecnologia em Processamento de Dados. TOPOLOGIAS DE REDE. <http://www.micropic.com.br/noronha/Informatica/REDES/Redes.pdf>, acesso em 07 jun. 2011.

[12] <http://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens>, acesso em 07 jun. 2011.

[13] <http://pt.scribd.com/doc/402365/Topologias-de-Rede>, acesso em 07 jun. 2011.

[14] <https://encrypted.google.com/search?q=figuras+de+roteadores&hl=pt-BR&biw=1280&bih=699&prmd=ivns&tbm=isch&tbo=u&source=univ&sa=X&ei=jy_4TYaSL4LY0QHGwczHCw&ved=0CFoQsAQ>, acesso em 08 jun. 2011, ref. Figura 16 – Tipos de Roteadores.

[15] <http://penta.ufrgs.br/Esmilda/tcp.html>, acesso em 15 jun. 2011.

[16] <http://www.cbpf.br/~sun/pdf/tcp.pdf>, acesso em 15 jun. 2011.

[17] CBPF-NT-004/2000. PROTOCOLOS TCP/IP. 04/04/01. <http://mesonpi.cat.cbpf.br/naj/tcpipf.pdf>, acesso em 15 jun. 2011.

[18] <http://pt.kioskea.net/contents/internet/tcp.php3>, acesso em 15 jun. 2011.

[19] <http://www.pop-rs.rnp.br/ovni/tcpip/>, acesso em 15 jun. 2011.

[20] <http://www.pop-rs.rnp.br/ovni/tcpip/t_ip.htm>, acesso em 16 jun. 2011.

[21] <http://www.wirelessbrasil.org/wirelessbr/colaboradores/hisatugu/ipv6_03.html>, acesso em 16 jun. 2011, ref. Quadro 8 – Comparação do IPv6 com o IPv4.

[22] <http://www.hardware.com.br/termos/ipv6>, acesso em 16 jun. 2011.

[23] <http://penta.ufrgs.br/Esmilda/datagram.html>, acesso em 17 jun. 2011.

[24] <http://pt.kioskea.net/contents/internet/protip.php3>, acesso em 17 jun. 2011, ref. Figura 6 - Estrutura do Cabeçalho do Datagrama IP.

[25] <http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm>, acesso em 18 jun. 2011, ref. Figura 15 – Conversão do endereço MAC em IID.

[26] <http://www.mikrotik.com>, acesso em 19 jun. 2011.

[27] <https://encrypted.google.com/search?hl=pt-BR&biw=1280&bih=699&tbm=isch&sa=1&q=figuras+de+roteador+da+mikrotik&oq=figuras+de+roteador+da+mikrotik&aq=f&aqi=&aql=&gs_sm=e&gs_upl=2960l8764l0l14l14l0l12l0l0l310l514l2-1.1>, acesso em 19 jun. 2011, ref. Figura 19 - *Routerboard MikroTik.*

[28] <http://wiki.locaweb.com.br/pt-br/Como_utilizar_os_comandos_Ping_e_Tracert%3F>, acesso em 19 jun. 2011.

APÊNDICES

APÊNDICE A – SUGESTÃO DE EXPERIÊNCIA

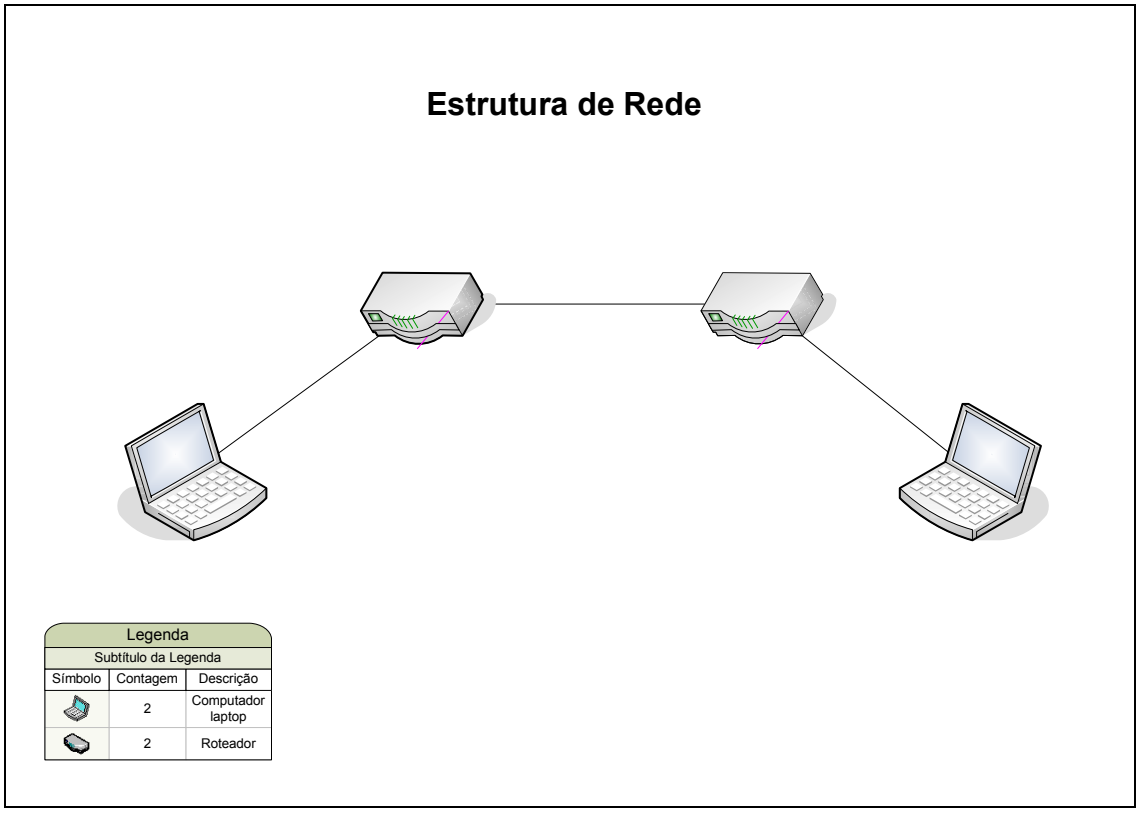

Figura 50 - Experiência realizada em laboratório

Foi simulada em laboratório a experiência 8 mostrada na figura à cima.
Nesta sugestão deve-se testar a simulação utilizando os comandos “ping” e “tracert”. Descrevendo esse procedimento temos:

1) Primeiramente foram separados os seguintes equipamentos:
   - 2 Roteadores (*Routerboard MikroTik*);
   - 3 Cabos de rede;
   - 2 *Laptops*;

2) Utilizando os cabos de rede, ligaram-se os *Laptops* aos roteadores, e os roteadores entre si, sobrando assim nenhum cabo;

3) Depois de ligados deve-se obter acesso aos roteadores por meio dos *Laptops* da seguinte maneira, primeiro encontra-se o endereço IP do roteador conectado ao respectivo *Laptop* por meio do *winbox,* segundo passo é colocar o *Laptop* na mesma rede IP sendo que o *Gateway* inserido no *Laptop* deve ser o endereço IP do roteador em que o *Laptop* está conectado, depois configurar qualquer outra porta do roteador para que esta esteja na mesma rede do outro roteador, essas redes tem que ser distintas, totalizando três redes diferentes;

4) Após serem configuradas as portas dos roteadores, tem-se que criar as rotas de um roteador para o outro, dizendo a rede de destino e o *Gateway* (porta do outro roteador);

5) Depois de configuradas as rotas, devem-se usar os comandos “ping” e “tracert” para testar se a rede de um *Laptop* está conectada a outra. Assim concluindo essa rede de roteamento estático.

APÊNDICE B – FOTOS

Figura 51 - Montagem em laboratório da experiência 1

Figura 52 - Montagem em laboratório da experiência 1

Figura 53 - Montagem em laboratório da experiência 1

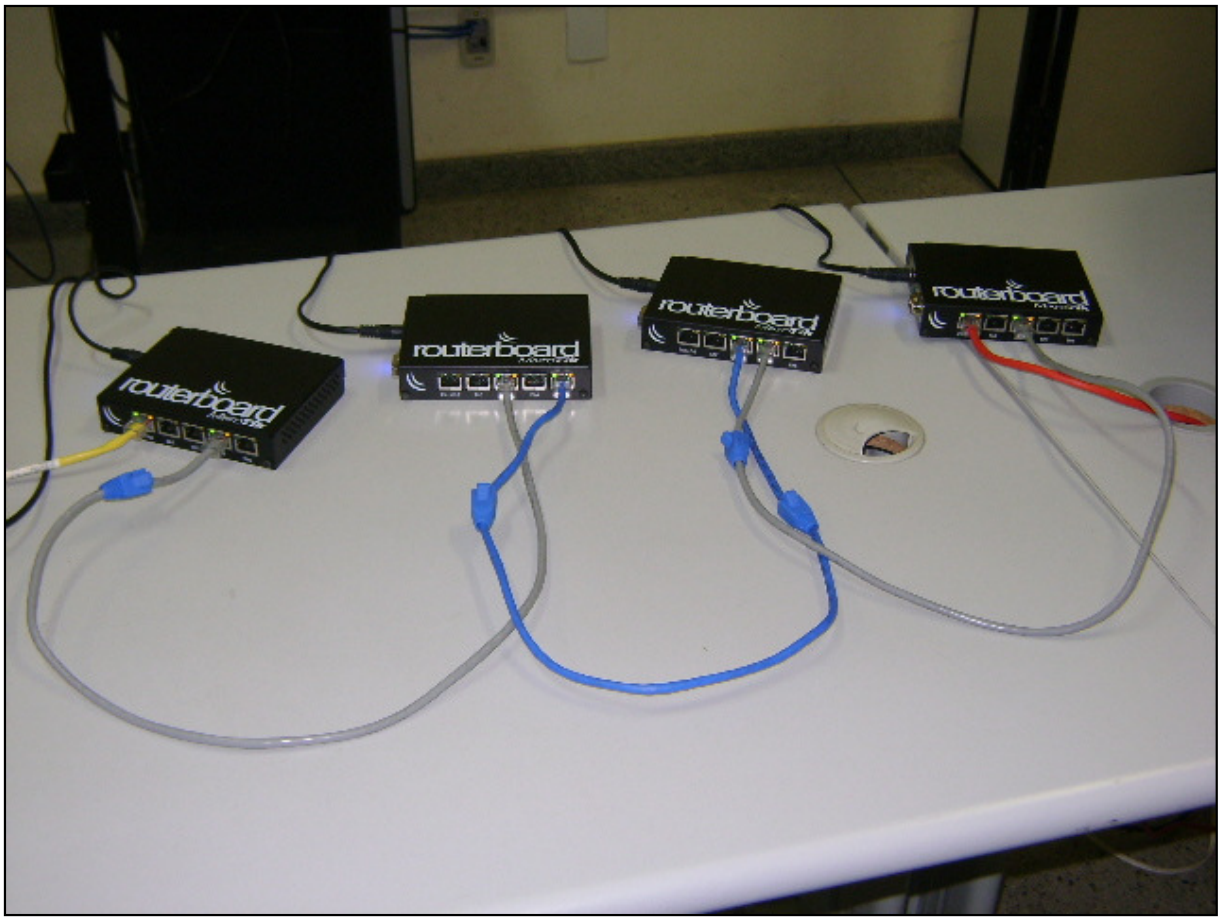

Figura 54 - Montagem em laboratório da experiência 1, roteadores

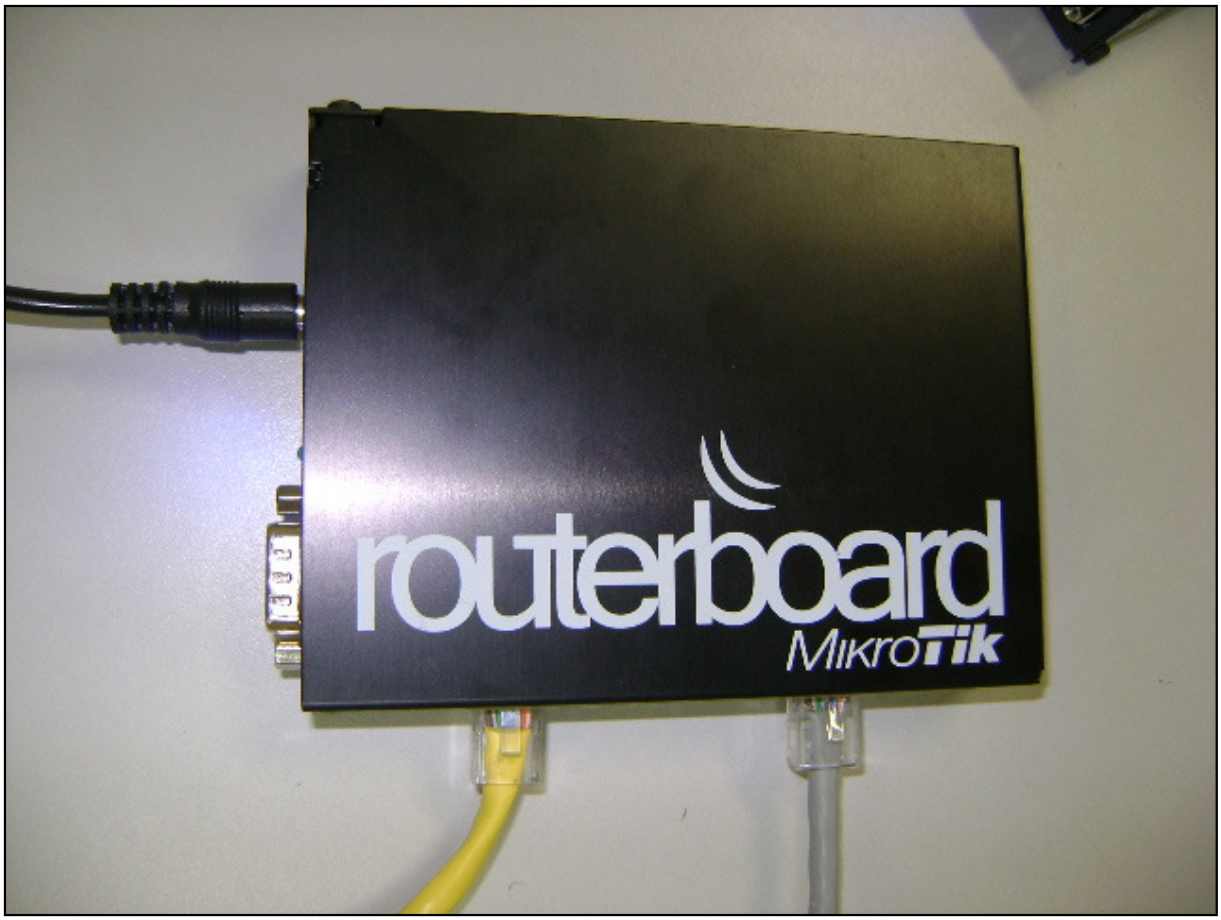

Figura 55 - Montagem em laboratório da experiência 1, roteador