

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM SOFTWARE LIVRE APLICADO
A TELEMÁTICA

Implantação de Compartilhamento de Internet em Condomínios
Residenciais

IVO RODRIGUES DE OLIVEIRA

CURITIBA

2013

IVO RODRIGUES DE OLIVEIRA

**Implantação de Compartilhamento de Internet em Condomínios
Residenciais**

Monografia apresentada como requisito parcial para obtenção do título de Especialista no Curso de Especialização em Software Livre Aplicado em Telemática da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Kleber Kendy Horikawa Nabas

CURITIBA

2013

DEDICATÓRIA

Dedico este trabalho à minha esposa Solange, pelo incentivo, paciência, dedicação e principalmente à compreensão pelas horas que não passamos juntos, abdicando do seu tempo para que eu pudesse realizar um sonho.

RESUMO

A internet está cada vez mais inserida em nosso cotidiano, já não há distinção de classe social. Mas ainda o custo de se instalar internet banda larga em residências de população de baixa renda ainda é proibitivo. Este trabalho tem por objetivo planejar, projetar e implantar acesso à banda larga à condomínios residenciais utilizando equipamentos de alta tecnologia e baixo custo.

SUMÁRIO

LISTA DE FIGURAS	4
LISTA ABREVIATURAS E SIGLAS	5
1 - Introdução	8
1.1 Objetivos.....	9
1.2 Organização do Trabalho	9
2 – Fundamentação Teórica.....	10
2.1 Redes Locais	10
2.1.1 Topologia em estrela.....	11
2.1.2 Topologia em anel.....	12
2.1.3 Topologia em barramento	13
2.1.4 Rede Ethernet	14
2.1.5 O padrão Ethernet na camada física.....	15
2.1.6 Proteção da rede – <i>Firewall</i>	16
2.1.7 Protocolo TCP/IP.....	17
3 – Implementação da rede.....	19
3.1 Topologia utilizada	19
3.2 Ativos da rede utilizados	20
3.3 Configuração dos equipamentos	21
3.4 Instalação Mikrotik	21
3.5 Configurando Nat no Mikrotik	25
3.6 Configurando servidor PPPoE	26
3.7 Adicionando clientes PPPoE	28
3.8 <i>Firewall</i> no Mikrotik	29
4 – Conclusão	31

LISTA DE FIGURAS

Figura 1 - Topologia em estrela cada computador liga-se ao ponto central do hub.	11
Figura 2 - Topologia em anel em que os computadores são conectados entre si e em loop fechado.....	12
Figura 3 - Topologia de barramento em que todos os computadores estão ligados a um cabo único.	13
Figura 4 - Funcionamento do mecanismo CSMA/CD.....	15
Figura 5 - Pacote TCP/IP	17
Figura 6 - Rede computadores em condomínio compartilhando a internet.	20
Figura 7- Instalação servidor Mikrotik.....	21
Figura 8 - Tela do Winbox Mikrotik.....	22
Figura 9 - Configuração IP concessionária	23
Figura 10 - Configuração endereço de rede LAN.....	24
Figura 11 - Configurando NAT no Mikrotik	25
Figura 12 - Configurando o servidor PPPoE	27
Figura 13 - Adicionando clientes PPPoE.....	28
Figura 14 - Firewall Mikrotik	29

LISTA ABREVIATURAS E SIGLAS

LAN -	Local Area Network
UTP -	Unshielded Twisted Pair (Par Trançado sem Blindagem)
Gbps-	Giga bytes por segundo
CSMA/CD -	Carrier Sense Multiple Access with Collision Detect
IEEE -	Institute of Electrical and Eletronic Engineers
AUI -	Attachment Unit Interface
MII -	Media Independent Interface
GMII -	Gigabit Media Independent Interface
TCP -	Transmission Control Protocol
IP -	Internet Protocol
FTP -	File Transfer Protocol
UDP -	User Datagram Protocol
QoS -	Quality Of Service
MAC -	Media Access Control
PPP -	Point – to - Point Protocol
PPPoE -	Point – to - Point Protocol Over Ethernet

1 - Introdução

O aumento da demanda por acesso à banda larga no Brasil seja para as empresas ou para usuários residenciais, tem gerado um grande fluxo de dados transmitidos pelas redes de internet. Esse fluxo crescente de dados traz consigo os perigos inerentes a esse aumento de tráfego como redes instáveis, acesso não autorizado a dados, roubo de dados, senhas e arquivos confidenciais. Além disso, a população de baixa renda ainda não tem acesso à internet banda larga, pois o maior percentual de instalação de internet banda larga está nas mãos das grandes operadoras de telefonia, gerando tarifas inviáveis a essas famílias.

Para resolver parte destes problemas várias empresas criaram soluções para gerenciar redes com baixos custos e minimizar estes riscos, uma que merece destaque é a Mikrotik, empresa criada na Letônia em 1995 que produz equipamentos voltados para gerenciamento de redes cabeadas e *wireless*.

Neste trabalho será abordado o referido sistema; um software baseado em sistema Linux que pode ser usado em microcomputadores ou *routerboards* fabricados pela mesma empresa. É um software proprietário, ou seja, não é gratuito, apesar de seu custo consideravelmente baixo, pode-se destacar sua excelente capacidade de gerenciamento.

O sistema possui *interface* gráfica em ambiente Windows amigável, de fácil administração, além disso, há a opção para usuários da plataforma Linux, com exibição de gráficos de utilização em tempo real, controle de banda, monitoramento de acessos e bloqueio de máquinas.

1.1 Objetivos

O objetivo geral deste trabalho é através de pesquisas realizar um levantamento das tecnologias de conexões de redes utilizadas atualmente. Após este estudo, implementar uma rede estruturada de conexão à internet em um condomínio residencial, através de um ponto de acesso comum, disponibilizar acesso à rede mundial de computadores, zelando pela segurança dos condôminos utilizando um computador firewall.

1.2 Organização do Trabalho

Este trabalho está dividido em 4 capítulos

O capítulo 2 apresenta um embasamento teórico sobre o tema que será abordado.

O capítulo 3 traz o modelo de configuração de rede implantada bem como suas configurações.

O capítulo 4 refere-se à conclusão do trabalho apresentado.

2 – Fundamentação Teórica

2.1 Redes Locais

As redes locais, muitas vezes chamadas de LANs, são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais de empresas, permitindo o compartilhamento de recursos (por exemplo, impressoras e arquivos) e a troca de informações. As LANs têm três características que as distinguem de outros tipos de redes: (1) tamanho, (2) tecnologia de transmissão e (3) topologia (TANENBAUM, 2003).

As LANs têm tamanho restrito, o que significa que o pior tempo de transmissão é limitado e conhecido com antecedência. O conhecimento deste limite permite a utilização de determinados tipos de projetos que em outras circunstâncias não seriam possíveis, além de simplificar o gerenciamento da rede.

A tecnologia de transmissão das LANs pode ser via conexão sem fio, fibra ótica ou através de um cabo de cobre, as quais todas as máquinas estão conectadas. As LANs tradicionais funcionam em velocidade de 10 Mbps a 100 Mbps, têm baixo retardo (microsegundos ou nanossegundos) e cometem pouquíssimos erros. As LANs mais modernas operam em até 10 Gbps (TANENBAUM, 2003).

Diversos tipos de tecnologias de LAN têm sido inventadas, é importante conhecer como as tecnologias específicas são semelhantes e como diferem. Para

ajudar a entender as semelhanças, cada rede é classificada em uma categoria de acordo com sua topologia ou forma geral (COMER, 2007).

2.1.1 Topologia em estrela

Uma rede usa a topologia de estrela se todos os computadores se prendem a um ponto central figura 1.

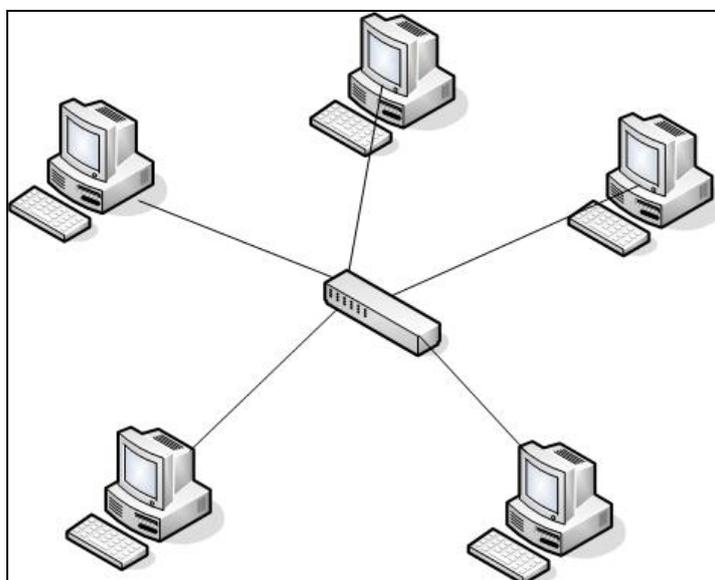


Figura 1 - Topologia em estrela cada computador liga-se ao ponto central do hub.

Uma vez que uma rede em forma de estrela se assemelha a uma roda, o centro de uma rede em estrela é freqüentemente chamado de *hub*. Um *hub* típico consiste de um dispositivo eletrônico que aceita dados de um computador remetente e os entrega para o destino apropriado.

Na prática, as redes em estrela raramente têm uma forma simétrica em que o *hub* esteja a uma distância igual de todos os computadores. Freqüentemente um *hub* reside em uma localização separada dos computadores acoplados a ele.

2.1.2 Topologia em anel

Na topologia em anel, os computadores são organizados de forma que estejam conectados em um loop fechado, um cabo conecta o primeiro computador a um segundo computador, outro cabo conecta o segundo a um terceiro, e assim por diante, até que um cabo conecte o computador final de volta ao primeiro. É importante entender que o anel, assim como a topologia em estrela, refere-se a conexões lógicas entre computadores, não à orientação física, os computadores e as conexões em uma rede em anel não precisam ser organizados em círculo (COMER, 2007).

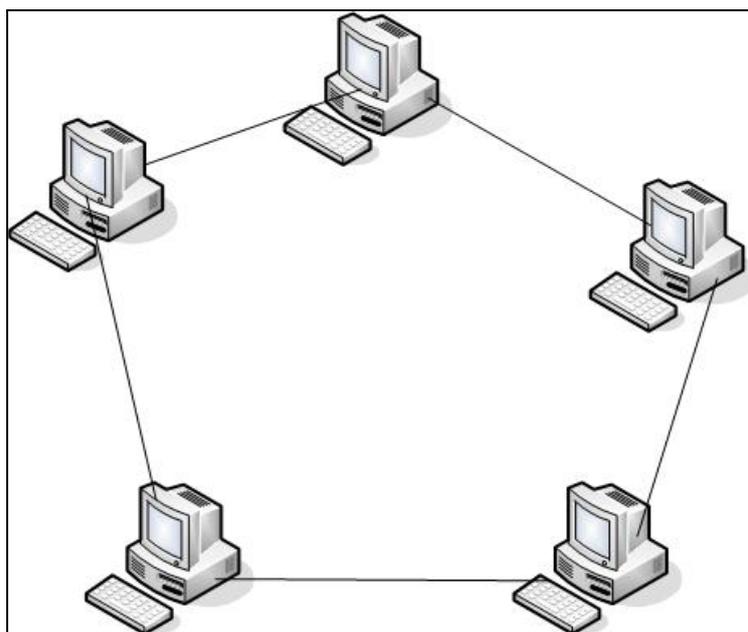


Figura 2 - Topologia em anel em que os computadores são conectados entre si e em loop fechado.

2.1.3 Topologia em barramento

Uma rede que usa uma topologia de barramento normalmente consiste em um único cabo longo aos quais computadores se acoplam. Qualquer computador conectado a um barramento pode enviar um sinal através do cabo, e todos os computadores receberão esse sinal. Como todos os computadores ligados pelo cabo podem detectar um sinal elétrico, qualquer computador pode enviar dados a qualquer computador outro computador. Naturalmente, os computadores acoplados a uma rede de barramento devem se coordenar para assegurar que somente um computador envie um sinal a cada momento, evitando o caos.

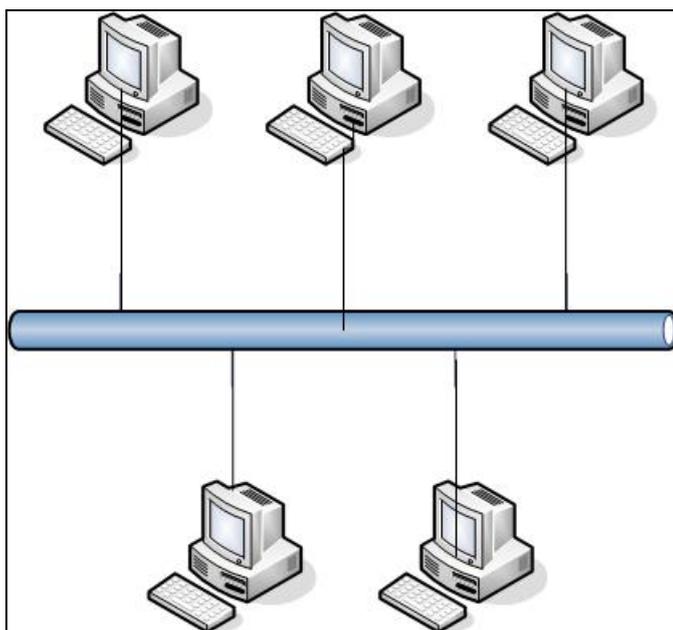


Figura 3 - Topologia de barramento em que todos os computadores estão ligados a um cabo único.

2.1.4 Rede Ethernet

Ethernet é um método de acesso ao meio por contenção (*contention media access method*) que permite que todos os dispositivos (*hosts*) em uma rede Ethernet compartilhem a mesma largura de banda de um link. A Ethernet é muito popular devido à sua descomplicada implementação, consolidação no mercado, escalabilidade, baixo custo e facilidade de atualização para novas tecnologias (como Gigabit e 10 Gigabit Ethernet). O padrão Ethernet utiliza especificações das camadas de enlace e física.

Redes Ethernet utilizam uma técnica de acesso chamada de Carrier Sense Multiple Access with Collision Detect (CSMA/CD), o que permite aos dispositivos o compartilhamento homogêneo de largura de banda, evitando que dois dispositivos transmitam simultaneamente em um mesmo meio (figura 4). A técnica CSMA/CD foi a solução encontrada para o problema de colisões que ocorriam quando pacotes eram simultaneamente transmitidos de diferentes dispositivos em um mesmo meio (FILIPPETTI, 2008).

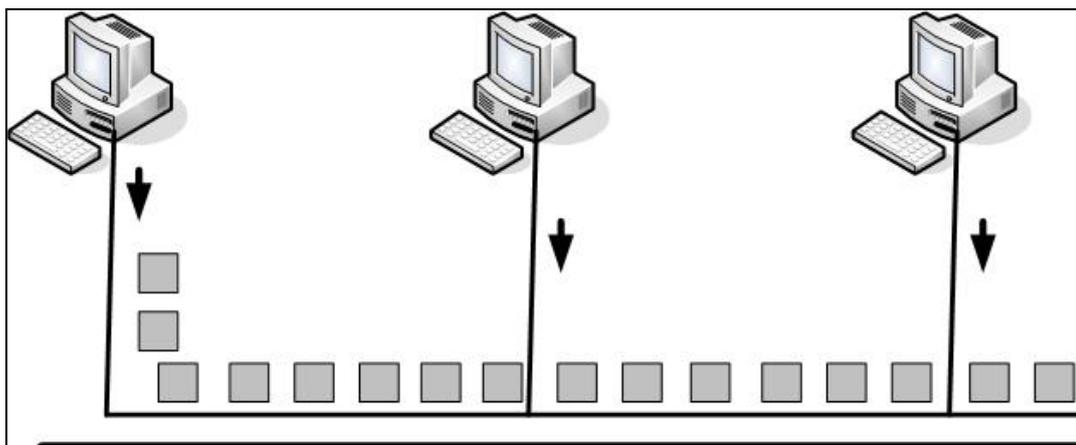


Figura 4 - Funcionamento do mecanismo CSMA/CD

2.1.5 O padrão Ethernet na camada física

10Base2	185 metros
10Base5	500 metros
10BaseT	100 metros (CAT 3 par trançado sem blindagem - UTP)
100BaseTX	100 metros (CAT 5, 6, 7 par trançado sem blindagem - UTP)
100BaseFX	400 metros (65,2/125 μ fibra monomodo)
1000BaseCX	25 metros (para trançado blindado - STP)
1000BaseT	100 metros (CAT5 – 4 pares trançados sem blindagem - UTP)
1000BaseSX	260 metros (62,5/50 μ fibra multimodo)
1000BaseLX	10 Km (9 μ fibra monomodo)

Tabela 1 - Padrão Ethernet

Cada uma das notações anteriores define uma interface de conexão diferente. Tais notações são de extrema valia na identificação de informações importantes, o significado da sintaxe utilizada é:

[taxa máxima de transmissão] [tipo de transmissão] [comprimento máximo do cabo]

Exemplo : 10Base2 = [10 Mbps] [*Baseband*] [aprox. 200 metros (185 metros)]

OS padrões 10 Base2, 10Base5 e 10BaseT são originais, definidos pelo padrão 802.3 do *IEEE (Institute of Electrical and Eletronic Engineers)*. Cada um deles define a interface de conexão (*Attachment Unit Interface - AUI*).

A interface AUI entretanto não suportava transmissões a 100 Mbps devido às altas frequências envolvidas. O padrão 100BaseT *Ethernet* precisava de uma nova interface, e as especificações 802.31u vieram a definir um novo padrão, chamado *MII (Media Independent Interface)*, permitindo taxas de até 100 Mbps, 4 bits por vez. O padrão *Gigabit Ethernet* utiliza um outro padrão de interface, chamado de *GMII (Gigabit Media Independent Interface)*, 8 bits por vez

2.1.6 Proteção da rede – Firewall

A função básica de um *firewall* em um servidor é bloquear o acesso a portas que não estão em uso. Evitando assim a exposição de serviços vulneráveis, ou que não devem receber conexões por parte da internet. A idéia é que sejam especificadas quais portas devem permanecer abertas e o *firewall* feche as demais.

Embora *firewalls* dedicados sejam também bastante comuns e os preferidos em grandes redes, onde o investimento é justificável, podemos obter um nível de segurança similar simplesmente usando os recursos nativos do sistema *Linux*, configurando o *Iptables*. O *firewall* trabalha como um fiscal da alfândega, que analisa todos os pacotes que chegam, decidindo o que deve passar e o que deve ficar retido, através de um conjunto de regras definidas (MORIMOTO, 2011).

2.1.7 Protocolo TCP/IP

Todos os dados transmitidos através da internet são agrupados em pacotes TCP, que podem conter até 1460 *bytes* de dados. Além dos dados, cada pacote inclui 40 *bytes* adicionais, contendo o endereço IP de origem, endereço IP de destino, porta de origem, porta de destino, códigos de verificação, número de pacote, campo para inclusão de opções e assim por diante.

No total temos 20 *bytes* para os *headers* do protocolo TCP e mais 20 *bytes* para os *headers* do protocolo IP, totalizando 40 *bytes* de *headers* por pacote. Dessa forma, temos 1460 *bytes* de dados em um pacote de 1500 *bytes* e 536 *bytes* de dados em um pacote de 576 *bytes* figura 5.

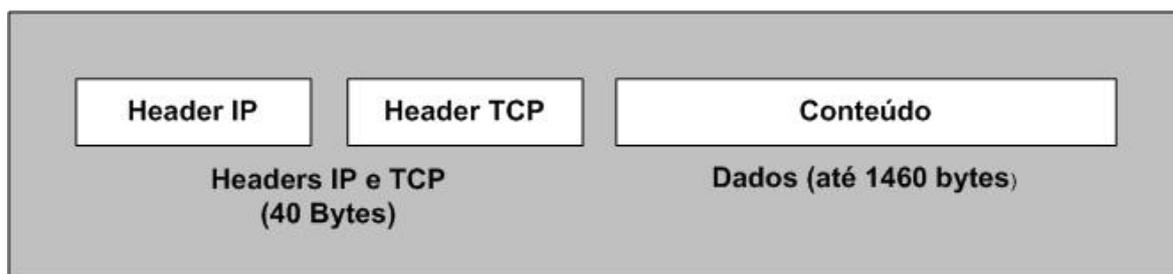


Figura 5 - Pacote TCP/IP

Pode parecer estranho que sejam incluídos *headers* separados para o TCP e o IP, mas a verdade é que os dois são complementares e por isso não podem ser dissociados. É por isso que usamos o termo “TCP/IP”, como se os dois protocolos fossem uma coisa só.

Os *headers* do protocolo IP incluem o endereço IP de origem e de destino, enquanto os *headers* do TCP incluem a porta de origem e de destino. Em resumo podemos dizer que o IP se encarrega do endereçamento e da entrega dos pacotes, enquanto o TCP se encarrega da verificação de erros, numeração de portas e outras funções (MORIMOTO, 2011).

Depois dos endereços IP, usados para endereçar os *hosts* na internet e nas redes locais, temos as portas TCP, usadas pelos diferentes serviços e programas que transmitem dados através da rede. Existem 65.536 portas TCP, numeradas de 0 a 65.535. Cada porta pode ser usada por um programa ou serviço diferente, de forma que em teoria poderíamos ter até 65.536 serviços diferentes ativos simultaneamente em um mesmo servidor, com um único IP válido.

As portas TCP mais usadas são as portas de 0 a 1023, que são reservadas para serviços mais conhecidos e utilizados, como servidores web, FTP, servidores de e-mail, compartilhamento de arquivos, etc.

Além do endereço IP, qualquer pacote que circula na internet precisa conter também a porta TCP a que se destina. É isso que faz com que um pacote chegue até o servidor web e não ao servidor FTP instalado na mesma máquina. Além das 65.536 portas TCP, temos o mesmo número de portas UDP. O UDP

oferece uma forma alternativa de envio de dados onde, em vez da confiabilidade, é privilegiada a velocidade e a simplicidade (MORIMOTO, 2011).

3 – Implementação da rede

3.1 Topologia utilizada

Cada topologia tem vantagens e desvantagens. Uma topologia em anel torna mais fácil aos computadores coordenarem o acesso e detectarem se a rede está operando corretamente. Porém, uma rede inteira em anel é desativada se um dos cabos é cortado. Uma topologia em estrela ajuda a proteger a rede de danos em um único cabo, já que cada cabo conecta somente uma máquina. Um barramento exige menos fios que uma estrela, mas tem a mesma desvantagem de um anel, uma rede é desativada se alguém acidentalmente corta o cabo principal (COMER, 2007).

A topologia de rede utilizada foi a árvore (topologia estrela com sub-redes), pois levou-se em conta a melhor relação de custo/benefício e segurança, Utilizando-se Switch de borda de maior capacidade e diversos switch de menor capacidade nas pontas, melhora-se a banda passante e divide-se o tráfego, assim se um determinado segmento da rede for danificado, não interfere-se no funcionamento dos demais segmentos.

Para a implementação da rede optou-se por conectar os blocos dos apartamentos através de cabo UTP categoria 5e, pois a tubulação era enterrada e protegida de intempéries, além da distância máxima entre blocos não ser maior que 80 metros. O ponto de conexão da rede mundial até o roteador Mikrotik

optou-se por fibra ótica tendo em vista a grande estabilidade de sinal, isenção de interferência de qualquer natureza e velocidades de até 10 Gbps.

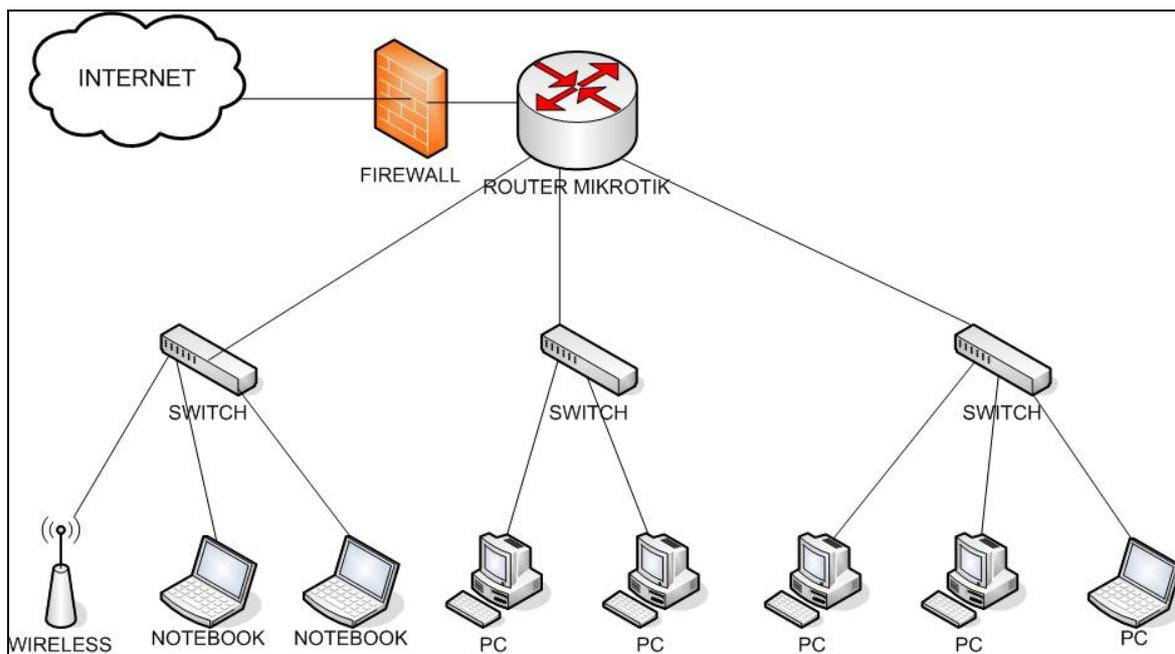


Figura 6 - Rede computadores em condomínio compartilhando a internet.

3.2 Ativos da rede utilizados

Os equipamentos utilizados na implementação foram:

- Roteador / Firewall marca Mikrotik
- Switches marca HP
- Computadores, notebook e roteadores wireless no cliente

3.3 Configuração dos equipamentos

Existem duas maneiras de se utilizar o software da Mikrotik, a primeira é instalar num servidor através de uma imagem em um cd do sistema operacional e a outra é utilizando hardware fabricado pela Mikrotik que já vem instalado com o sistema operacional Linux.

3.4 Instalação Mikrotik

Inserindo o cd no servidor e dando o boot aparecerão as opções de instalação. Pode-se selecionar os pacotes desejados pressionando-se a barra de espaço ou “a” para todos. Em seguida “i” irá instalar os pacotes selecionados.

```

Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

[X] system          [X] led             [X] synchronous
[X] ppp             [X] ntp            [X] telephony
[X] dhcp            [X] radiolan       [X] ups
[X] advanced-tools [X] routerboard    [X] user-manager
[X] arlan           [X] routing        [X] web-proxy
[X] gps             [X] routing-test   [X] uebproxy-test
[X] hotspot        [X] rstp-bridge-test [X] wireless
[X] isdn           [X] security       [X] wireless-legacy

system (depends on nothing):
Main package with basic services and drivers

Do you want to keep old configuration? [y/n]:
```

Figura 7- Instalação servidor Mikrotik

O hardware da Mikrotik exibe uma tela conforme a figura 8, onde a parametrização da configuração é feita numa interface gráfica Winbox que pode ser baixada no site da própria Mikrotik.

Interface gráfica para a administração do Mikrotik:

- Funciona em Windows e Linux
- Utiliza a porta TCP 8291
- Quase todas as funcionalidades do terminal podem ser configuradas via winbox.

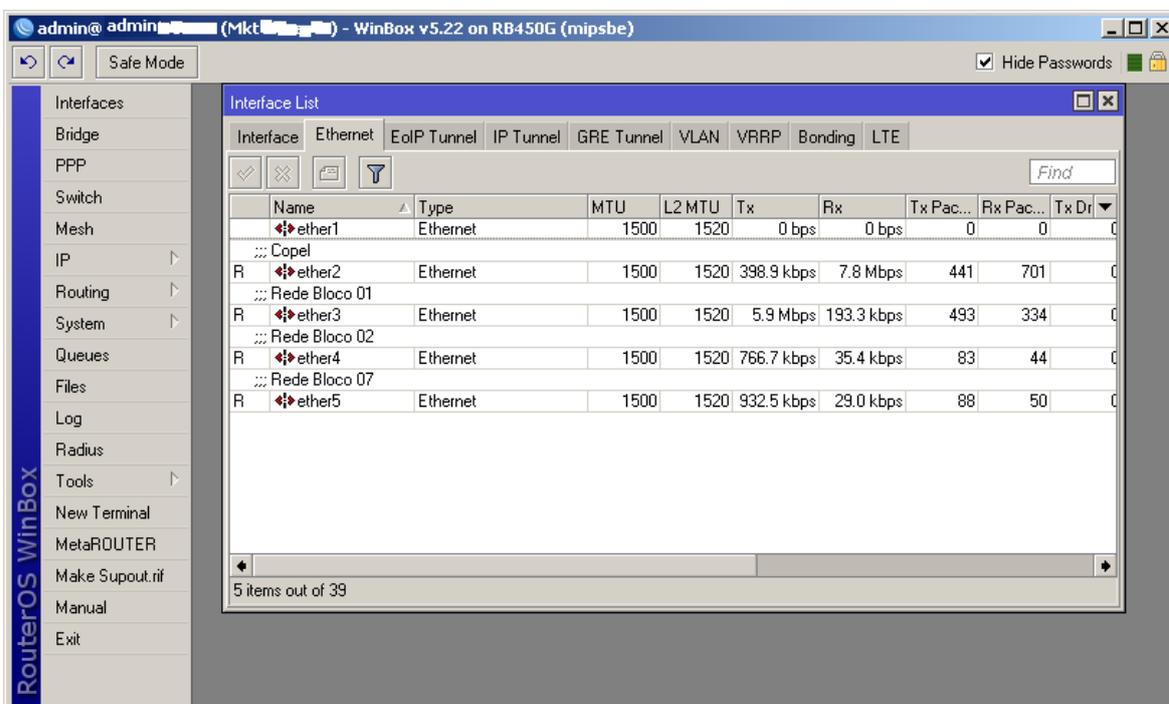


Figura 8 - Tela do Winbox Mikrotik

Em seguida selecione a aba IP, clique na aba Pool e adicione o range de IP privado para a rede local.

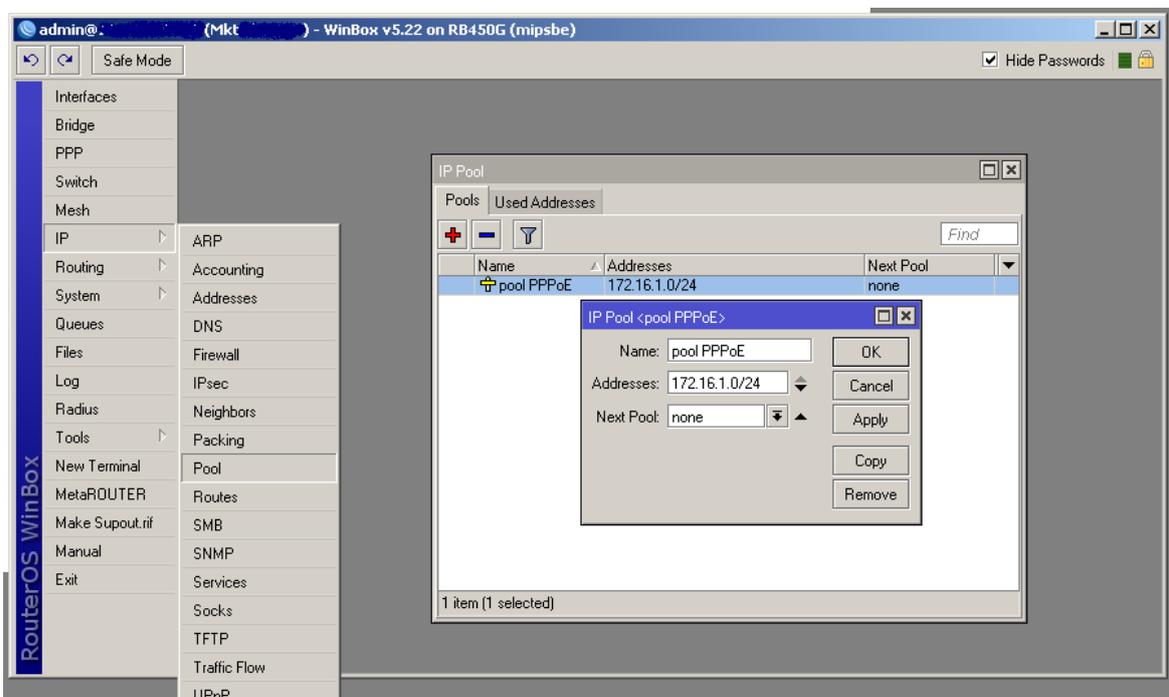


Figura 10 - Configuração endereço de rede LAN

3.5 Configurando Nat no Mikrotik

Após adicionar o IP público e o range de IP da rede local, é necessário configurar o NAT, para isso clique na aba IP, selecione a aba *firewall*, no menu suspenso clique em NAT. Em seguida adicione mais uma regra no ícone +, na janela que aparece clique em *Action* selecione na janela action src-nat. Após isso adicione o endereço da rede pública e Clique em OK, conforme figura 11.

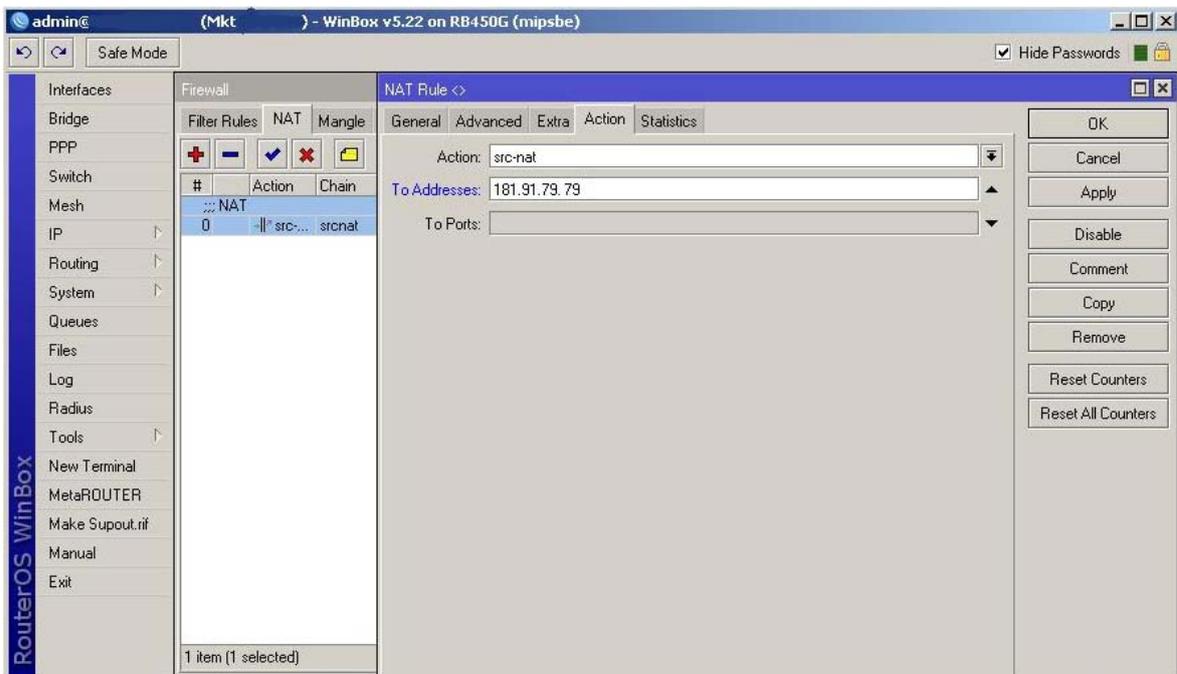


Figura 11 - Configurando NAT no Mikrotik

3.6 Configurando servidor PPPoE

PPPoE (point-to-point protocol over Ethernet) é uma adaptação do PPP para funcionar em redes Ethernet. Pelo fato da rede Ethernet não ser ponto a ponto, o cabeçalho PPPoE inclui informações sobre o remetente e destinatário, desperdiçando mais banda (~2% a mais).

Muito usado para autenticação de clientes com Base em Login e senha. O PPPoE estabelece a sessão e realiza a autenticação como provedor de acesso a Internet. O cliente não tem IP configurado, o qual é atribuído pelo PPPoE Server (concentrador), normalmente operando em conjunto com um servidor Radius. No Mikrotik não é obrigatório o uso de servidor Radius, pois o mesmo permite a criação e gerenciamento de usuários e senhas em uma tabela local (/pppsecrets). PPPoE, por padrão, não é criptografado

Crie um pool de IP's para o PPPoE na aba IP, clique em Pool, na janela que se abre clique no ícone “ + “, coloque o IP correspondente junto com a máscara de rede, conforme a figura 12.

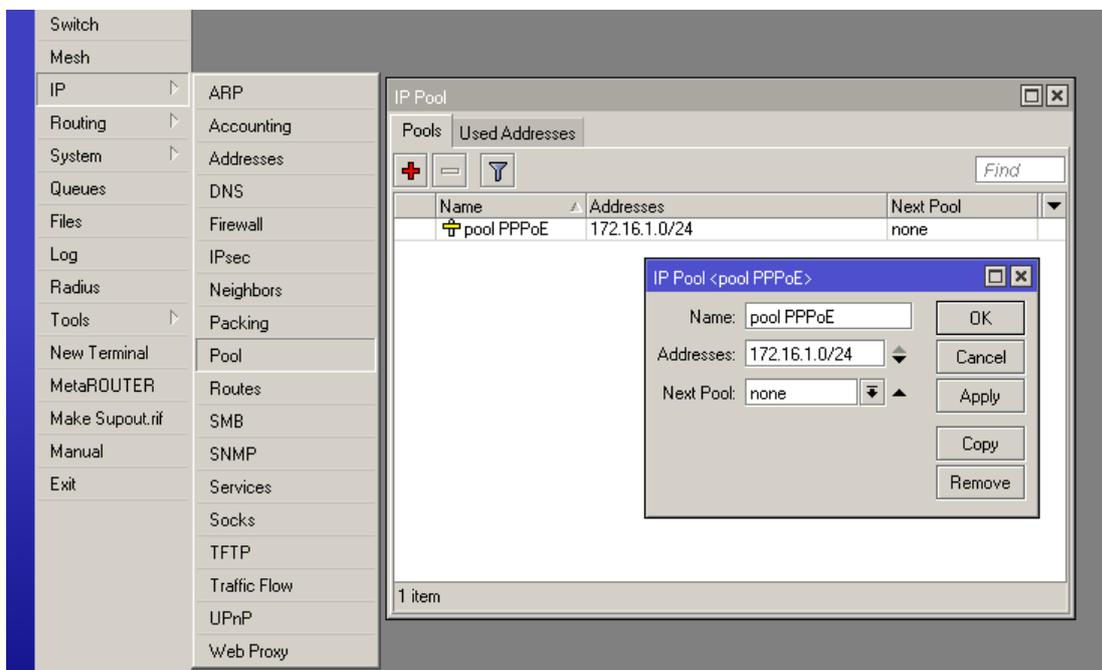


Figura 12 - Configurando o servidor PPPoE

3.7 Adicionando clientes PPPoE

Após a configuração do servidor PPOE, o próximo passo é adicionar clientes para que o usuários possam se conectar no servidor Mikrotik.

Selecione a aba PPP, na janela que se abre, clique no menu suspenso em Secrets, clique no ícone “ + “, informe o nome do cliente em Name, informe a senha em Password, selecione o protocolo PPPoE e clique em OK.

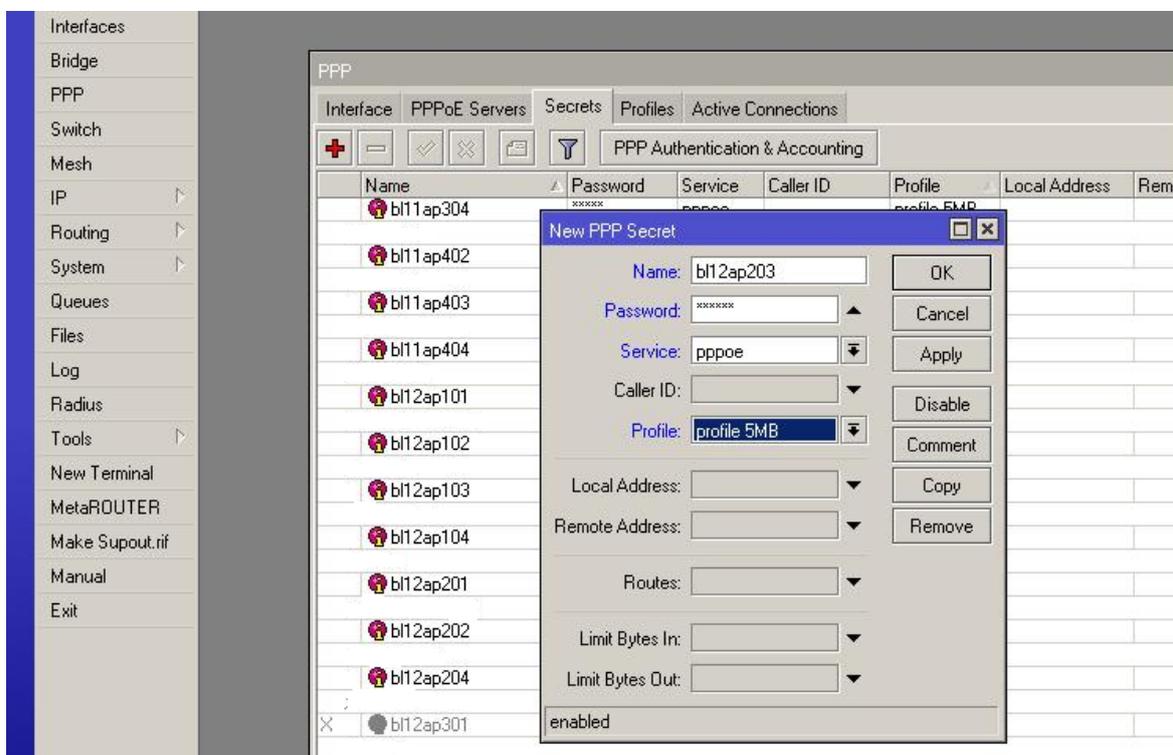


Figura 13 - Adicionando clientes PPPoE

3.8 Firewall no Mikrotik

O *Firewall* é normalmente usado como ferramenta de segurança para prevenir o acesso não autorizado à rede interna e ou acesso ao roteador em si, bloquear diversos tipos de ataques e controlar o fluxo de dados tanto de entrada como de saída.

Além de segurança, é no *Firewall* que serão desempenhadas diversas funções importantes como a classificação e marcação de pacotes para uso nas ferramentas de QoS.

A classificação do tráfego feita no Firewall pode ser baseada em vários classificadores como endereços MAC, endereços IP, tipos de endereços IP (*broadcast*, *multicast*, etc) portas de origem e de destino, range de portas, protocolos, Tipo do Serviço (ToS), tamanho do pacote, conteúdo do pacote, etc etc.

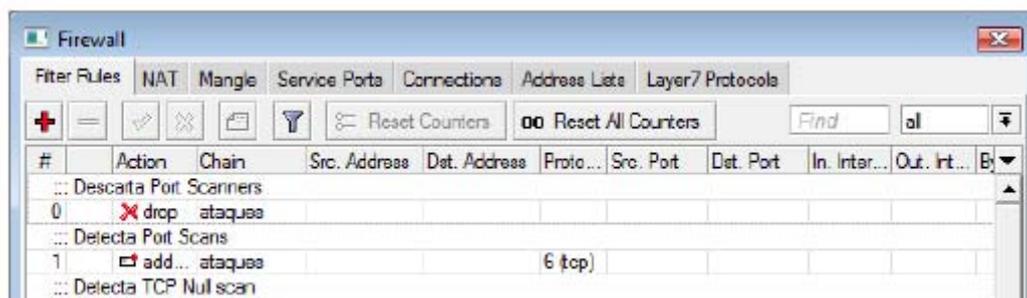


Figura 14 - Firewall Mikrotik

Filter Rules: é onde ficam as regras de filtros de pacotes.

NAT: onde é feito a tradução de endereços (mascaramento).

Mangle: onde é feita a marcação de pacotes, conexões e roteamento.

Connections: onde são visualizadas as conexões existentes

Address Lists: lista de endereços IP inserida manual ou dinamicamente que podem ser utilizados em várias partes do Firewall

Layer 7 Protocols: Filtros de camada 7 (Aplicação)

4 – Conclusão

Este trabalho teve o intuito de pesquisar, planejar e implementar a internet de banda larga em um condomínio residencial horizontal, utilizando-se tecnologia de rede ethernet estável, confiável e com tecnologias e equipamentos de última geração.

Procurou-se demonstrar também que o nível de segurança para o tráfego entrante é bastante confiável, tendo em vista a utilização de equipamento firewall de baixo custo, no caso o software e hardware da empresa Mikrotik, viabilizando a internet de banda larga a população de baixa renda, com preço acessível, estabilidade de conexão, e banda larga com velocidades de 5 a 10 Mbps.

Com o software Linux demonstrou-se que a utilização de software livre para controle de conexão à internet, torna-se viável levar a internet banda larga à população mais carente sem degradação de sinal nem limite de banda, contribuindo-se assim para a inclusão digital destes indivíduos.

Bibliografia

TANENBAUM, A. S.. **Redes de Computadores**. 4 Ed. Rio de Janeiro, Elsevier 2003.

COMER, DOUGLAS E.. **Redes de Computadores e Internet**. 4 Ed. Porto Alegre, Bookman, 2007.

FILIPPETTI, MARCO A.. **CCNA 4.1 Guia Completo de Estudo**. Florianópolis, Visual Books, 2008.

Wikipedia Mikrotik. Disponível 'em http://wiki.mikrotik.com/wiki/Main_Page

Acessado em 14/01/2013.

MORIMOTO, CARLOS E.. **Servidores Linux, Guia Prático**. Porto Alegre, Sul Editores, 2011.