SILVIO FERREIRA

REDES SEM FIO

O Livro de Bolso do Iniciante

INSTITUTO ALPHA

Editores: Silvio Ferreira e Josiane Gonçalves
Editoração Eletrônica: Instituto Alpha Educação à distância e Editora
Capa: Instituto Alpha Educação à distância e Editora
Produção: Instituto Alpha Educação à distância e Editora
Impressão e acabamento: Instituto Alpha Educação à distância e Editora

Co-Editora: Júlio Battisti – Livros e Cursos Ltda

Redes Sem Fio - O Livro de Bolso do Inicianete

Silvio Ferreira

ISBN: 978-85-66018-55-4

❖ Editora ❖

Instituto Alpha Educação à distância e Editora

Rua Divina Correia, 693, Bairro Cidade Nova I
Juatuba – MG
CEP: 35675-000
Tel: (31) 8486-4546
www.institutoalpha.net.br

❖ Co-Editora ❖

Júlio Battisti – Livros e Cursos Ltda

Rua Vereador Ivo Cláudio Weigel, 537 – Bairro Universitário
Santa Cruz do Sul-RS
CEP: 96816-200
Tel: (51) 3717-3796
www.juliobattisti.com.br

Agradecimentos

Primeiramente agradeço a Deus, pelo nascer de cada dia, pela força e motivação diária. Sem Ele não somos nada.

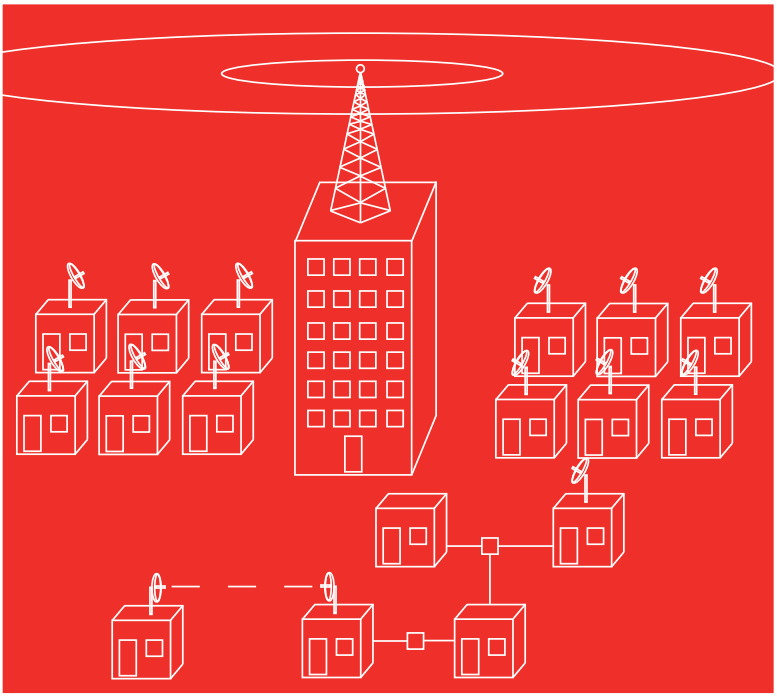
Agradeço a todos aqueles que direta ou indiretamente contribuíram com essa obra.

Agradeço a meu amigo Júlio Battisti, pela parceria de sempre.

Dedico esta obra a minha esposa e sócia no trabalho e na vida, Josiane Gonçalves e a meus filhos André e Geovane.

Sumário

❖



Capítulo 01 - Vamos Começar Nossa Jornada

PRIMEIRAS PALAVRAS

Primeiramente quero parabenizá-lo por ter decidido iniciar seus estudos em redes sem fio. Esse livro foi escrito para você que está começando agora, do zero absoluto. Se você já entende sobre redes sem fio, esse livro não foi feito para você. Esse livro foi feito para quem vai dar os primeiros passos. E eu, Silvio Ferreira, serei o seu tutor nessa incrível jornada.

Redes sem fio é algo empolgante. Você tem muito à aprender mesmo depois de ler este livro. Sugiro enfaticamente que acompanhe meus novos livros: há muitas novidades para serem lançadas, inclusive redes sem fio em nível avançado (ou seja, o seu segundo passo).

QUAL O OBJETIVO AQUI

O objetivo é que você aprenda certo e direito. Para ter sucesso em uma empreitada devemos começar corretamente. Ensinar é uma tarefa de muita responsabilidade. Eu considero que todos os meus livros são cursos/treinamentos. E cada livro que eu escrevo é carregado de responsabilidade e preocupação com cada leitor/estudante/aluno.

Por isso, existe didática aplicada aqui. Eu não estou ensinando o que eu “acho” que o leitor/aluno vai querer aprender. Eu estou ensinando o que o leitor precisa aprender para obter sucesso na sua jornada.

DEFINIÇÃO DE REDES SEM FIO / O BÁSICO A SABER

A palavra Wireless significa redes sem fio (wire: fio, cabo; less: sem). Se haver a comunicação de pelo menos dois dispositivos (que em redes são chamados pelo termo técnico nós), sem o intermédio de fios e cabos, há uma comunicação sem fio, ou seja, uma rede sem fio.

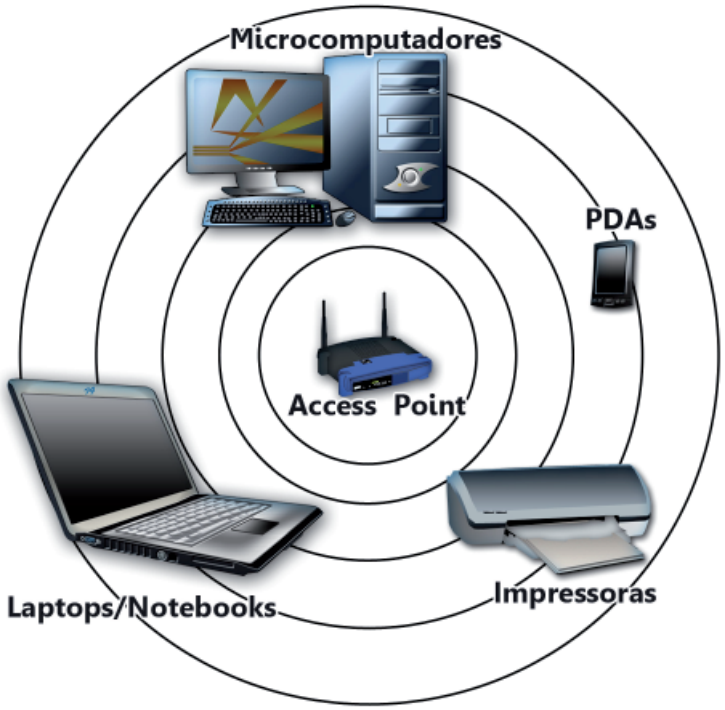


Figura 01.1: exemplo de uma rede sem fio (com AP). Observe que nessa imagem já se é possível observar que vários equipamentos podem usufruir da comunicação sem fio, como o microcomputador, PDAs (dentre outros portáteis semelhantes), notebooks e laptops, impressoras, dentre outros. Todos, nesse exemplo, são ligados um dispositivo central: o Access Point (AP).

Se haver, por exemplo, um notebook trocando informações com um microcomputador via bluetooth, já haverá ali uma rede, embora muito pequena. Perceba, que o exemplo dado é de uma rede mínima, onde um notebook troca informações com um microcomputador. Redes como essa são chamadas de WPAN (Wireless Personal Area Network), que são redes pessoais.

E se a rede for maior, contendo uma ou algumas salas interligadas? Aí elas passam a serem chamadas de WLAN (Wireless Local Area Network), que são as redes locais sem fio. As famosas lan house (que utilizam comunicação sem fio) são bons exemplos de uma de WLAN.

Acima dessa, chegamos às WMAN (Wireless Metropolitan Area Network), que são a redes metropolitanas. Metropolitana nos remete à metrópole, ou seja, cidade (muito embora o significado, em sua essência, seja um pouco mais do que isso). Isso quer dizer que uma WMAN é uma rede sem fio espalhada em uma cidade. Basta imaginar vários prédios interligados, ou ainda, uma empresa que ofereça acesso a Internet (Internet via a rádio) utilizando comunicação sem fio.

Por fim, depois das WMAN vêem as gigantes WWAN (Wireless Wide Area Network), que são as redes geograficamente distribuídas e, como se é de imaginar, pode interligar países e continentes (além de cidades, claro). O maior exemplo de todos você provavelmente usa todos os dias: a Internet.

BLUETOOTH, WI-FI E WIMAX

Todos esses termos esdrúxulos designam redes que utilizam comunicação sem fio graças ao uso de ondas de rádio.

O primeiro, Bluetooth, nada mais são do que as redes pessoais (ou sejam, essa tecnologia é usada nessas redes). Possui alcance pequeno, no geral (e na prática), os dispositivos envolvidos não ficam mais do que dois metros de distância uns dos outros. Atualmente é muito utilizada para a interligação de notebooks, celulares, impressoras, entre vários outros exemplos que podíamos citar aqui, a um microcomputrador.

Wi-Fi é a tecnologia empregada nas redes locais sem fio, que é o escopo dessa obra. Possui um alcance maior, e no geral um dispositivo pode ficar até um 100 metros de distância do nó central (AP – Access Point), muito embora diversos fatores contribuem para que essa distância seja maior ou menor.

Por fim, um termo em ascensão é WiMax. Essa é uma tecnologia de comunicação sem fio em alta velocidade e que permite a interligação de

nós em longas distâncias (algo nas casas dos kilômetros). Desse modo, redes WiMax podem ser empregadas nas WMAN.

O QUE É NECESSÁRIO PARA A MONTAGEM DE UMA WLAN/PADRÕES IEEE 802.11

Existem vários hardwares que podem ser usados na montagem de uma rede wireless. Mas, nesta publicação, há explicações de que montar dois tipos de redes:

- **Sem AP:** é uma rede wireless “placa-a-placa”;
- **Com AP:** que irá centralizar o sinal de rádio.

Desse modo, para acompanhar os exercícios, você precisará de:

- **Placa de rede wireless do padrão PCI:** é necessário uma para cada microcomputador envolvido. O padrão escolhido foi o IEEE 802.11g, que alcança uma taxa de 54Mbits/s na freqüência de 2,4GHz. Você deve estar se perguntando: existem outros padrões? Sim. São eles: IEEE 802.11a (54Mbits/s; 5GHz) e IEEE 802.11b (11Mbits/s; 2,4GHz);

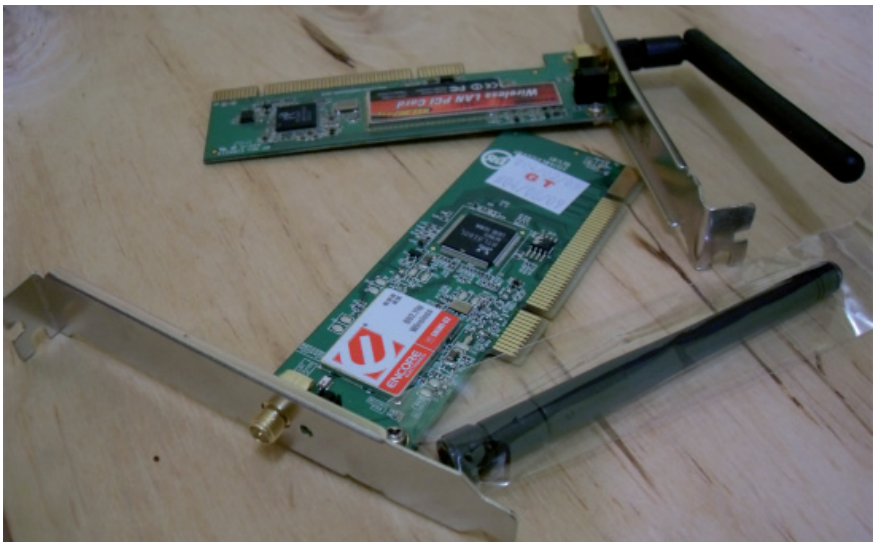


Figura 01.2: placa de rede wireless (PCI).

Observe na figura anterior que cada placa possui uma pequena antena dobrável. Ela pode possuir um formato diferente, tal como um dispositivo que é ligado e um fio de mais um menos um metro, o que permite posicioná-lo melhor, objetivando pegar um melhor sinal.

- **AP (Acess Point):** também seguem o padrão IEEE 802.11, dessa forma, você irá encontrar AP nos padrões IEEE 802.11a, IEEE 802.11b e IEEE 802.11g. Para evitar maiores problemas, adquira um do mesmo padrão das placas, que também devem ser do mesmo padrão. Isso é uma garantia a mais de conseguir montar a rede do início ao fim sem maiores dificuldades. É imprescindível se fazer constar que existem vários modelos de AP com funções “extras”, tais como switch e até roteador.

Figura 01.3: AP usado nessa publicação. Modelo Zplus G220 da Zinwell. **Você pode usar qualquer outro AP**, uma vez que as configurações primordiais (tais como IP, sub-máscara, SSID, Band, entre outras abordadas no decorrer do livro) estão presentes em todos.

O QUE É IEEE?

Esse IEEE que citei é uma organização sem fins lucrativos fundada nos Estados Unidos e que se dedica ao avanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação. A IEEE ajuda a desenvolver novas carreiras, financiar atividades, estabelecer normas e boas práticas, e por aí vai. E já estava me esquecendo, IEEE significa Institute Of Eletrical And Eletronic Enginers – Que significa Instituto

de Engenheiros Eletricistas e Eletrônicos.

Se você não tiver ouvido falar em normas IEEE, com certeza absoluta irá ouvir algum dia. As normas IEEE abrangem os campos da energia, biomedicina, saúde, tecnologia da informação, telecomunicações, transportes, nanotecnologia, segurança da informação e muito mais.

QUAL AP VOU USAR?

Vou repetir o que acabei de dizer. Para esse curso básico você pode utilizar qualquer Access Point básico. E sugiro que você compre um modelo realmente básico, para fins de estudo e análise.

Não pretendo indicar nenhuma marca e modelo. Neste livro estou usando o Zplus G220 da Zinwell por se tratar de um modelo extremamente didático e que possui uma vasta gama de configurações. Configurações essas que irão cobrir qualquer modelo básico que você adquirir. Por exemplo: a configuração de modos de operação, banda, canais, entre tantas outras, será igual em qualquer AP (é o mesmo conceito). Você irá apenas aprender o conceito e terá condições e conhecimento de pôr em prática.

Obviamente esse curso não é feito para configurar um Mikrotik por exemplo. Mas, você irá se dar bem na configuração de APs tais como TP-Link, D-Link, IntelBras, etc.

Aprenda os conceitos que vou te ensinar. Ok? E tente por em prática na "vida real". Esse é o caminho.

ENTENDA O AP

Ao comprar o Access Point, observe atentamente o seu painel frontal e traseiro. No frontal há, geralmente, alguns LEDs que indicam a atividade/funcionamento tais como LAN (fica acesso quanto estiver ligado em algum equipamento e pisca quando ocorrer atividade.), Tx/Rx (indica que é há, naquele momento, tráfego de dados na rede wireless, ou seja, está ocorrendo o envio e/ou recebimento de dados) e PWR (Power. Indica que o AP está ligado).

Dependendo do modelo haverá mais LEDs indicadores de atividade/ funcionamento. Um outro que não podemos deixar de mencionar é o LED que indica conexão com algum roteador de Internet banda larga (ou rede), indicado, geralmente, por WAN. Se o AP tiver a função de switch, poderá haver LEDs para cada porta RJ-45, indicados por LAN (eles ficam acesso quando tiver um dispositivo conectado na porta em questão).

Algumas dessas informações podem estar presentes na placa de rede wireless, e indica a mesma coisa. Geralmente a placa contém somente dois LEDs que é um que indica que a rede está funcionando (LINK) e o que indica atividade de envio e/ou recebimento de dados (Tx/Rx). Este último pode ser indicado por Activity.

No painel traseiro é onde está presente as portas RJ-45, entre outros itens. Vejamos os principais deles:

- **Conector para a fonte:** no geral um AP é alimentado por 5V (2A). Essa fonte é importante e é parte integrante do produto. Use somente a fonte apropriada, para evitar problemas tais como usar a fonte que fornece uma tensão maior do que a suportada pelo AP;

- **Porta WAN/LAN:** é onde interligamos um roteador, para conexão com a Internet banda larga ou outra rede. É uma porta RJ-45, no geral do padrão 10/100Mbits/s;

- **Porta LAN:** essa porta (RJ-45, no geral do padrão 10/100Mbits/s;) pode ser usada para interligar o AP em um micro servidor (ou qualquer outro micro) ou em um Hub/Switch, integrando rede cabeada à rede wireless. Inclusive, ao configurar o AP pela primeira vez, o mais usual é interligá-lo a um computador através dessa porta. Obviamente, o computador em questão deverá ter uma placa de rede comum (placa para rede cabeada) instalada e configurada corretamente;

- **Botão Reset:** esse é um botão bem pequeno (para pressioná-lo, na maioria das vezes, é necessário usar um objeto fino e alongado, como um palito de fósforos) e usado para apagar as configurações realizadas posteriormente no aparelho, retornando às configurações de fábricas. Deve-se ter cuidado ao optar em utilizá-lo, pois, ele apaga todas os

ajustes feitos, e a rede poderá não funcionar novamente até que ele seja reconfigurado. Mas é extremamente útil em diversos casos, como por exemplo a perda da senha de acesso ao “websetup”. Basta apagar suas informações e ele voltará ao estado tal como saiu de fábrica, com a senha e login padrão do fabricante (alguns modelos não pedem senha nos primeiros acessos, até que o usuário a configure);

- **Antena:** é o conector onde acopla-se a antena.

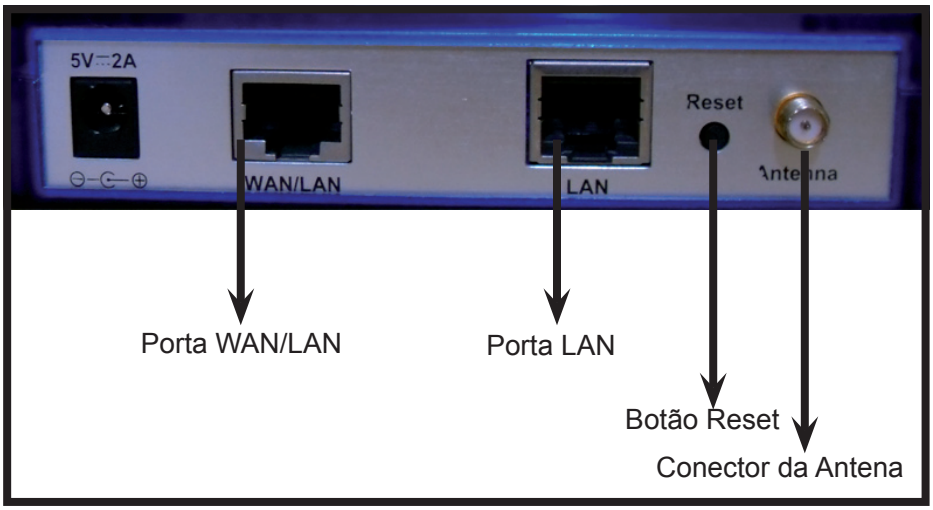


Figura 01.4: painel traseiro de um AP (Zplus G220 da Zinwell. Vale lembrar que esses itens possuem, basicamente, a mesma função em qualquer AP.

Quanto a instalação física do AP, escolha um bom local. Lembre-se: paredes, aquários, armários, entre outros, são obstáculos que vão fazendo com que o sinal wireless perca força. Alguns modelos são construídos para serem colocados sobre uma mesa (ou armário, por exemplo), enquanto outros podem também serem fixados em uma parede. Se os computadores da rede ficarem todos dentro de uma única sala, coloque-o em um local de tal forma que todos os micros o “enxerguem” sem muito problemas. Se os micros ficarem em duas salas, que ficam separadas por uma porta, uma

boa alternativa é colocá-lo nessa porta (no marco), bem na divisão entre as duas salas.

No geral, quando os computadores (e demais nós) envolvidos ficam próximos, o sinal ficará bom, mesmo com obstáculos tais como os citados. Esse sinal, ou seja, a "força" com que a placa de rede wireless está pegando esse sinal é medida pelo próprio sistema operacional, como está demonstrado mais à frente, neste livro, com o Windows XP e Vista.

INSTALAÇÃO E CONFIGURAÇÃO DAS PLACAS WIRELESS (PCI)

É fundamental deixar todos os micros preparados para ingressarem em uma rede sem fio. E isso é feito através da correta instalação e configuração das placas de redes wireless. Existem outros hardware que podem ser utilizados, como dispositivos USB ou cartões wireless (para notebooks). Mas, nesta publicação é usado como referencia as placas PCI.

O processo de instalação inicia-se em abrir o gabinete e "espetar" a placa em um slot PCI livre. Cuidado: faça isso com o microcomputador desligado. Aparafuse-a corretamente para que não fique solta. Feito isso, feche o gabinete e reinicie-o. Não se esqueça de colocar a antena na placa. Os próximos são no sistema operacional. Acompanhe a seguir um resumo da instalação no Windows 7.

Esse curso não é sobre hardware, montagem e configuração de microcomputadores. Mas vou te dar algumas instruções e informações à seguir para evitar erros.

Barramento PCI

Foram desenvolvidos quatro tamanhos de slots PCI, onde cada um varia em tensão de trabalho (V), bits e taxa de transferência. São eles:

- **Slot 32 bits (3,3V):** taxa de transferência máxima de 133MB/s;
- **Slot 32 bits (5V):** taxa de transferência máxima de 266MB/s;

- **Slot 64 bits (3,3V):** taxa de transferência máxima de 266MB/s;
- **Slot 64 bits (5V):** taxa de transferência máxima de 533MB/s.

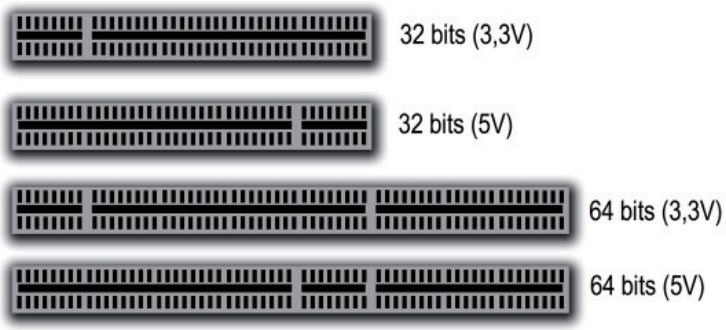


Figura 01.5: diferentes slots PCI.

Como foram criados slots diferentes, também foram criadas placas para cada um desses slots. Existem também placas PCI universais de 32 ou 64 bits. Uma placa universal de 32 bits pode se conectada em qualquer slot de 32 bits. Placas universais de 64 bits pode ser conectada em qualquer slot PCI de 64 bits.

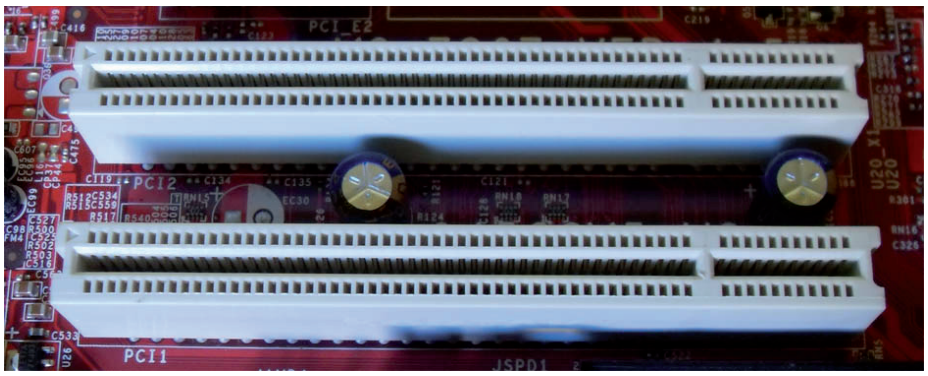


Figura 01.6: slots PCI em uma placa-mãe.

O barramento PCI possui suporte ao padrão Plug and Play (PnP). Qualquer hardware que possui suporte a esse padrão é reconhecido automaticamente ao iniciar o computador.

É por isso que ao instalar uma nova placa e reiniciar o computador, o sistema operacional já nos “avisa” que há um novo hardware detectado, e é informado inclusive a marca e modelo desse novo hardware. Isso se dá graças ao padrão Plug and Play.

Para que um hardware possa ser reconhecido automaticamente ao iniciar o computador, existe um cabeçalho de configuração, que são informações sobre o hardware em questão que ficam armazenados em um chip (no próprio hardware).

Atualmente, esse barramento é muito utilizado para a instalação de placas de rede cabeada ou sem fio, placa de áudio e de captura de TV e rádio AM/FM, entre vários outros exemplos. Um em futuro próximo ele pode ser substituído totalmente pela barramento PCI Express.

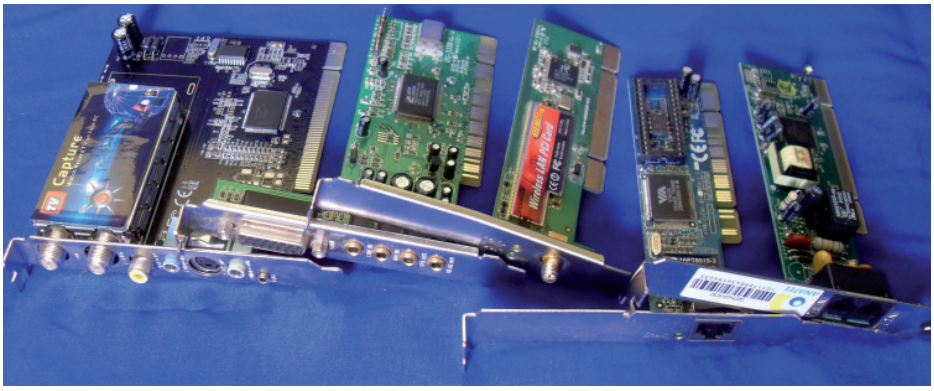


Figura 01.7: placas PCI diversas.

Configuração no Windows

Basicamente, com o microcomputador desligado, “espete” a placa no slot e reinicie o micro (feche o gabinete antes, se preferir). O novo hardware será detectado. Se o Windows tiver os drivers da placa, ela já é automaticamente instalada. As informações de novo hardware detectado e sua instalação, surgem na barra de ferramentas.

Eu usei como referencia o Windows 7 por se tratar de uma versão muito usada, mas muito usada mesmo (ainda em 2019).

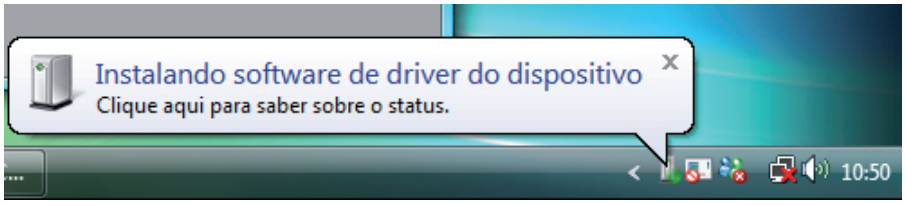


Figura 01.8: novo hardware detectado e sendo instalado. Observe que essas informações aparecem na barra de ferramentas.

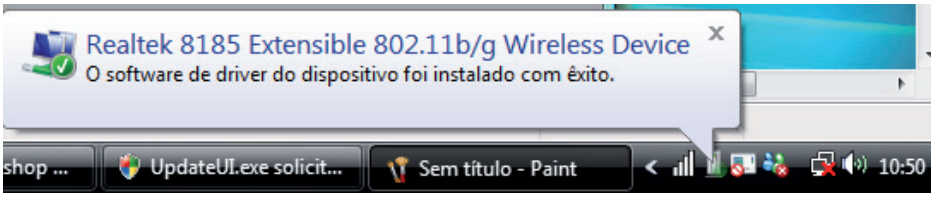


Figura 01.9: driver instalado. No nosso exemplo, o Windows 7 já tinha o driver, detectou e instalou tudo automaticamente!

Caso o Windows não tenha o driver, basta usar o CD da placa (ou o driver atualizado baixado do site do fabricante) e proceder com a instalação.

Quanto ao gerenciador de dispositivos: Para acessar, clique com o botão direito sobre o ícone Computador e clique em Propriedades normalmente.

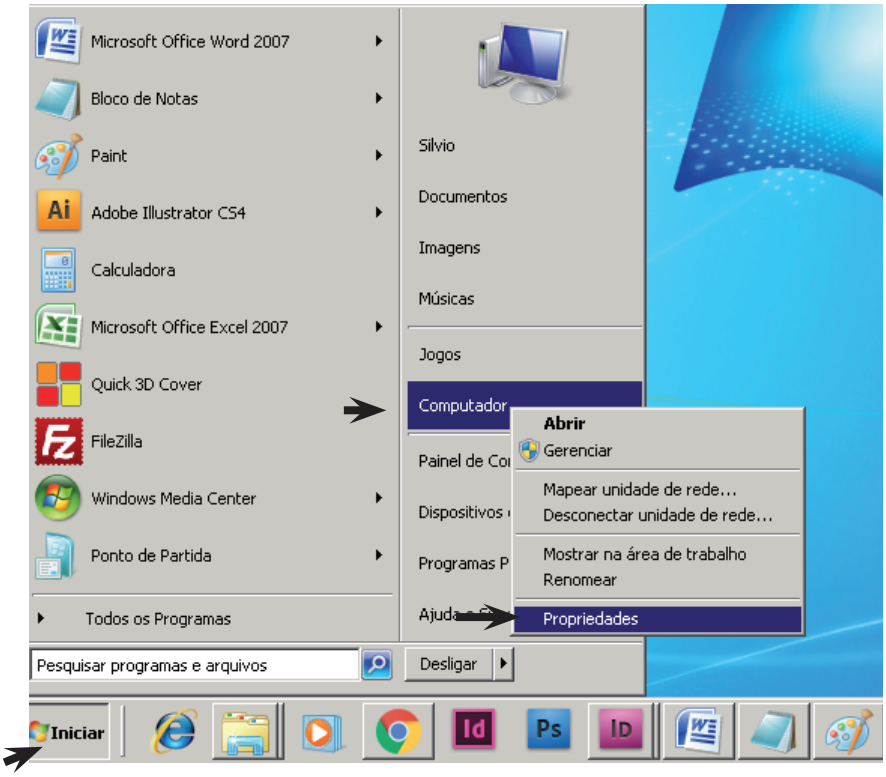


Figura 01.10: Iniciar – Computador. Clique com o botão direito em Computador e vá em Propriedades.

Irá abrir a janela Sistema, escrito “Exibir Informações básicas sobre o computador”. Na esquerda dessa janela, clique em Gerenciador de dispositivos. Pronto! Você já está no gerenciador de dispositivos.

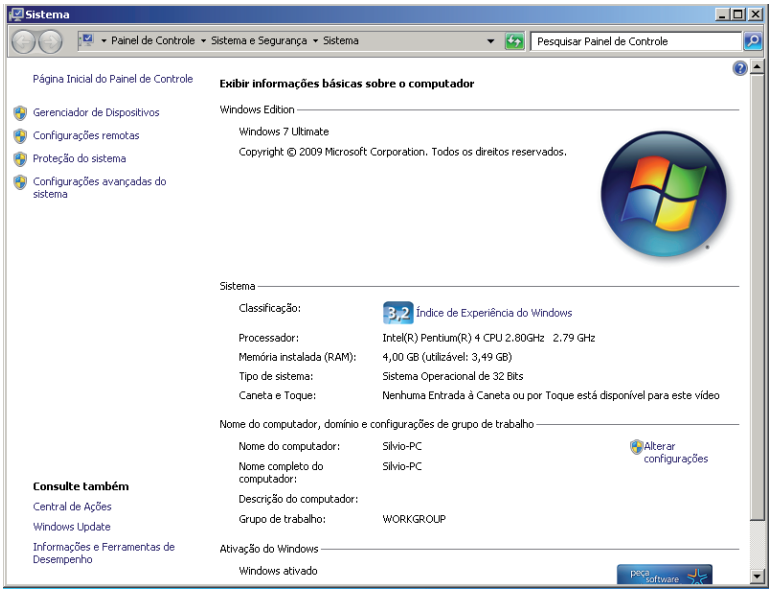


Figura 01.11: clique em Gerenciador de dispositivos.

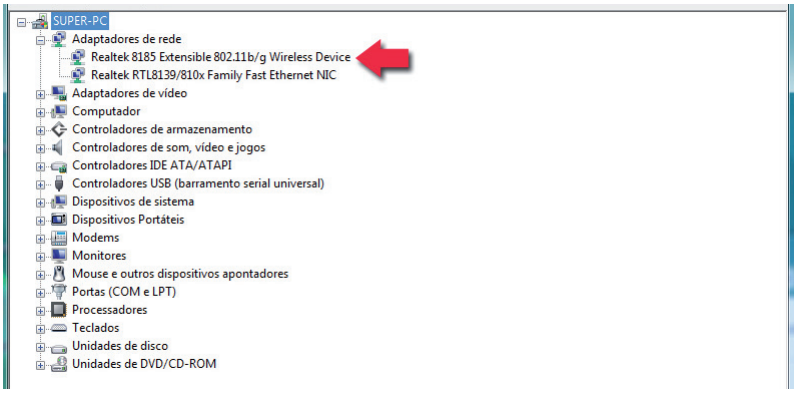


Figura 01.12: Gerenciador de dispositivos do Windows. Observe que a placa de rede wireless já se encontra instalada. Nesse exemplo, há duas Realtek instalada: 8185 (Wireless) e 8239 (placa para rede cabeada).

A placa de rede wireless fica listada no item Adaptadores de Rede. Se ela estiver descriminada com sua marca e modelo corretamente, e, caso não haja nenhum ponto de exclamação (amarelo) junto ao nome, significa que está tudo instalado corretamente;

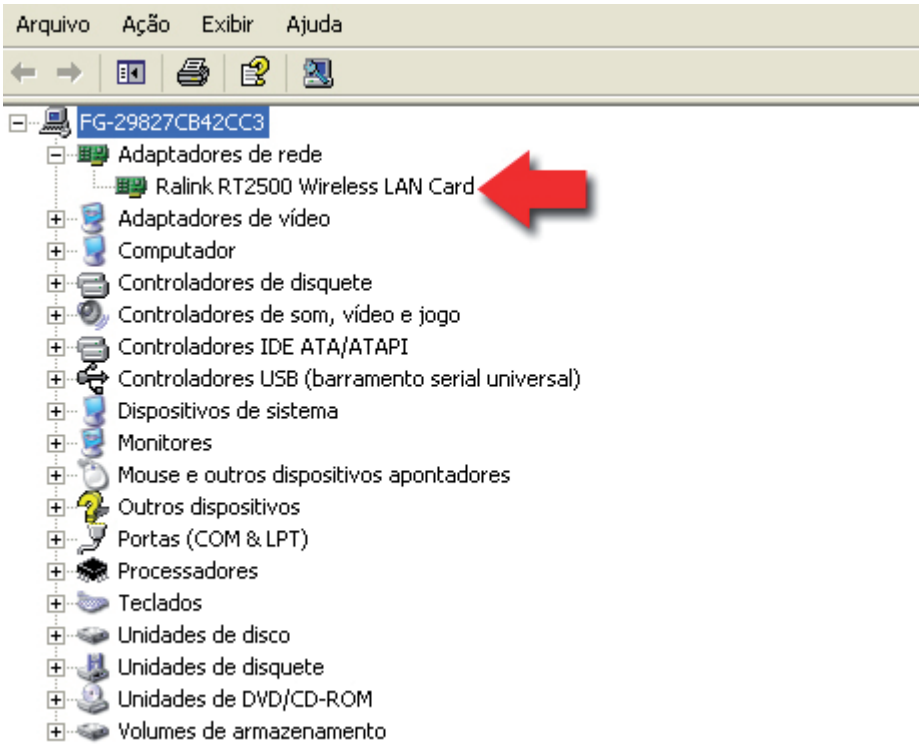


Figura 01.13: Gerenciador de dispositivos – Placa de rede Wireless Instalada corettamente.

Caso haja um ponto de exclamação, significa que há algum erro. Experimente apagar o driver (simplesmente clique uma vez sobre ele e pressione a tecla DEL. Confirme na seqüência.) e reiniciar o micro. Caso não dê certo, visite o site do fabricante e faça o download da versão mais recente do driver para o modelo de sua placa.

Uma vez a placa instalada corretamente, já haverá, no canto inferior direito da barra de ferramentas do Windows, o ícone que exibe as conexões de redes sem fio . Clique uma vez sobre ele e caso exista alguma rede sem fio ao alcance, ela será exibida. Caso não exista nenhuma rede sem fio ao alcance, não irá aparecer nenhum, pois, você ainda não configurou nenhuma rede. No próximo capítulo faremos isso.

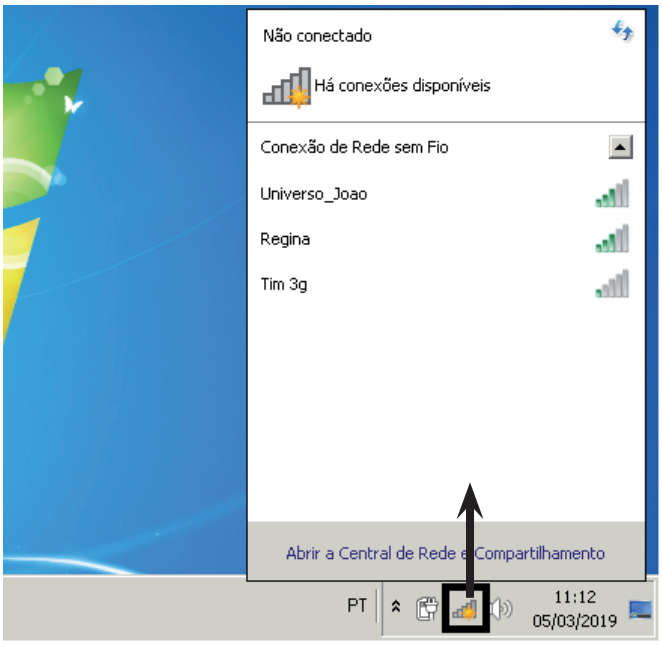


Figura 01.14: ao instalar a placa de rede em um micro, em nossos testes, ela já identificou redes sem fio por perto. Mas, é comum que nenhuma rede seja exibida, uma vez que você provavelmente ainda não configurou nenhuma.

A figura 01.14 na verdade está exibindo a opção Conectar a uma rede do Windows 7. Todas as opções de conexão são exibidas nessa janela. Você também pode abrir a janela Conectar a uma rede da seguinte forma:

1 – Clique em Iniciar;

2 - Na opção Pesquisar programas e arquivos digite: Conectar a uma rede;

3 - A opção Conectar a uma rede será exibida.

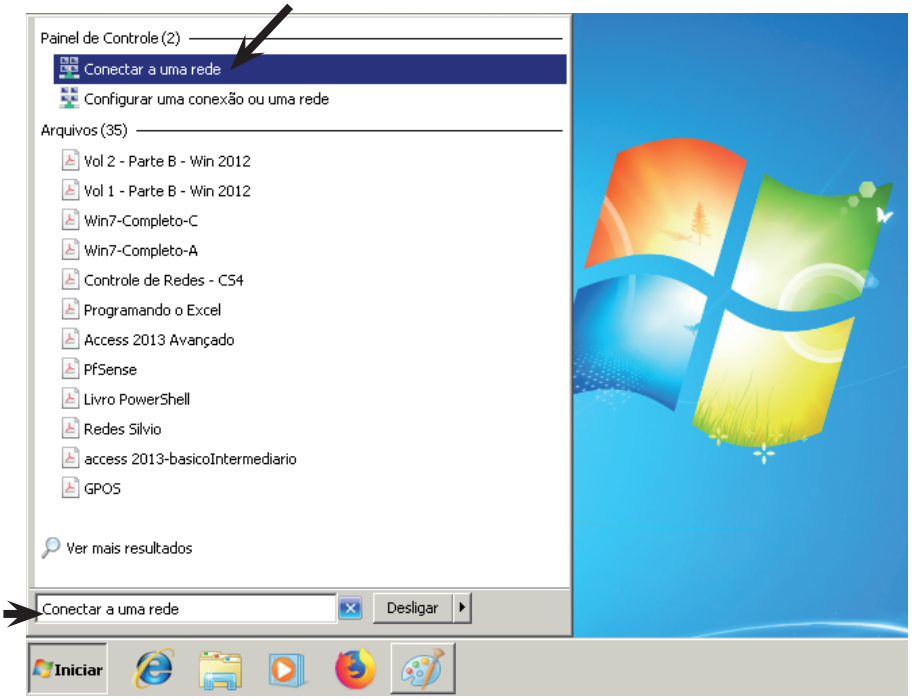
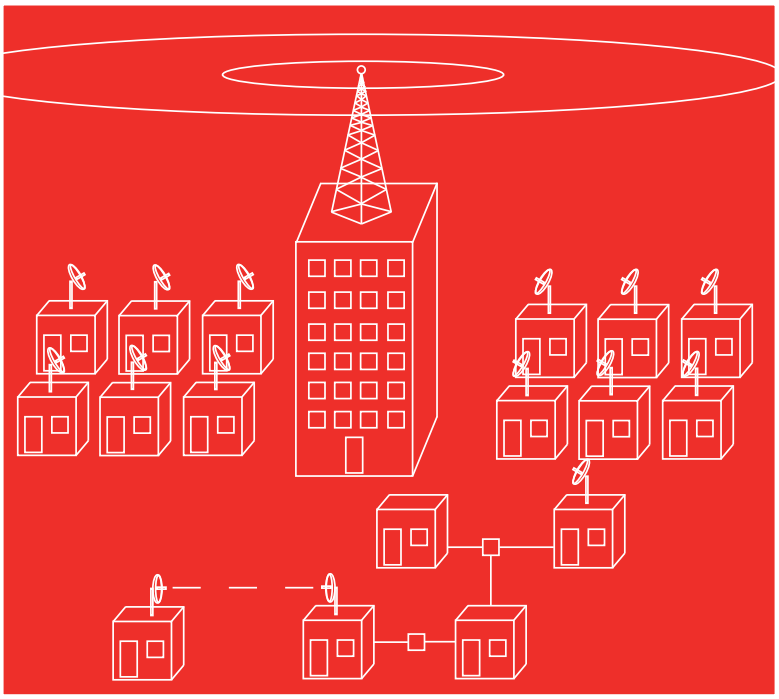


Figura 01.15: opção Conectar a uma rede



Capítulo 02 - Montagem de uma rede AD HOC

REDES AD HOC

Neste capítulo você aprenderá a configurar um tipo de rede em grande acessão no momento, que são as redes AD HOC. As redes wireless são sempre vistas, pelos iniciantes e pelos “não-entendidos”, com muito misticismo, como algo muito complicado de se lidar, cujos equipamentos (hardware) necessários são caros, que são muito vulneráveis, etc.

Em todas essas afirmações há verdades e mentiras. O quão complicado será montar uma rede wireless depende unicamente de seu tamanho e tipo. Ser for uma pequena rede, principalmente uma AD HOC, saiba que é mais fácil montá-la do que você imagina. Por outro lado, se for uma rede metropolitana (WMAN) para distribuição de Internet via à rádio em um cidade, você precisará se especializar mais no assunto. E no final das contas, se você tiver domínio dos assuntos, não será tão difícil quanto parece.

Quanto ao preços dos equipamentos, mais uma vez depende do projeto. Uma rede AD HOC necessita somente de uma placa wireless em cada micro envolvido. Sim, é isso mesmo que você acabou de ler. Então, uma rede dessas saí até mais barata do que uma rede cabeada. Se você uma rede maior, uma WMAN por exemplo, aí sim, é necessários equipamentos mais caros, como antes que devem ser instaladas em torres, repetidores, etc.

A questão da vulnerabilidade é o único assunto que existe muita verdade envolvida. Redes AD HOC são mais vulneráveis do que uma rede infra-estruturada (que utilizam AP), e se você deixá-la acessível sem uma proteção mínima, qualquer um que pegar seu sinal pode tentar se conectar e usar sua Internet de graça, por exemplo. Mas, no decorrer da leitura você verá como aplicar uma segurança mínima em sua rede.

Um outro assunto que não podemos deixar de fora, é quanto à velocidade com que dados podem ser transportados pela rede, ou seja, a taxa de transferência, que possui um limite de 11Mbits/s, não importando se você usar um padrão acima desse (como o IEEE 802.11g, que alcança uma taxa de 54Mbits/s em redes infra-estruturada).

MAS AFINAL, O QUE É UMA REDE AD HOC?

É comum, principalmente nos leigos no assunto, acharem que para montar uma rede WLAN, mesmo se ela for ter poucos computadores, é necessário adquirir um AP, instalá-lo em algum lugar do imóvel, instalar uma placa wireless em cada micro, configurar, etc. o que acaba encarecendo a construção da rede. Mas, há uma forma de se montar uma rede sem fio de forma fácil e bem mais econômica do que uma rede wireless infra-estruturada: as redes AD HOC.

Basicamente, uma rede AD HOC é aquela cuja comunicação entre os nós envolvidos não é intermediada por um Access Point. Todos os nós se comunicam diretamente entre si. Sua montagem é rápida e não requer uma infra-estrutura de rede previamente montada. Esses tipos de redes também são chamadas por IBSS (Independent Basic Service Set). Algumas publicações podem tratar dessas redes como “Rede de computador a computador”.

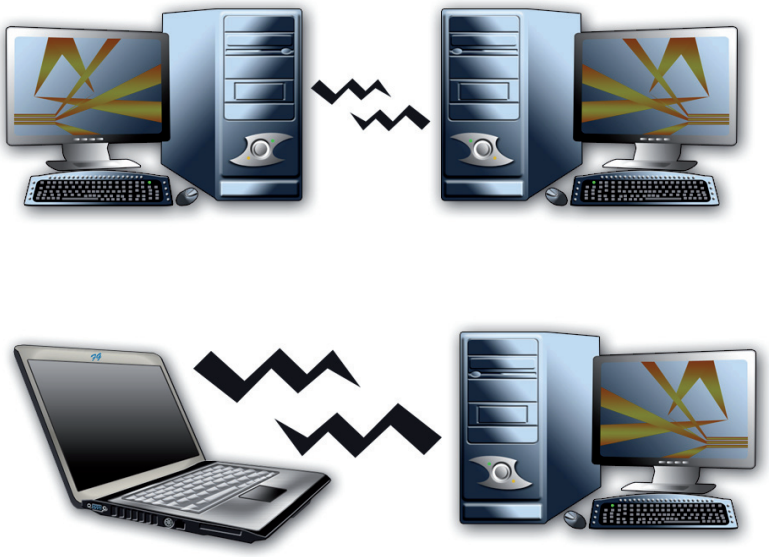


Figura 02.1: exemplo de uma rede AD HOC.

É comum algumas publicações traduzirem as redes AD HOC como “aquela que não utiliza cabos de redes”. Ora, uma rede wireless não utiliza cabos de redes, mesmo se ela tiver um AP centralizando e intermediando a comunicação entre os nós (você pode até conectar um cabo de rede no AP para configurá-lo, mas, ela continua sendo uma rede wireless. Depois da configuração o cabo de rede pode até ser desconectado). O que pode ocorrer é de uma rede wireless possuir um microcomputador que é interligado a um roteador (via cabo de rede) e que dá, a ele, acesso à Internet banda larga. Mas, se essa rede não possuir um AP centralizando o sinal, mesmo assim ela é uma rede AD HOC.

Por outro lado, se a rede wireless estiver ligada a uma rede cabeada (o AP ligado a um switch, só para citar como exemplo), aí é outro caso. Chamamos essa rede, como um todo, de rede mista. E, nada mais é do que duas redes (uma wireless e outra cabeada) se comunicando entre si, ou seja, elas estão interligadas.

VANTAGENS

As principais vantagens são o baixo custo e a facilidade em montar. Como já foi dito anteriormente, montar essas redes ficam bem mais baratas do que montar uma rede infra-estruturada.

São bem mais fáceis de montar também. Basta configurar o Windows corretamente e você já terá uma rede AD HOC funcionando. Imagine a seguinte situação: uma sala de aula onde alguns (ou todos) possuem notebooks com recurso de rede wireless. Nesse cenário, em questão de minutos uma rede AD HOC pode ser estabelecida e todos passam a trocar informações entre si. Esse tipo de rede pode ser estabelecida em qualquer local, em qualquer hora. Basta haver, pelo menos, dois computadores (ou dois notebooks, ou, um notebook e um computador) com suporte à rede sem fio. Nas linhas que se seguem, é demonstrado como configurar o Windows 7.

Existe ainda a vantagem da conectividade. A comunicação é direta. Se você colocar dois microcomputadores um ao lado do outro, a comunicação será realizado entre eles, com sinal perfeito. Já em uma rede infra-estruturada, mesmo se você colocar dois microcomputadores lado-a-lado,

a comunicação deverá passar primeiro pelo AP, e se ele estiver muito longe, o sinal wireless poderá ficar fraco.

São indicadas para pequenas redes, para compartilhar arquivos, dispositivos e Internet (mas, é preciso observar essa questão a seguir, em desvantagens).

DESVANTAGENS

Algumas das principais desvantagens é que os computadores envolvidos não podem ficar muito longe uns dos outros. Somente algo em torno de nove metros.

Outra desvantagem evidente é que o micro que tiver Internet compartilhada deve ficar sempre ligado, caso contrário, todos perdem a conexão com a Internet.

Por fim, um fato que já foi dito, é que essas redes são menos seguras. Em primeiro lugar, nunca deixe-a sem uma proteção mínima (de tal forma que qualquer um que captar seu sinal consiga se conectar). Configure-a de forma com que somente as pessoas que você permitir possa acessa-la. Mas, é importante ter em mente que a criptografia em redes AD HOC são mais fracas se comparadas à criptografia de roteadores, por exemplo. Em redes infra-estruturadas, quando o roteador é ligado ao AP para compartilhar banda larga na rede, a segurança é maior, devido ao fato desse dispositivo possuir firewall e criptografia com boa eficiência.

Devido a esses fatos, esse tipo de rede não é recomendado para ambientes empresariais, a não ser que não haja (nessa rede) nenhum tipo de dado sigiloso ou de grande importância, o que é muito pouco provável. Uma simples tabela com os dados pessoais dos funcionários já é um dado importante e sigiloso (nenhuma empresa sai por aí repassando os dados de seus funcionários). Além disso, ela não é recomendada para médias ou grandes redes, já que não existe uma administração tal como ocorre nas redes com AP.

CRIAÇÃO DA REDE NO WINDOWS

No Windows 7 podemos configurar a rede facilmente. Vejamos:

1 - Clique no menu Iniciar – Painel de Controle;

2 - Clique em Rede e Internet;

Figura 02.2: vá em Rede e Internet.

3 - Na sequencia clique em Central de Rede e Compartilhamento;

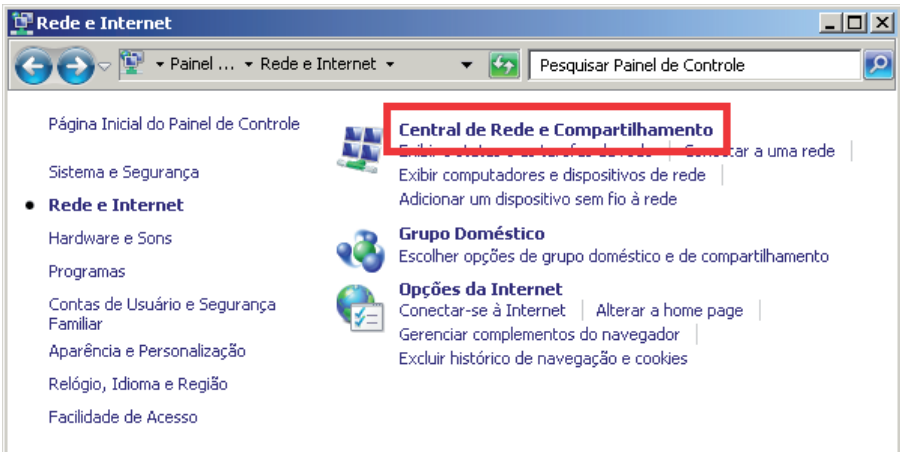


Figura 02.3: clique em Central de Rede e Compartilhamento.

4 - E finalmente, clique em Configurar uma nova conexão ou rede;

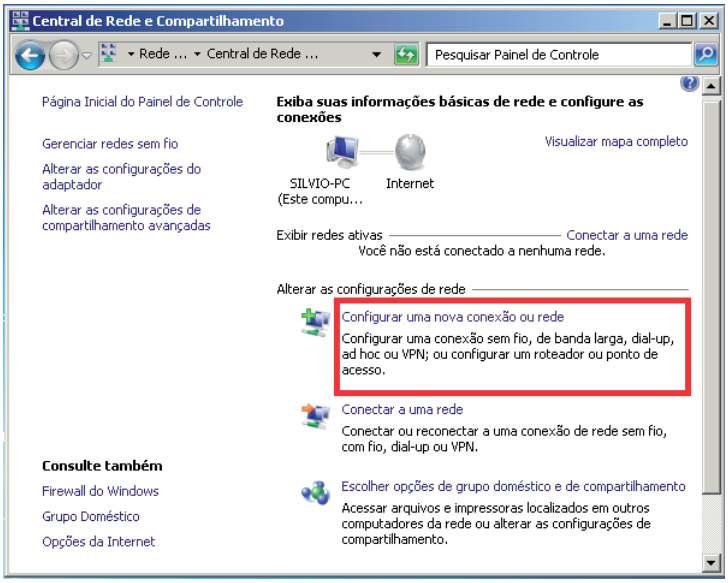


Figura 02.4: agora clique em Configurar uma nova conexão ou rede.

5 - Agora chegamos no ponto que nos interessa. Estaremos na janela Configurar uma nova conexão ou rede. A opção que usaremos é a Configurar rede ad hoc. Portanto, selecione-a (clique uma vez sobre essa opção) e clique em Avançar;

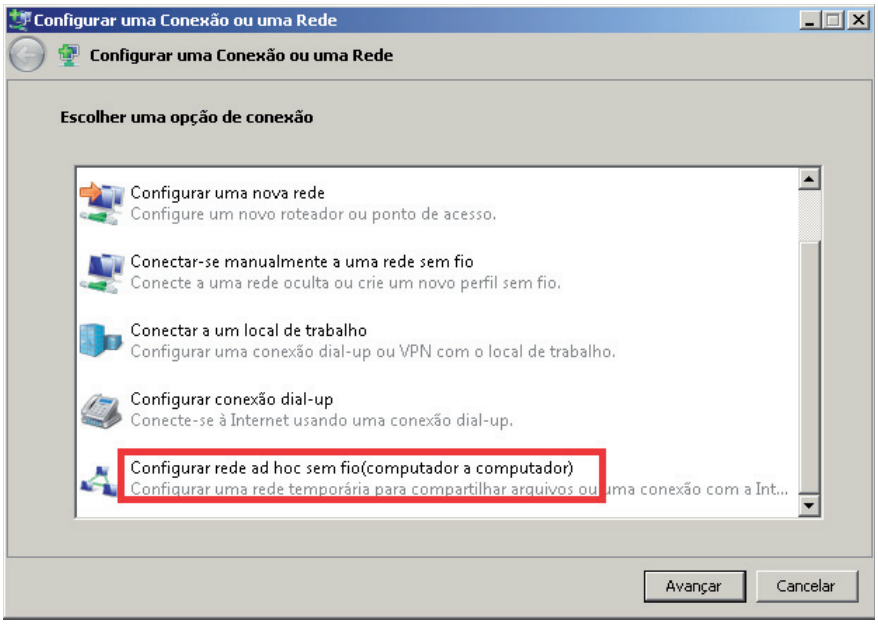


Figura 02.5: clique em Configurar rede ad hoc sem fio (computador a computador) e clique no botão Avançar.

6 - Irá abrir a janela Configurar rede ad hoc sem fio com explicações a respeito desse tipo de rede. Clique no botão Avançar;

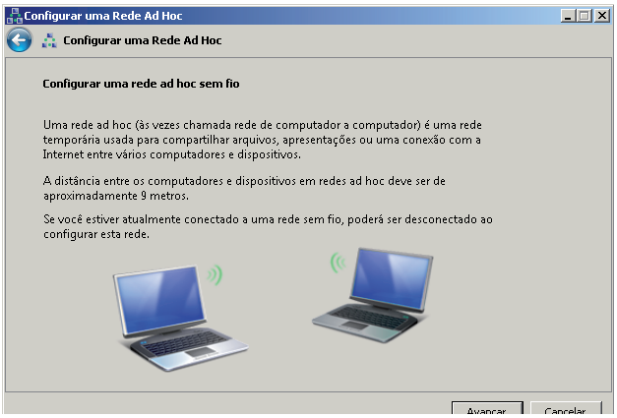


Figura 02.6: nesta tela você pode ler um pouco mais sobre as redes AD HOC. Para continuar, clique em avançar.

7 - Na próxima tela, é onde você deve fazer as configurações. No campo Nome da rede (SSID) é onde colocamos o nome que aparece quando algum micro detectá-la. SSID significa Service Set Identifier. É esse nome que identifica uma rede wireless de outra. Crie um nome preenchendo esse campo. Como exemplo, estamos criando a rede Universo1;

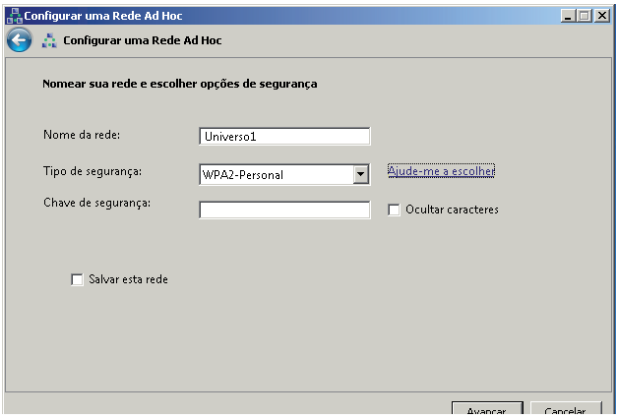
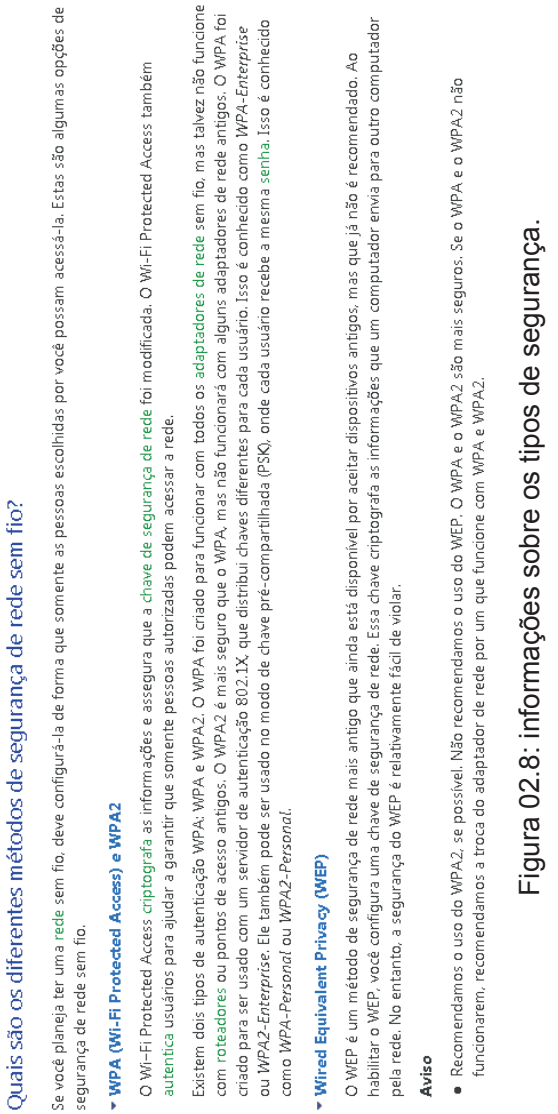


Figura 02.7: configurando uma rede ad hoc.

8 - Logo abaixo, em Tipo de Segurança escolha WPA2-Personal. Mais à frente neste livro irei abordar isso em mais detalhes. Mas, por hora, se tiver dúvidas clique em Ajude-me a escolher;



Quais são os diferentes métodos de segurança de rede sem fio?

Se você planeja ter uma rede sem fio, deve configurá-la de forma que somente as pessoas escolhidas por você possam acessá-la. Estas são algumas opções de segurança de rede sem fio.

WPA (Wi-Fi Protected Access) e WPA2

O Wi-Fi Protected Access criptografa as informações e assegura que a chave de segurança de rede foi modificada. O Wi-Fi Protected Access também autentica usuários para ajudar a garantir que somente pessoas autorizadas podem acessar a rede.

Existem dois tipos de autenticação WPA: WPA e WPA2. O WPA foi criado para funcionar com todos os adaptadores de rede sem fio, mas talvez não funcione com roteadores ou pontos de acesso antigos. O WPA2 é mais seguro que o WPA, mas não funcionará com alguns adaptadores de rede antigos. O WPA foi criado para ser usado com um servidor de autenticação 802.1X, que distribui chaves diferentes para cada usuário. Isso é conhecido como *WPA-Enterprise* ou *WPA2-Enterprise*. Ele também pode ser usado no modo de chave pré-compartilhada (PSK), onde cada usuário recebe a mesma senha. Isso é conhecido como *WPA-Personal* ou *WPA2-Personal*.

Wired Equivalent Privacy (WEP)

O WEP é um método de segurança de rede mais antigo que ainda está disponível por aceitar dispositivos antigos, mas que já não é recomendado. Ao habilitar o WEP, você configura uma chave de segurança de rede. Essa chave criptografa as informações que um computador envia para outro computador pela rede. No entanto, a segurança do WEP é relativamente fácil de violar.

Aviso

- Recomendamos o uso do WPA2, se possível. Não recomendamos o uso do WEP. O WPA e o WPA2 são mais seguros. Se o WPA e o WPA2 não funcionarem, recomendamos a troca do adaptador de rede por um que funcione com WPA e WPA2.

Figura 02.8: informações sobre os tipos de segurança.

9 - Agora devemos digitar a nossa chave de rede, que será solicitada a cada usuário que tentar se conectar na rede. Desse modo, digite-a em Chave de segurança.

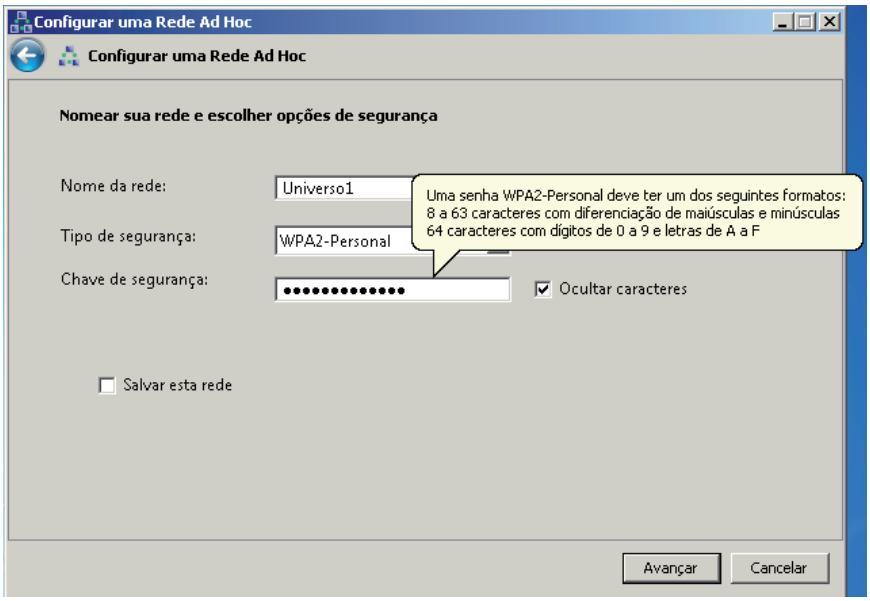


Figura 02.9: digite a Chave de segurança.

10 - Marque a opção Salvar esta rede caso deseje que ela fique salva mesmo depois de reiniciar o computador. Clique no botão Avançar;

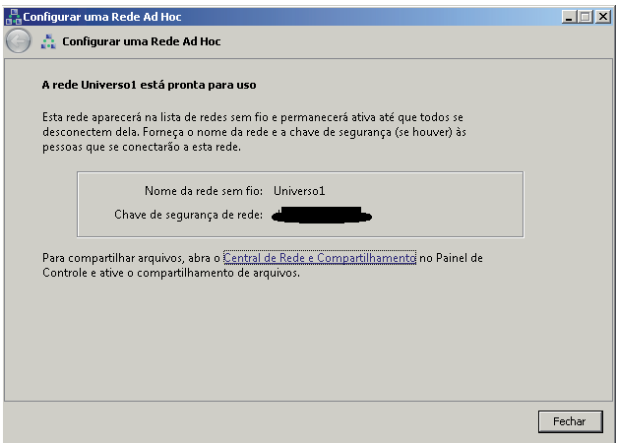


Figura 02.10: a rede será configurada e você verá esta janela. Clique em Fechar.

11 - Para verificar se a rede foi criada corretamente, vá à opção Conectar a uma rede: no canto inferior direito da barra de ferramentas do Windows, clique no ícone que exibe as conexões de redes sem fio. Você verá a rede com a informação “Aguardando usuários”.

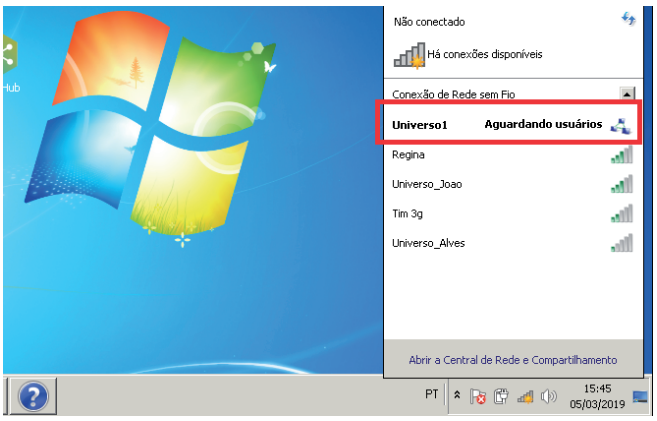


Figura 02.11: rede criada com sucesso!

INGRESSANDO COMPUTADORES NA REDE

Através dos textos anteriores você pode acompanhar que configurar uma rede AD HOC no Windows é muito fácil e rápido. Agora, vêem a parte ainda mais fácil e rápida, que é incluir (ingressar) um microcomputador ou notebook que possua recurso wireless na rede.

Para se conectar à rede a partir de um microconptador/notebook com Windows, faça o seguinte:

As instruções que vou te dar agora independem de versão do Windows. Por isso, vai ser instruções um pouco “genérica”.

1 - Vá à opção Conectar a uma rede: no canto inferior direito da barra de ferramentas do Windows, clique no ícone que exibe as conexões de redes sem fio;

2 - Na janela Conectar-se a uma rede, clique uma vez sobre a rede Wireless que deseja se conectar e clique no botão Conectar;

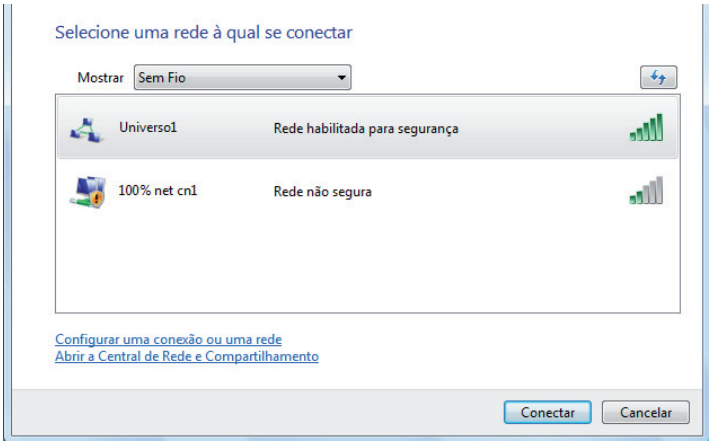


Figura 02.12: selecione a rede pretendida e clique no botão Conectar.

3 - Será solicitado a chave de segurança. Digite e clique no botão Conectar.

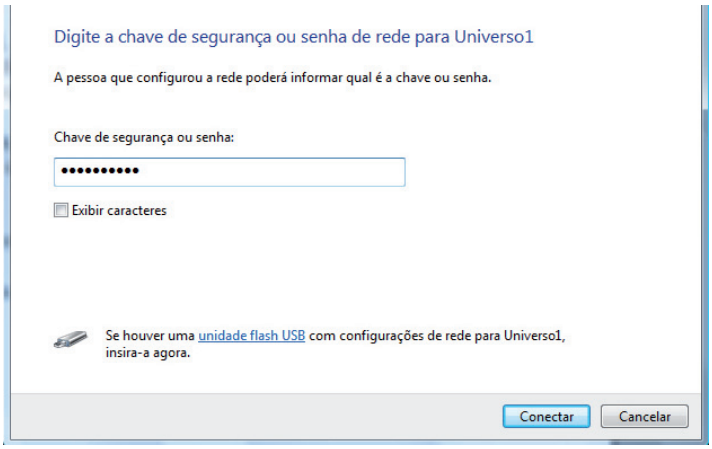


Figura 02.13: digite a chave de segurança e clique no botão Conectar.

Uma vez conectado, volte à opção Conectar a uma rede. Observe que na rede sem fio, agora, haverá a inscrição “Conectado”. Para ver o status, clique com o botão direito do mouse sobre a conexão de rede sem fio e clique em Status.

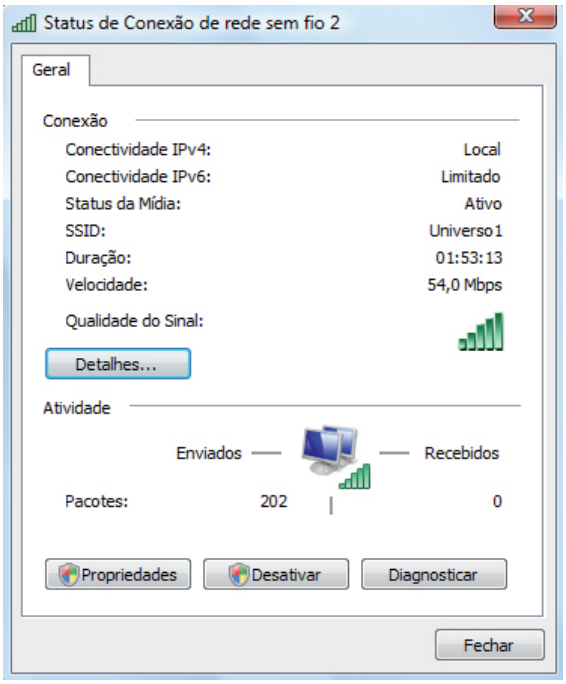


Figura 02.14: status da conexão de rede sem fio. Observe que há várias informações, tais como o nome da rede, duração, etc.

Na janela Status de Conexão de rede sem fio há informações tais como: o estado (status) atual (conectado ou desconectado), o nome da rede, a duração (o tempo em que está conectado), velocidade (taxa de transmissão de dados) máxima alcançada (11,0Mbits/s), a força do sinal e a atividade (quantidade de bits enviados e recebidos).

Para mais informações, clique no botão Detalhes. Agora, você terá acesso a várias informações, tais como IP, endereço físico, máscara de sub-rede, etc.

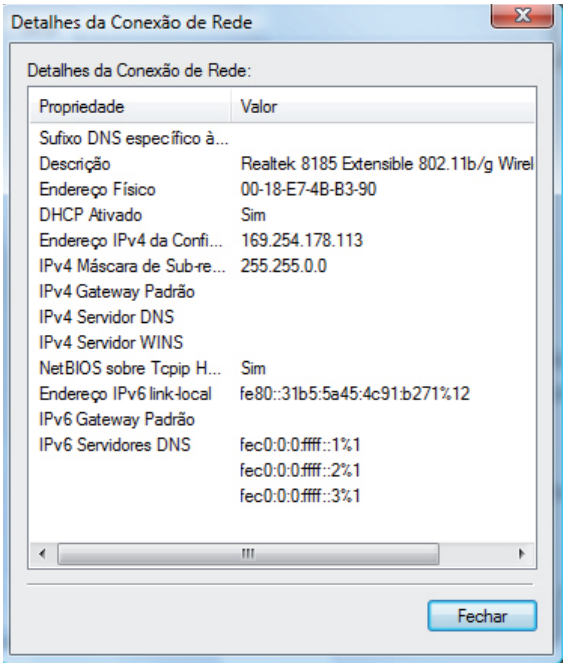


Figura 02.22: detalhes da conexão de rede sem fio.

TESTE DE CONECTIVIDADE DA REDE

Caso deseje, você pode realizar um teste de conectividade na rede, através do comando ping, que envia quatro pacotes de 32 bytes em direção ao micro destino. Para fazer isso, basta abrir o prompt de comando. Para isso, no Windows, clique no menu Iniciar – Todos os programas – Acessórios – Prompt de comando.

No prompt de comando, digite o comando ping + o IP do micro de destino (o qual deseja testar a conectividade). Exemplo:

Ping 169.254.178.113

Para descobrir o IP, basta clicar em detalhes, na janela status da conexão de rede sem fio. Isso já foi mencionando anteriormente.

No final do envio, será mostrado uma estatística contendo o número de pacotes enviados (que são quatro), os recebidos, perdidos, etc.

Caso seja acusado algum erro, como por exemplo, numero de pacotes recebidos igual a 0 (zero), verifique se o micro de destino possui algum firewall ativo (que pode impedir o acesso de outros micros via rede. Caso afirmativo, desative-o.

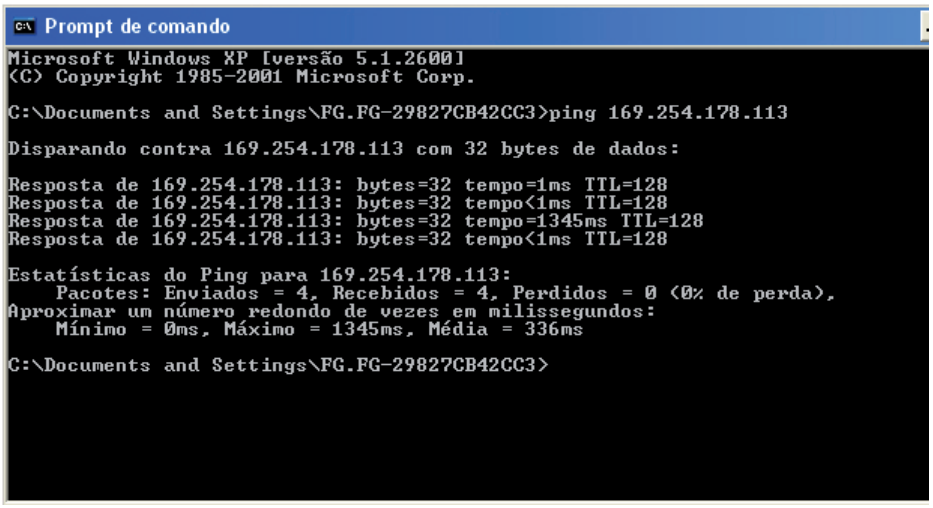


Figura 02.16: aqui, o teste de conectividade foi positivo. Observe que todos os pacotes enviados foram recebidos.

Como você pode perceber, o ping envia quatros pacotes de 32 bytes ao micro destino. Mas, você pode forçá-lo a enviar pacotes “infinitamente” até que as teclas CTRL + C sejam pressionadas para parar (ou as teclas CTRL + Break, que pausa, permitindo voltar ao teste se desejar). Para isso, use a seguinte sintaxe:

Ping ip destino -t

Exemplo:

Ping 169.254.178.113 -t

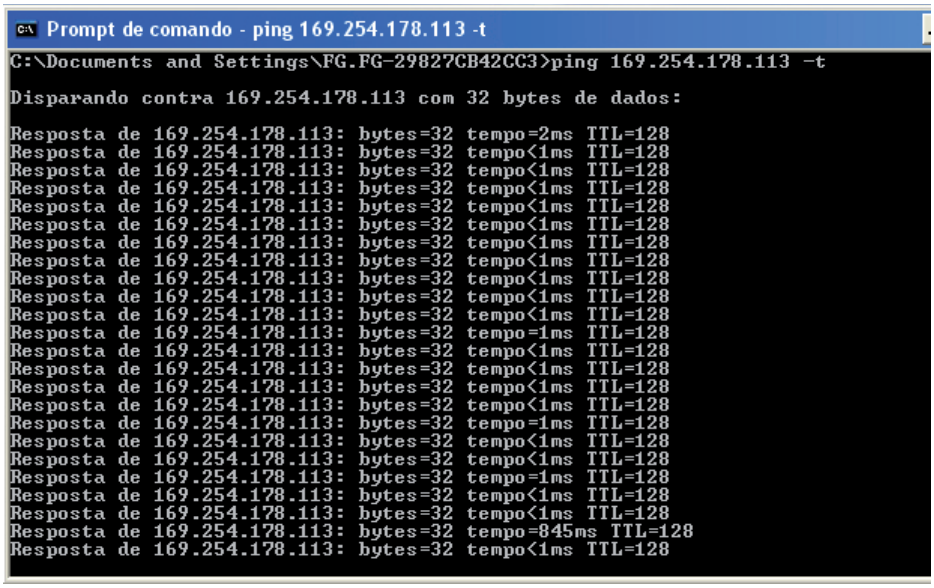


Figura 02.17: usando o ping -t.

COMO EXCLUIR A REDE

Se for necessário você pode excluir uma rede AD HOC criada. Isso pode ser necessário por vários motivos, mas, o principal deles é deixar a rede indisponível (de tal forma que ela não seja detectada por nenhum micro). Vejamos como fazer isso:

1 - Vá à opção Conectar a uma rede: no canto inferior direito da barra de ferramentas do Windows, clique no ícone que exibe as conexões de redes sem fio. Observe que em sua parte inferior há a opção Abrir a central de rede e compartilhamento. Clique uma vez sobre ela;

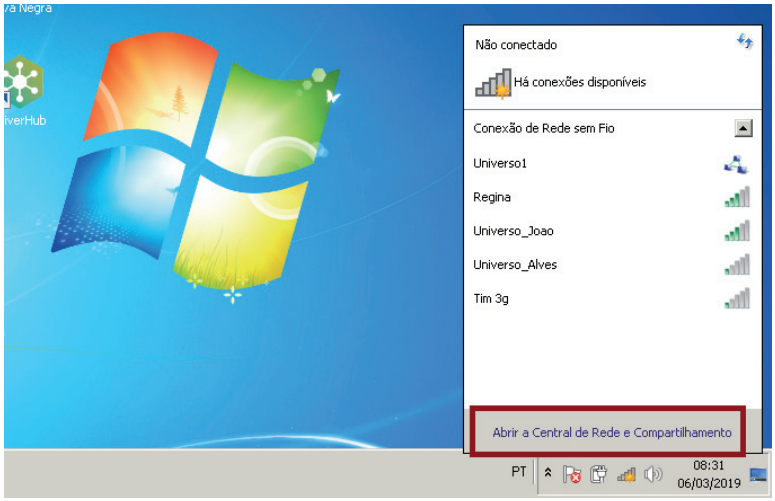


Figura 02.18: clique em Abrir a central de rede e compartilhamento.

2 - Irá abrir a janela Central de rede e compartilhamento. Clique, à esquerda dessa janela, em Gerenciar Redes sem fio;

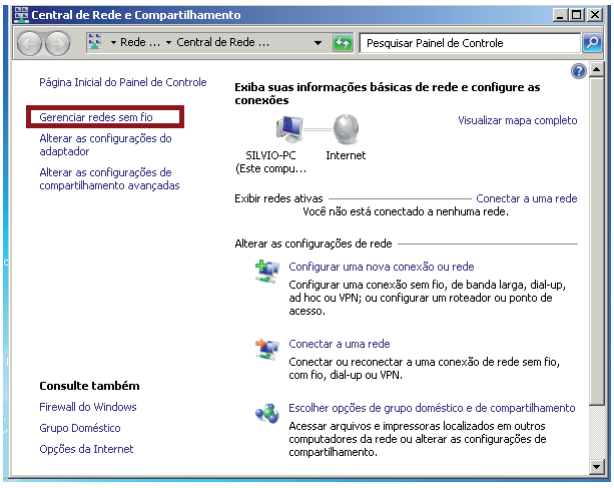


Figura 02.19: Clique em Gerenciar Redes sem fio.

3 - Irá abrir a janela Gerenciar Redes sem fio;

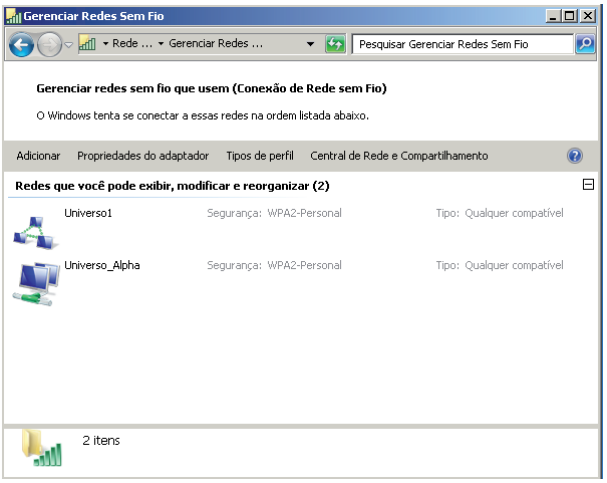
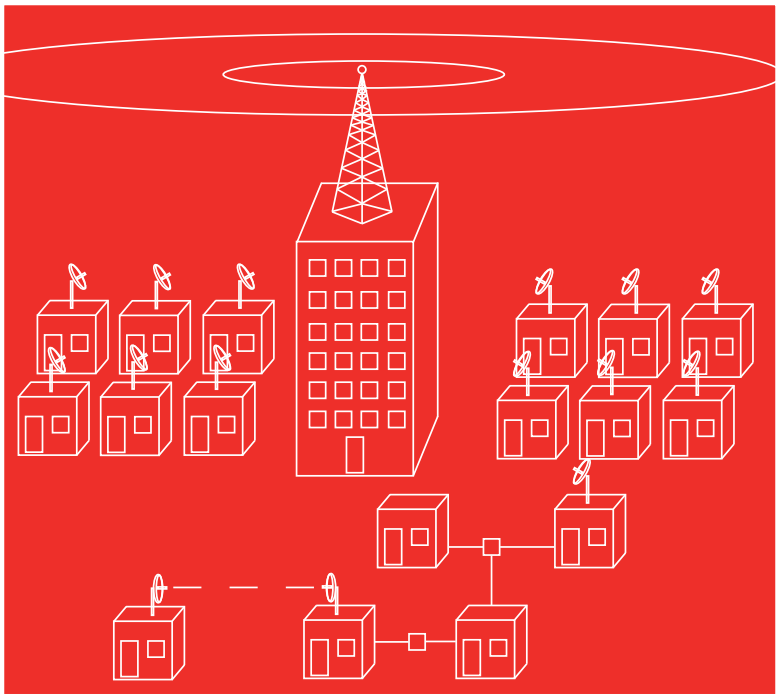


Figura 02.20: janela Gerenciar Redes sem fio.

4 - Clique uma vez sobre a rede sem fio que irá excluir. Por fim, clique em Remover e confirme na seqüência, clicando em OK.



Capítulo 03 - Instalação de uma rede Infra-estruturada

INTRODUÇÃO

A partir desse ponto do livro é abordado temas mais avançados, como a montagem de uma rede wireless infra-estruturada. Isso que dizer que a rede irá ter um ponto de acesso que centraliza toda a comunicação de todos os nós envolvidos. Não importa se dois microcomputadores, por exemplo, que querem se comunicar entre si estão a menos de 30 centímetros um do outro e o ponto de acesso está a 20 metros de distância. A comunicação deverá ser intermediada pelo ponto de acesso.

Esse ponto de acesso é o AP, siglas das palavras em inglês Access Point. Além dele centralizar e intermediar a comunicação entre os dispositivos da rede, ele possui também a função de firewall, protegendo a rede contra qualquer tipo de acesso não autorizado.

Um AP pode ter algumas funções embutidas, como switch (que permite ligar outros nós através de um cabo RJ-45) e roteador (que permite ligar a rede wireless a outra rede, como a Internet). Mas, além disso, ele pode ser configurado para trabalhar com determinados modos de funcionamento (ou modos de operação, que dá no mesmo), tais como Bridge, Wireless ISP, etc. Todos esse modos de operação serão abordados em momento mais oportuno, neste livro.

VANTAGENS DE UMA REDE INFRA-ESTRUTURADA

As redes infra-estruturadas são mais seguradas, permitem uma maior gerenciamento e controle dos usuários. O que não ocorre em redes AD HOC.

Ao instalar um AP, em suas várias configurações há o firewall, que ajuda a proteger a rede contra acessos de intrusos. Além disso, é possível, por exemplo, verificar quantos usuários estão conectados e até saber, através do seu número MAC, quem são esses usuários (basta fazer, em seu micro, um cadastro de todos os usuários, associando cada um deles ao número MAC da placa de rede wireless deles).

E se, por acaso, algum microcomputador acessar a rede com um numero MAC não conhecido, você pode simplesmente bloqueá-lo (e mais tarde

pode desbloqueá-lo, caso o identifique e autorize sua entrada). Mais adiante, nesta obra, há explicações sobre endereços MACs.

Como se é de perceber, a administração da rede também é bem ampla. É possível não somente saber quantos e quais usuários estão ingressados na rede no momento, mas é possível rastrear outras redes wireless ao alcance, obter informações das configurações atuais do AP, configurar data e hora tendo como base um servidor público NTP, etc.

DESVANTAGENS DE UMA REDE INFRA-ESTRUTURADA

Devido as vantagens, as desvantagens que podemos dizer que são realmente válidas são o custo, instalação e administração um pouco mais difícil, sem comparado a um rede AD HOC, claro.

Vamos começar falando do custo. Como esse tipo de rede exigi alguns equipamentos específicos (como APs e/ou roteadores), o valor gasto na montagem fica mais alto. Além disso, é necessário contratar a mão de obra qualificada, caso a rede não for montada por você. Tudo isso gera um orçamento maior.

A administração também exige um pouco mais de conhecimento. Aliás, redes AD HOC não exigem administração. Isso nem se aplica a elas. O mesmo não ocorre com redes infra-estruturadas, que necessitam de uma certa administração. Para configurar o AP, por exemplo, exige conhecimento a respeito dos vários parâmetros envolvidos. É necessário conhecer para quê serve cada configuração realizada e seus efeitos.

Mas, as redes infra-estruturadas são as ideais para qualquer empresa de qualquer porte, devido ás vantagens já mencionadas.

ONDE INSTALAR O ACESS POINT

A primeira providência a tomar é quanto ao local de instalação do AP. O local onde ele será colocado depende muito da rede, do seu tamanho, da função do AP, etc. Ele pode ser colocado sobre uma mesa ou armário, caso os nós envolvidos fiquem em uma ou duas salas (uma pequena escola de informática ou um escritório, por exemplo.).

Mas, se o objetivo é interligar dois segmentos de rede (nesse caso o AP é configurado para trabalhar no modo de operação Bridge), ele pode ser colocado dentro de uma caixa de proteção que fica na base (no tubo de aço ou torre) da antena. E a antena, por sua vez, é colocada em um local de tal forma que as duas antenas (parabólicas) se “enxerguem”. Por exemplo, suponhamos a interligação de duas redes que ficam em dois prédios que ficam um em frente do outro. Nesse caso, as antenas podem ser colocadas na cobertura do prédio, na parte mais alta, uma apontando para a outra.

Bom, os textos que seguem tem como base a montagem de uma WLAN, ou seja, uma pequena rede local sem fio. Desse modo, o AP pode ser colocado em um local onde ele fica protegido (onde não corra o risco de ninguém esbarrar nele ou até mesmo jogá-lo no chão), mas, não escondido. Se, ao montar a rede, perceber que alguns nós (que estão mais longe do AP) estão captando um sinal fraco, então, você deve reposicionar o AP, colocando-o em um local onde todos os nós fiquem com um bom sinal.

Alguns APs permitem serem configurados para trabalharem como repetidor. Um repetidor é usado quando se deseja enviar o sinal de rádio mais longe, aumentando a área de abrangência da rede. O que ele faz é “escutar” o sinal e repeti-lo, fazendo com que ele consiga alcançar uma distância maior. Para você entender melhor, vamos a um exemplo: suponhamos que você contratou o serviço de Internet via à rádio de sua cidade. Mas, quando a empresa foi até a sua casa para instalá-la, descobriu que o sinal captado está muito fraco, porque a sua casa fica muito longe da antena (que possui o ponto de acesso da empresa) deles. Para resolver o problema, a empresa pode instalar em alguma região próximo da tua residência (onde seja possível captar o sinal da antena da empresa) um repetidor, que irá “escutar” o sinal e repeti-lo em seu bairro. A partir daí o sinal de rádio em sua residência será captado com muito mais força e você (e todo os eu bairro) poderá usar a Internet.

Alguns APs podem ser afixados, através de parafusos, a uma parede. Mas, antes de furar a parede, configure a rede. Observe se todos os nós estão captando o sinal de rádio com um bom sinal. Somente depois fixe-o na parede.

Se você utiliza um roteador para conexão com a Internet via banda larga (chamado pelas operadoras de “modem”), então deve considerar a sua ligação ao AP, compartilhando a Internet com todos os microcomputadores/ notebooks envolvidos. Ele possui um cabo do tipo par trançado que não passa, geralmente, de dois metros.

E não se esqueça que ambos, AP e roteador, devem ser alimentados eletricamente. Dessa forma, deve haver por perto duas tomadas (se for usar os dois dispositivos) ou uma extensão com as tomadas necessárias.

PREPARATIVOS PARA A MONTAGEM DA REDE

Nesse momento, todos os microcomputadores ou notebooks que forem usar a rede devem conter uma placa de rede wireless perfeitamente instalada e configurada. Para saber como fazer isso, leia o capítulo 01 deste livro.

O AP deve estar previamente instalado fisicamente em um local escolhido. Além disso, o método adotado neste livro necessita que você ligue-o em um microcomputador ou notebook usando um cabo de rede par trançado, para que seja feita as primeiras configurações. Uma vez a rede configurada, o cabo de rede pode ser desconectado.

Para configurar a rede, apenas um microcomputador já é suficiente. Uma vez pronta, basta que os clientes sejam conectados nela.

O cabo de rede que acompanha o AP deve estar ligado à placa de rede cabeada do microcomputador (e esta, por sua vez, deve estar perfeitamente instalada) que você usará para configurá-lo, e, a outra ponta deve estar ligada à porta LAN do AP. Deixe a placa de rede (cabeada) configurada para obter IP automaticamente. Para isso, faça o seguinte:

1 - Acesse a Central de Rede e Compartilhamento. No capítulo anterior já vimos como fazer isso. Na janela Central de Rede e Compartilhamento, clique, à esquerda, em Alterar Configurações do Adaptador;

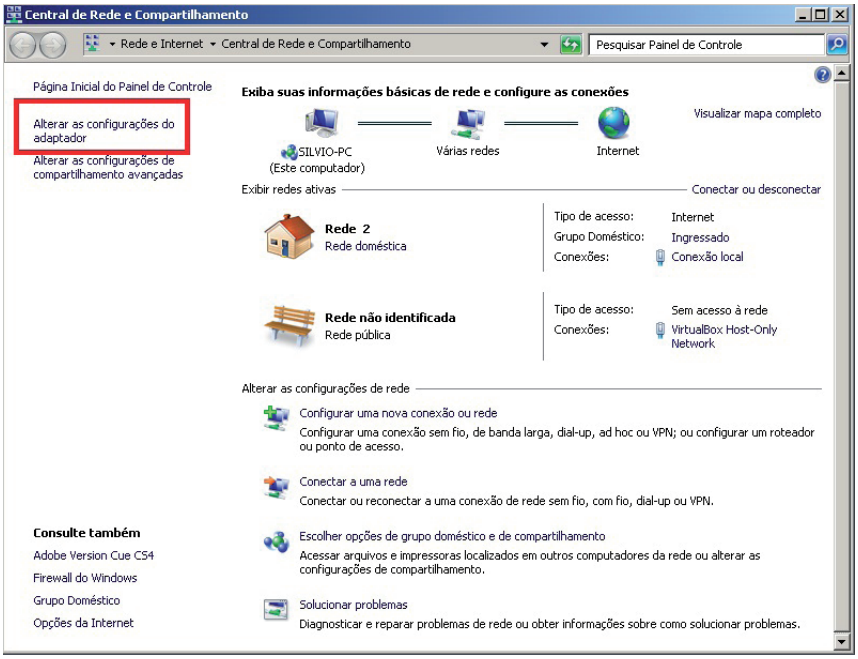


Figura 03.1: clique em Alterar Configurações do Adaptador.

2 - Clique com o botão direito sobre Conexão local e clique em propriedades;

3 - Na janela que se abre, clique uma vez (na lista Essa conexão usa estes itens) em Protocolo TCP/IP Versão 4 (TCP/Ipv4);

4 - Na janela Propriedades de Protocolo TCP/IP deixe marcado as opções “Obter um endereço IP automaticamente” e “Obter o endereço dos servidores DNS automaticamente”. Clique no botão OK. Clique em Fechar para fechar a janela;

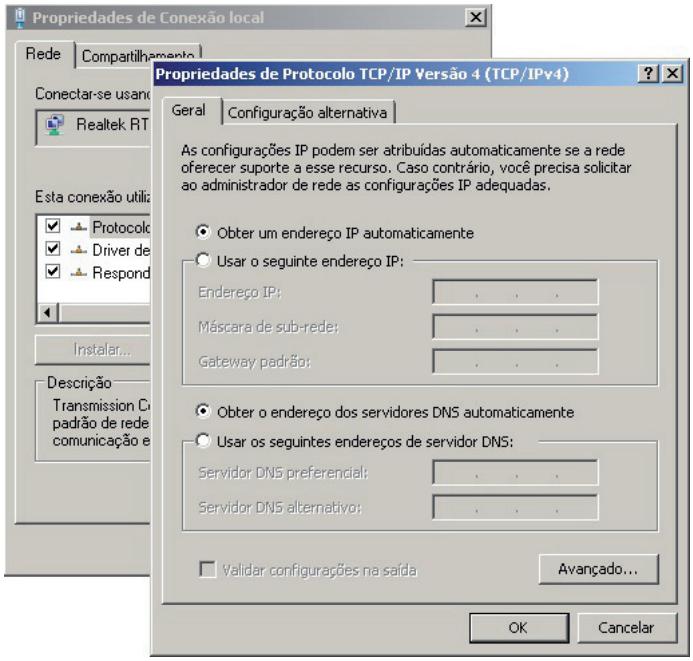


Figura 03.2: propriedades do protocolo TCP/IP no Windows 7.

Além disso, a conexão de rede local deve está Ativada. Para isso, faça o demonstrado a seguir.

1 - Clique no menu Iniciar – Rede;

2 - Acesse a Central de Rede e Compartilhamento. À esquerda dessa janela, clique em Alterar Configurações do Adaptador;

3 - Se a Conexão local estiver desconectada, você verá a descrição “Desativada” (além do ícone estar em uma cor bem opaca) no ícone da rede local, caso contrário, ele estará em uma cor azulada. Para ativar, se for necessário, clique com o botão direito do mouse sobre ele e clique em Ativar.

Na seqüência falamos sobre o cabo do tipo par trançado, caso você não tenha-o.

CABO DE REDE PAR TRANÇADO

Ao comprar o AP poderá vir junto, na embalagem, um cabo de rede do tipo par trançado com conectores RJ-45, com mais ou menos uns dois metros de comprimento. Esse cabo é utilizado para ligar o AP a um switch ou hub, ou ainda, para ligá-lo diretamente a um microcomputador (através de sua placa de rede). Esse é um cabo comum, usado em uma rede cabeada com switch ou hub.

Caso o seu AP não possua esse cabo, ou você tenha-o perdido, será necessário montar um. Para isso, será necessário:

- **Mais ou menos dois metros de cabo UTP CAT.5e:** esse é o padrão utilizado atualmente em redes cabeada. A metragem podem ser maior, se o AP estiver longe do micro onde você irá conectá-lo. O comprimento máximo recomendado é de 100 metros;

Figura 03.3: cabo UTP CAT.5e na metragem necessária.

- **Dois conectores RJ-45:** um para cada ponta do cabo. Se preferir, pode adquirir mais, pois, caso monte errado em na primeira tentativa, terá alguns reservas para substituir;

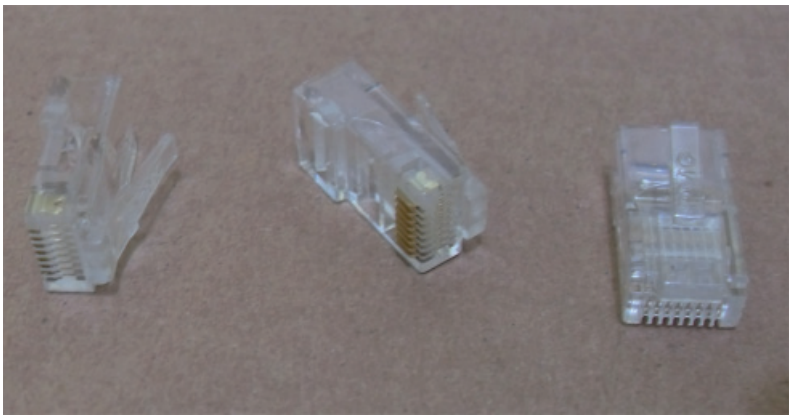


Figura 03.4: conectores RJ-45.

- **Um alicate crimpador de conectores RJ-45:** muita atenção nesse item, pois, assim como existem conectores diferentes existem alicates diferentes. Por exemplo: existe o conector RJ-11 (usado em telefonia). O tipo usado em redes de computadores, evidentemente, é o RJ-45;

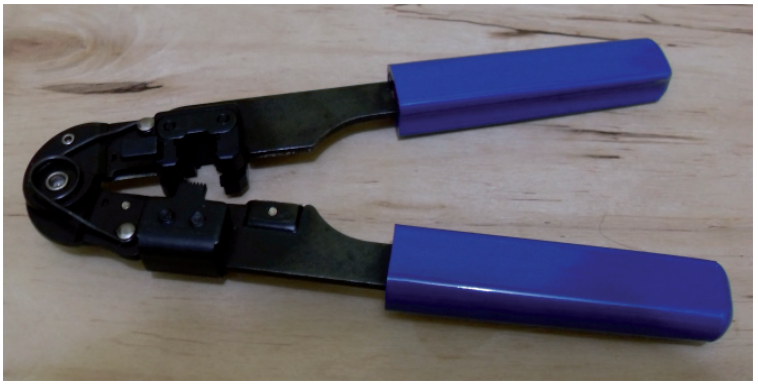


Figura 03.5: alicate crimpador.

- **Um testador de cabos para conectores RJ-45:** tal como ocorre com o alicate crimpador, existem testadores para todo tipo de conector. Adquira um para redes de computadores. Um testado típico é contém oito LEDs, um para cada fio do cabo.

Figura 03.6: testador de cabos.

Para montar o cabo basta ordenar os fios corretamente, esticá-los e aparálos, inseri-los no conector e crimpar. Os fios devem seguir uma ordem prédefinida. Existe a norma EIA/TIA 568A, que defini a seguinte ordem para os fios:

- Branco-Verde, verde, branco-laranja, azul, branco-azul, laranja, branco-marrom, marrom.

A ordem dos fios é da esquerda para a direita. Quando se diz fio “branco-verde”, por exemplo, estamos nos referenciando ao fio branco com listras verdes ou o fio verde claro. O mesmo ocorre com todos os outros. Por exemplo: um fio branco-marrom pode ser um fio branco com listras marrom ou um marrom claro.

Retire de 1,5 a 2 centímetros de capa plástica de proteção do cabo. Não é necessário medir em uma régua para retirar a quantidade ‘exata’. Faça

isso com a parte de corte do alicate (aquela que possui duas lâminas). Não ponha muita força para não correr o risco de “ferir” nenhum dos fios.

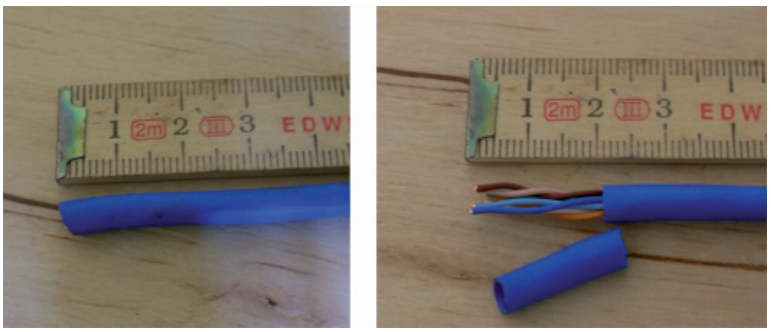


Figura 03.7: ponta decapada.

Ao ordenar os fios, use uma chave de fenda para deixá-los bem esticados. Isso é importante, pois, facilitará uma montagem correta. Perceba que ao esticá-los, as pontas ficam desiguais. Use a parte de core do alicate (aquela que possui apenas uma lâmina) para apará-los, deixando-os iguais.

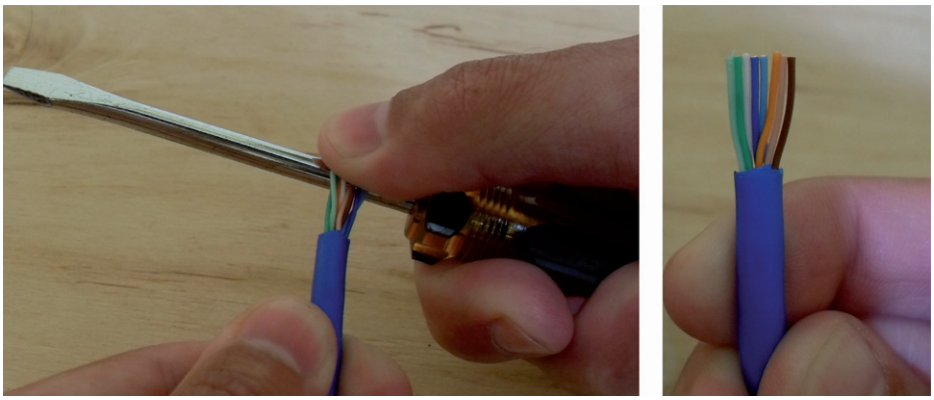


Figura 03.8: deixe os fios bem esticados e aparados.

Introduza os fios no conector com os contatos metálicos voltados para cima e finalize a montagem crimpando (introduza-o na parte de crimpar do alicate e aperte com força os cabos do mesmo).

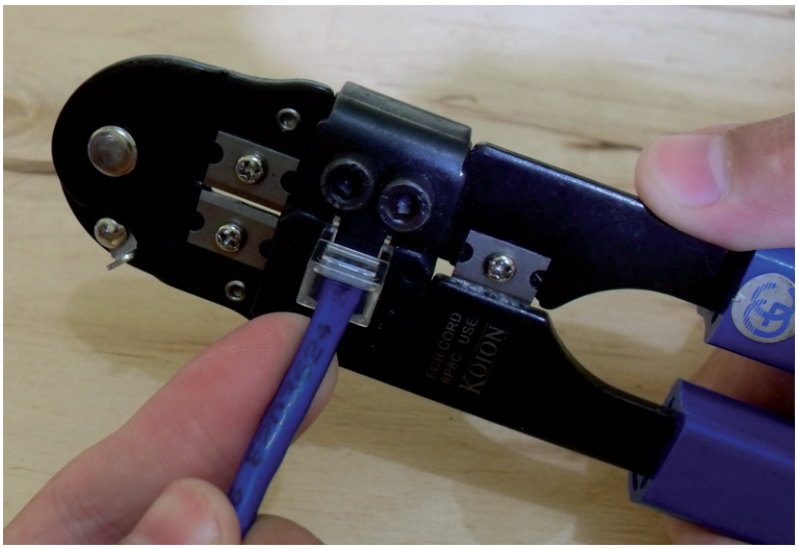


Figura 03.9: crimpagem.

Faça o mesmo procedimento com a segunda ponta do cabo. Ao final, basta testar-lo. O testador de cabos possui dois módulos, onde cada um deve ser conectado a uma ponta do cabo a ser testado. Para o testador típico, de oito LEDs, a ordem com que eles irão ascender deve ser 1, 2, 3, 4, 5, 6, 7 e 8. Isso deve ocorrer nos dois módulos, o que indica que o cabo está montado corretamente.

Veja bem: o módulo de comando do testador é aquele que possui a chave de ligar e desligar (o que possui a bateria). Ele irá sempre ascender na ordem 1, 2, 3, 4, 5, 6, 7 e 8. O segundo módulo apenas recebe o sinal do primeiro, e, se a ordem estiver errada, os LEDs ascenderão em uma ordem truncada. Caso isso ocorra, será necessário montar o cabo novamente.

Figura 03.10: teste do cabo.

DEVO RESETAR O AP?

Quando resetar o AP? Ao fazer isso, todas as configurações que estavam gravadas se perdem. Por isso, é preciso atentar-se quanto a essa decisão. Se nele existir ajustes que foram feitos e que você não sabe como fazer, então, o ideal é não resetá-lo.

Mas, antes de mais nada, se pergunte: por que resetá-lo? Você perdeu a senha de acesso ao “Web-Setup”? Talvez esse seja o motivo mais comum. Se foi configurado uma senha e você a perdeu, não conseguindo mais acessa-lo, e não há ninguém que possa saber a senha que foi configurada, então, não há outra saída.

Fora isso, uma vez tendo acesso ao “Web-Setup”, você pode ajustar, configurar, re-configurar, etc. E, portanto, não há motivo para resetar suas configurações.

Figura 03.11: use um palito de fósforos (ou algum objeto pontiagudo e fino) para resetar o AP. Mantenha pressionado o botão durante uns 10 segundos.

COMO ACESSAR O "WEB-SETUP"

Toda a configuração do AP se dá através de um setup que é acessado através de qualquer browser. Por isso, no meio técnico, esse setup é chamado de "Web-Setup".

Cada AP possui um número IP, e é través dele que acessamos o "Web-Setup". Consulte o manual do seu AP para saber o IP usado. Mas, caso não descubra o IP, vamos demonstrar como descobri-lo facilmente. Nós já sabemos com antecedência que o IP do nosso AP Zinwell G220 é 192.168.2.254. Vejamos agora como obter essa informação pelo sistema operacional Windows 7:

1 - Acesse a Central de Rede e Compartilhamento. No capítulo anterior já vimos como fazer isso. Na janela Central de Rede e Compartilhamento, clique, à esquerda, em Alterar Configurações do Adaptador;

2 - Verifique se a Conexão local está Ativa. Caso afirmativo, clique com o botão direito do mouse sobre ela e clique em Status;

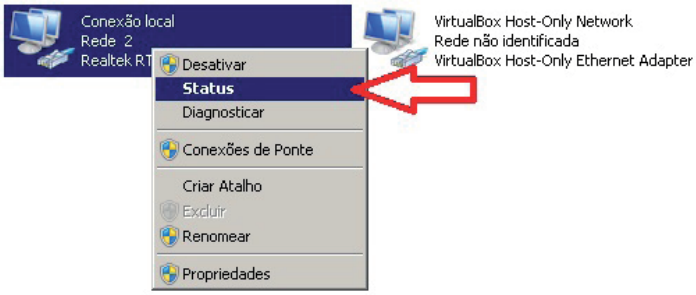


Figura 03.12: clique em Status.

3 - Clique em Detalhes. A informação de IP do AP estará lá. Procure pelo item Ipv4 Gateway padrão. Ele é o IP do AP.

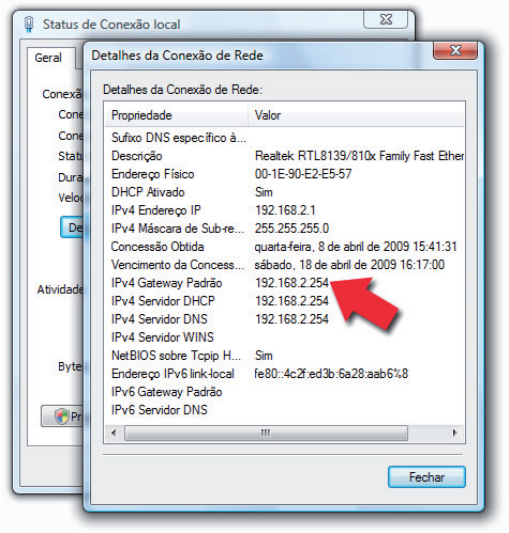


Figura 03.13: IP do AP no Windows.

Se a opção Status não estiver disponível, verifique o cabo de rede usado. Teste-o para verificar se não há nenhum problema. Se estiver tudo certo,

mas, mesmo assim não conseguir acessar o Status, use um cabo menor, com dois metros no máximo. Geralmente quando ocorre esse problema, também não é possível acessar ao “Web-Setup”.

Tendo as informações do IP do AP, o acesso pode ser feito em qualquer browser, como o Internet Explorer, Mozilla, etc. Basta digitá-lo no campo endereço (onde você digita a URL para acessar um site qualquer) e pressionar a tecla Enter. No nosso exemplo, digitamos assim:

http://192.168.2.254

Se preferir, nem precisa digitar ‘http://’, uma vez que, os browsers atuais já inserem essa informação automaticamente, quando ela não é digitada pelo usuário.

Pode acontecer de ser solicitado um nome e usuário e senha. Verifique no manual essas informações. Em APs novos (que ainda não foram configurados), pode ocorrer do nome de usuário ser Admin e a senha ser Admin (também), ou, pode não ser solicitado essas informações.

Figura 03.14: primeiro acesso ao “Web-Setup”. No nosso exemplo, não é solicitado nome de usuário e senha no primeiro acesso.

PRIMEIROS AJUSTES DO AP

Ao acessar o “Web-Setup”, observe que ele contém um menu, geralmente à esquerda da tela. Esse menu é dividido em seções, onde cada uma realiza um tipo bem específico de configuração. E isso vale para qualquer AP, de qualquer marca ou modelo.

Vale ressaltar que os nomes e quantidades de seções podem variar de acordo com a marca e modelo, uma vez que, não existe uma norma que regulamente isso. O menu do AP Zinwell Zplus G220 possui as seguintes seções:

- **Wizard:** é um item padrão em qualquer AP, ou seja, sempre que um AP tiver essa opção, saiba que se trata de um assistente de configuração, que guiará-o entre os principais passos necessário para que o AP possa ser configurado;

- **Wireless:** aqui podemos configurar diversos parâmetros da rede sem fio, tais como criptografia, autenticação, controlar o acesso dos usuários, etc;

- **Operation Mode:** configura o modo de operação do AP, como router, bridge e Wireless ISP;

- **TCP/IP:** faz o que o nome sugere, ou seja, nessa seção podemos configurar o IP do AP, a sub-máscara, o Gateway padrão, se o AP irá ser um servidor DHCP e qual a faixa de endereço IP será fornecido aos micros clientes, etc;

- **Firewall:** no geral, todo AP possui um firewall, e nessa seção podemos configurar vários aspectos de seu funcionamento;

- **Management:** aqui é a seção de gerenciamento da rede. É possível verificar o status atual (diversas configurações atuais), realizar ajustes de controle de banda, realizar upgrade do Firmware do AP, inserir um nome de usuário e senha para acessar o “Web-Setup”, etc;

- **Reboot:** reinicia o AP.

WIZARD

O Wizard provê uma forma fácil e rápida de realizar as primeiras configurações no setup. Você vai apenas escolhendo o que deseja e clicando em avançar (ou próximo, next, etc). neste capítulo veremos exatamente como é o seu funcionamento.

Lembramos que ao configurar somente pelo Wizard, já é possível deixar a rede em pleno funciomento, com a possibilidade dos micros clientes ingressarem nela, compartilhar arquivos, etc.

Vejamos, então, como configurar (AP base desse tutorial: AP Zinwell Zplus G220):

1 - Clique em Wizard;

2 - Irá abrir a página Setup Wizard. Nessa primeira página há instruções do que será feito. De acordo com as instruções da tela, percebemos que os passos seguintes (que iremos configurar) são: Setup Operation Mode, Choose your Time Zone, Setup LAN Interface, Setup WAN Interface, Wireless LAN Setting e Wireless Security Setting. Clique em Next>> para prosseguir;

Figura 03.15: página inicial do Wizard.

3 - Ao clicar em next chagamos à página Operation Mode (Modo de operação). Mais adiante, neste livro, há um estudo mais aprofundado dos modos de operação de um AP. Por enquanto, saiba que no modo router (roteador) o AP é usado para se conectar à Internet via ADSL / Cable Modem e a distribui na(s) sua(s) porta(s) LAN e na rede sem fio. O AP deve suportar esse modo, ou seja, ele deve ter embutido a função de roteador; no modo bridge, basicamente, ele atuará interligando duas redes. É muito usado para interligar os micros em rede e compartilhar a Internet recebida através de um roteador (perceba que é diferente do modo anterior, pois, nesse caso um roteador será ligado no AP através da porta WLAN, e, no modo anterior o AP já é um próprio roteador); no modo Wireless ISP (Internet Service Providers), que pode ser chamado também por WISP), ele recebe Internet através do sinal wireless e a distribui na(s) sua(s) porta(s) LAN. É um modo que pode ser usado, por exemplo, em empresas que oferecem Internet sem fio (wireless). No nosso exemplo, selecionamos o modo bridge. Clique em next>> para continuar;

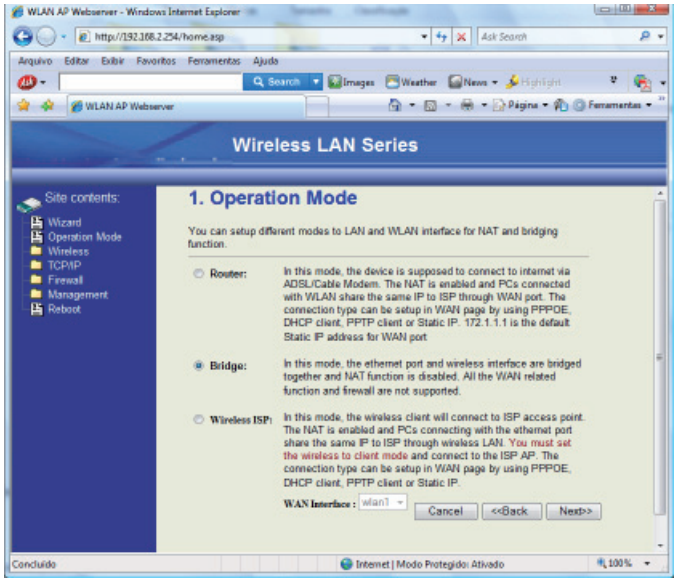


Figura 03.16: Operation Mode (Modo de operação).

4 - A próxima página é a Time Zone Setting (Fuso horário), onde é possível acertar a data e hora através de um servidor público NTP (Network Time Protocol). Para isso, marque a opção Enable NTP client update. É preciso selecionar o fuso horário correto e um servidor. Como exemplo, no Brasil selecionamos o fuso horário (GMT-03:00)Brasília. Para funcionar, o AP deve conseguir se conectar à Internet, de forma direta (quando o AP é um roteador) ou através de um roteador ligado à sua porta WLAN, por exemplo. Clique em next>> para continuar;

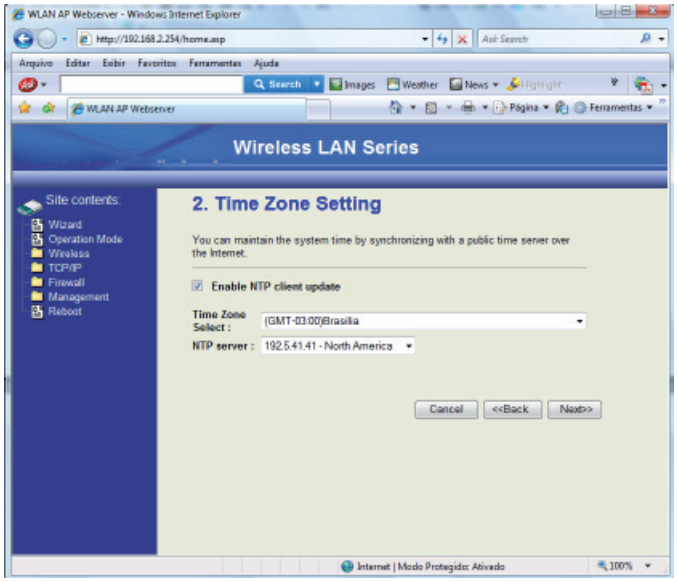


Figura 03.17: Time Zone Setting (Fuso horário).

5 - Na seqüência, chegamos à página LAN Interface Setup (configura parâmetros da rede local). Nesse momento podemos configurar o IP do Access point e a sub-máscara usada. Não é necessário mudar esse item, pois, o IP sugerido pelo fabricante já está na faixa de IPs para que a rede funcione normalmente. Clique em next>> para prosseguir;

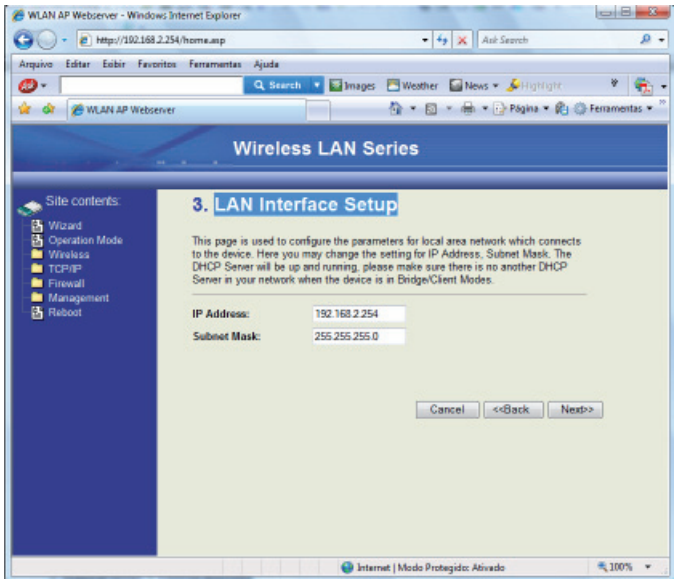


Figura 03.18: LAN Interface Setup.

6 - Na seqüência vem a penúltima página, que é a Wireless Basic Settings (que são definições básicas da rede sem fio). Não vamos nos aprofundar muito nesses parâmetros por enquanto, pois, no decorrer do livro voltaremos a esse assunto. Mas, por hora, em Band configure 2.4GHz (B+G); em Mode configure AP (dessa forma ele será um transmissor receptor) ou client (caso ele for apenas um receptor. Exemplo: se você tiver configurado-o para o modo Wireless ISP); em SSID coloque um nome que identificará a rede (é o nome da rede); em Channel Number escolha um canal ou deixe em Auto (basicamente, em uma rede não pode existir dois AP usando o mesmo canal). Clique em next>> para ir à última página;

Figura 03.19: Wireless Basic Settings.

7 - A página final é a Wireless Security Setup (Configuração de Segurança Wireless). É nesse ponto onde configuramos a segurança da rede sem fio. Isso é importante, pois, se não for configurado, qualquer pessoa que tiver um microcomputador ou notebook com uma placa de rede wireless e detectar a sua rede, poderá se conectar nela. Para ativar a segurança, em Encryption (criptografia) selecione o padrão de encriptação. Este assunto também é abordado mais detalhadamente, adiante neste livro, por isso, não iremos falar de cada um deles aqui para não tornar a leitura muito repetitiva. Por enquanto, selecione WEP. Em Encryption deixe em 64-bit. Em Key Format selecione ASCII ou hexadecimal. Em Default Tx Key deixe selecionado Key 1. E por fim, em Encryption Key 1 digite uma chave da rede. Por regra (e respeitando o que foi selecionado em Key Format), digite 5 caracteres ASCII ou 10 hexadecimais. Clique em Fineshed para finalizar.

Figura 03.20: Wireless Security Setup.

Com esse ajustes que foram realizados a rede já está funcionando. Os micros clientes já podem ingressar nela, compartilhar arquivos, dispositivos e programas.

Ao ingressar um micro cliente, será solicitado a chave da rede, que foi a criada no último passo (em Wireless Security Setup). Caso não tenha sido configurado essa parte, então nenhuma chave será solicitada e o acesso será livre.

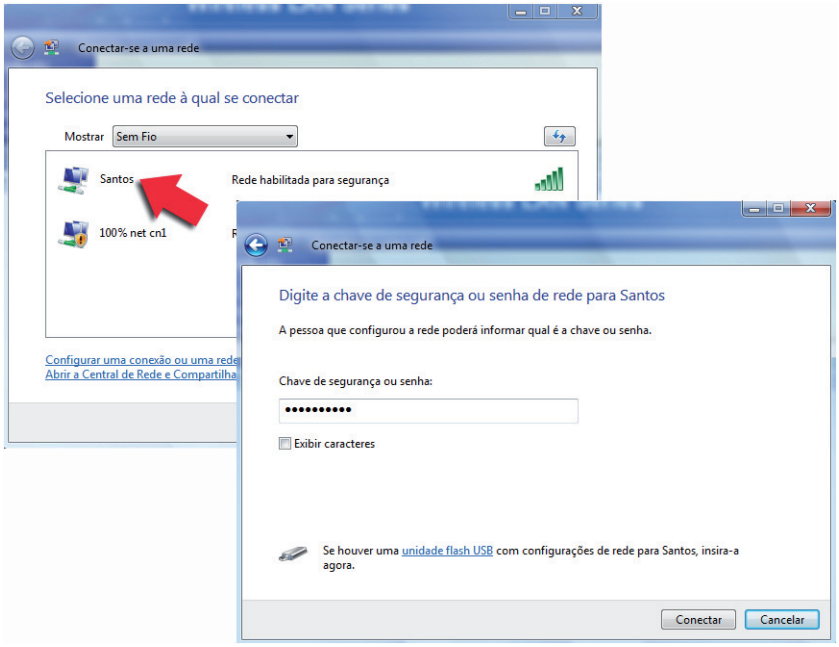
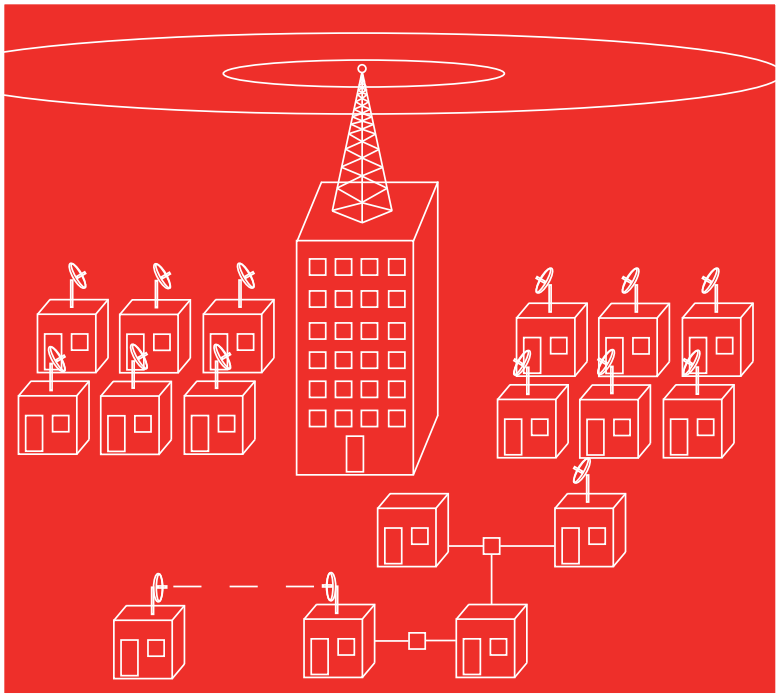


Figura 03.21: rede detectada no Windows – Solicitação de chave segurança ou senha.



Capítulo 4 - Modos de operação do Access Point

INTRODUÇÃO

Um Access Point pode operar de diferentes modos. Ao configurá-lo, é necessário conhecer bem para quê serve cada modo, para que dessa forma, a rede possa funcionar corretamente. Se você configurar um modo errado para o seu tipo de rede, ela pode simplesmente não funcionar.

Com este capítulo pretendemos apresentar os vários modos possíveis. Não necessariamente um determinado modelo de AP suportará todos os modos. Depende muito da marca, modelo, da versão do firmware instalada e principalmente, a que se destina o AP. Mas, estudando todos esses modos de funcionamento, ficará fácil configurar qualquer AP, de qualquer marca e modelo. É interessante se fazer constar, que ao configurar o AP, na seção sobre os modos de funcionamento, pode não ter todos esses modos listados, mas, mesmo assim o AP suportar todos eles. É comum, por exemplo, escolher um determinado modo de operação e configurá-lo de diferentes formas. Por exemplo: o modo bridge que pode ser configurado para trabalhar no modo AP (passando a trabalhar, basicamente, no modo raiz), Client (onde ele se tornará apenas cliente de um AP principal, o que nos remete ao modo Bridge ponto a multiponto e Wireless ISP), entre outros tipos de configurações que é abordado ao longo deste livro.

Por isso, o mais importante, neste capítulo, é entender o significado principal e para quê serve cada modo listado a seguir. Não se preocupe, por enquanto, se você irá ou não encontrar essa nomenclatura no seu AP. Não fique intrigado se eu AP possui no “Web-Setup” apenas os modos Router, Bridge e Wireless ISP (e não tem nenhum modo Raiz), pois, isso é normal e seu AP não está com defeito. Você vai conseguir fazer ele trabalhar no modo Raiz, e veremos como fazer isso nos capítulos que se seguem.

MODOS ESTUDADOS

Os modos de operação estudados neste capítulo são:

- Raiz
- Bridge ponto a ponto;

- Bridge ponto a multiponto;
- Router/Gateway;
- Wireless ISP;
- Repetidor.

É interessante adiantar, que dependendo do modo, configurações diferentes devem ser realizadas no “Web-Setup”. Até a antena utiliza pode ser diferente, ao configurar um ou outro modo. Esses detalhes são abordados ao longo do livro.

MODO RAIZ

Podemos dizer que esse é o modo “natural” de qualquer AP, pois, é nesse modo que ele permite que uma WLAN funcione normalmente. Os computadores podem compartilhar arquivos, dispositivos, programas e Internet entre si. Ou seja, ele atua tal como o switch ou hub, interligando todos os nós envolvidos na rede.

A antena comumente utilizada nesse modo é a onidirecional, que envia sinais em todas as direções.

Figura 04.1: exemplo clássico de uma rede em modo raiz.

Geralmente, ao configurar um AP, na seção Modo de Operação, não há o uso dessa nomenclatura (Modo Raiz). O comum de se usar é modo Bridge, como ocorre com o modelo que usamos como base para esse livro. E o modo bridge pode ser configurado como AP (e nesse caso será um perfeito modo Raiz), cliente, etc.

MODO BRIDGE PONTO A PONTO

A definição básica de bridge é um dispositivo que permite interligar dois trechos de uma rede ou duas redes que estejam em locais diferentes. Além disso, ele controla o tráfego de dados entre um trecho e outro. O AP também pode assumir essa função.

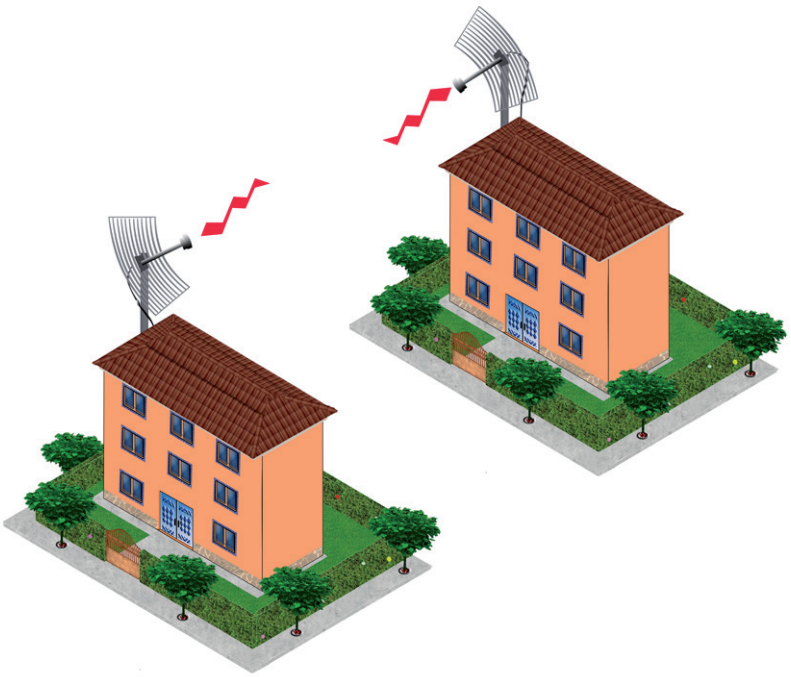


Figura 04.2: exemplo da utilização do modo bridge ponto a ponto. Observe que aqui temos a representação de dois imóveis onde, cada um possui uma rede (LAN ou WLAN), e, que são interligadas graças as antenas wireless.

Para ficar fácil entender, suponhamos duas redes: uma rede “LAN1” e outra “LAN2”, ambas em prédios diferentes, mas, em uma mesma quadra. O modo bridge ponto a ponto pode ser utilizado para interligar essas duas redes.

O tipo de antena geralmente utilizado para esse fim é a direcional. Essa antena deve ser apontada diretamente para o “alvo” (a antena da segunda rede ao qual ela deve se conectar), pois, ela envia o sinal apenas em uma direção. Árvoves, prédios, montanhas, entre outros obstáculos, podem denegrir (enfraquecer o sinal) ou até impedir a comunicação.

BRIDGE PONTO A MULTIPONTO

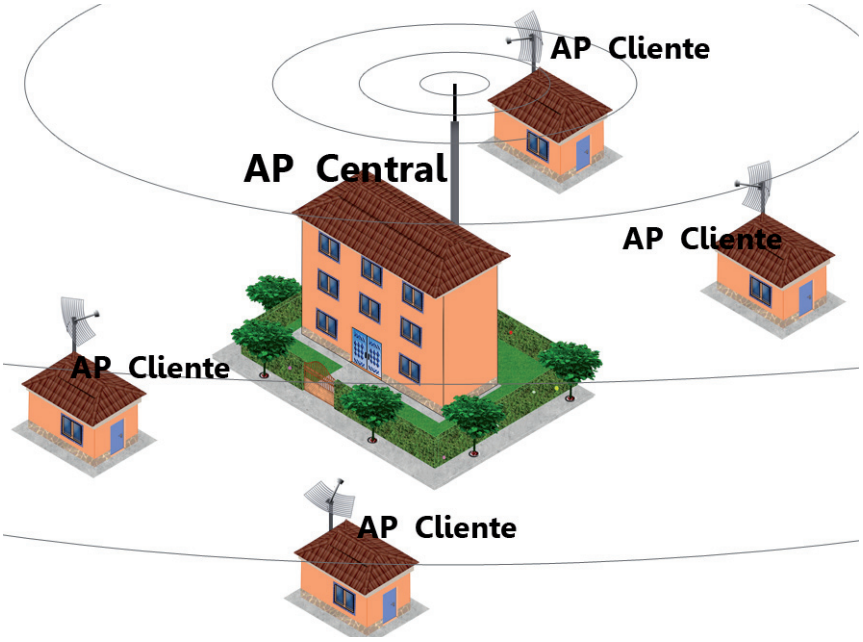


Figura 04.3: nesse exemplo, todos os clientes se conectam a um mesmo AP central. Esse esquema é muito utilizado por provedores de Internet via à rádio. Nesse caso, não necessariamente o cliente necessita de um AP (muitas vezes a antena direcional é conectada diretamente à placa wireless, através de um cabo coaxial), muito embora, o uso do AP ajude a manter o sinal mais estável.

É bem parecido com o modo ponto a ponto, com a diferença de existir um AP central, que utiliza uma antena onidirecional e que permiti a conexão de vários clientes (seja um micro ou seja uma rede). O modo que veremos a seguir, Modo Wireless ISP, é um modo bridge ponto a multiponto.

Um exemplo comum desse tipo de configuração são as conhecidas Internet via à rádio. O AP da casa do cliente é configurado para se conectar com a rede do provedor, tendo, assim, acesso à Internet. A antena do cliente é direcional, sendo apontada diretamente para a antena do provedor de acesso à Internet, que é onidirecional. Um perfeito exemplo de modo bridge ponto a multiponto.

Perceba que nesse caso os clientes não conseguem se comunicar diretamente entre si. Mesmo que um cliente compartilhe uma pasta, os outros não terão acesso a ela. Mas, todos estão interligados na mesma rede e tendo acesso à Internet.

MODO ROUTER/GATEWAY

Ambos dizem respeito ao mesmo tipo de configuração. Apenas o nome no “Web-Setup” é que muda (Router ou Gateway). O mais comum é o uso da nomenclatura Router.

Quando o AP é configurado nesse modo, ele irá receber, diretamente, através de um cabo a internet ADSL, só para citar como exemplo, e irá distribuí-la por toda a rede, seja através de ondas de rádio (wireless) ou através de suas portas LAN (quando existirem).

Por isso que se chama modo router, pois, nesse caso o AP estará atuando como um roteador. Alguns fabricantes chamam esse modo de gateway porque esse é um nome que se dá a qualquer dispositivo (incluindo microcomputadores) que compartilham Internet em uma rede.

Perceba, dessa forma, que o AP deve possuir essa função, ou seja, ele deve ter um roteador embutido, internamente. Caso contrário ele não será capaz de executar essa tarefa.

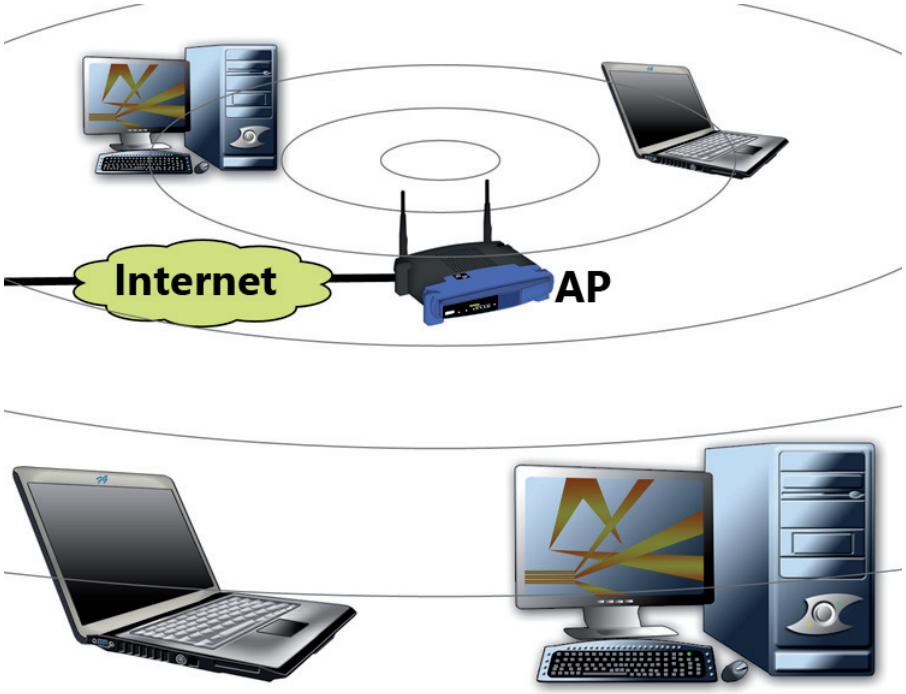


Figura 04.4: AP em modo router.

Uma dúvida comum: se ligarmos um roteador à porta WLAN do AP, ele deve ser configurado no modo Router? Apesar de, em um primeiro momento, a resposta parecer ser sim, a resposta certa é não. Nesse caso o AP deve ser configurado como bridge, pois, apesar do roteador estar conectado ao AP, ele é um dispositivo à parte. O papel do AP será tão somente interligar a rede local se fio (WLAN) à Internet que está sendo provida graças ao roteador. Ele irá interligar duas redes distintas.

MODO WIRELESS ISP

ISP significa Internet Service Providers. Muitas vezes é chamado por WISP (Wireless ISP). Quando o Access Point possui esse modo, ele é capaz de receber o sinal wireless de um provedor de Internet via à rádio e distribuí-lo através da(s) sua(s) porta(s) LAN. Nessa configuração, o AP atua apenas como um cliente wireless.

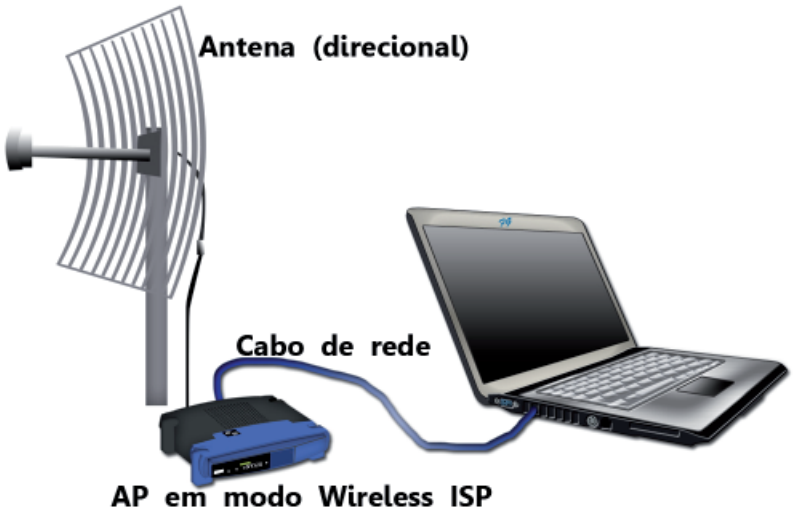


Figura 04.5: nesse esquema, observe que a antena tem o papel de se comunicar diretamente com a antena do provedor, obtendo, dessa forma, acesso à Internet. Outro detalhe, é que no nosso exemplo o cabo de rede está ligado diretamente a um notebook. Mas, ele pode ser conectado a um hub/switch, para que mais nós possam desfrutar da Internet.

Perceba que ele não redistribui essa Internet via ondas de rádio, e sim via porta LAN. O micro (ou os micros/notebooks) que forem usar essa internet, devem estar ligado ao AP via cabo de rede (do tipo para trançado. Para saber como montar esse caso, veja capítulo anterior). Se o AP tiver apenas uma porta LAN, e você tiver dois ou mais computadores (incluindo portáteis), basta ligá-la a um hub ou switch. A partir daí, você pode ligar quantos microcomputadores ou notebooks você quiser, de acordo com as portas LAN disponíveis no hub ou switch. Vale lembrar que quanto mais pessoas estiverem usando a Internet ao mesmo tempo, mais “pesado” fica para navegar.

Se você tiver apenas o AP (em modo Wireless ISP) não é possível ligar os micros em redes via ondas de rádio. É possível ligar o micro em rede apenas se o AP possuir portas LAN (se ele possuir a função de switch/hub), ou, ligando-o em um switch/hub à parte, ou seja, montando uma rede cabeada.

A essa altura, deve surgir uma dúvida em muitos que estão lendo esse tópico: será que, nesse modelo de configuração, tem como distribuir o acesso a Internet (que é fornecida graças ao “AP Wireless ISP”) através de ondas de rádio? Ou seja, em uma rede local sem fio? Sim. Mas, nesse caso é necessário usar dois APs: um configurado no modo Wireless ISP (recebendo a Internet via à rádio), que estará ligado a um segundo AP, via cabo de rede.

Esse segundo AP é configurado normalmente (como bridge, por exemplo) para distribuir a Internet na rede, através de ondas de rádio, e interligar os nós envolvidos para poderem compartilhar arquivos, programas, impressoras, etc, além de terem acesso à internet.

MODO REPETIDOR

O modo repetidor é usado quando o objetivo é aumentar a área de cobertura de uma rede wireless. Como se dá para perceber pelo nome, o que ele faz é repetir um dado sinal. Para isso ser possível, primeiramente ele precisa “escutar” o sinal de um Acces Point e em seguida repeti-lo. E isso deve ser feito dentro do mesmo canal do Access Point principal.

O processo todo (escutar e repetir) não é feito instantaneamente. É gasto um tempo (embora muito pequeno) para que isso possa ser feito. Quando se usa um segundo AP para repetir o sinal de um primeiro, não se chega a perder muito em desempenho da rede. Mas, se você precisar usar um terceiro para repetir o sinal do segundo, aí já se começa a notar diferença. E se você colocar um quarto para repetir o sinal do terceiro, a queda de desempenho pode se tornar visível.

Suponhamos que um cliente use a rede através do sinal repetido lá no quarto AP. Com certeza, as suas solicitações serão muito mais lentas. Quando ele solicitar algum dado da rede, o tempo a partir do momento da solicitação até a entrega do dado será muito maior, em comparação aos computadores que se conectam na rede a partir do primeiro AP.

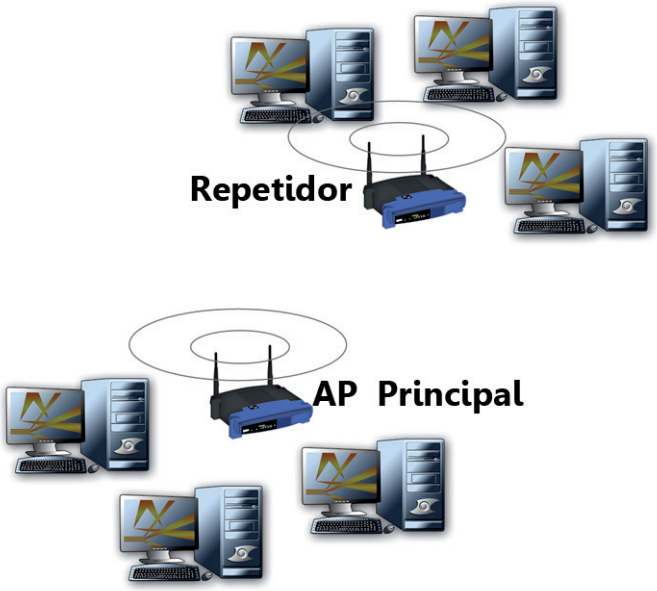


Figura 04.6: uso de repetidor. Nessa figura temos um AP principal e o repetidor, que "escuta" o sinal do AP principal e repete-o, ampliando a área de cobertura da rede.

O motivo de se usar repetidores, em um contexto geral, é que todo meio de transmissão contém limitações quanto à distância, comprimento. Um cabo UTP CAT.5, por exemplo, pode ter algo em torno de 100 metros. Estamos falando de um mesmo lance de cabo. Cabos do padrão 10Base-FP (Fibra óptica) podem ter o comprimento máximo girando em torno dos 500 metros, em um único lance.

Com redes wireless não é diferente. Uma WLAN, dependendo da configuração de hardware e software, possui uma área de cobertura girando em torno de 90 metros.

Mas, porque existem essas limitações? É porque conforme um sinal "caminha" através de um meio, ele vai enfraquecendo (atenuando), perdendo força. E isso vale para qualquer tipo de cabos ou fios, meios

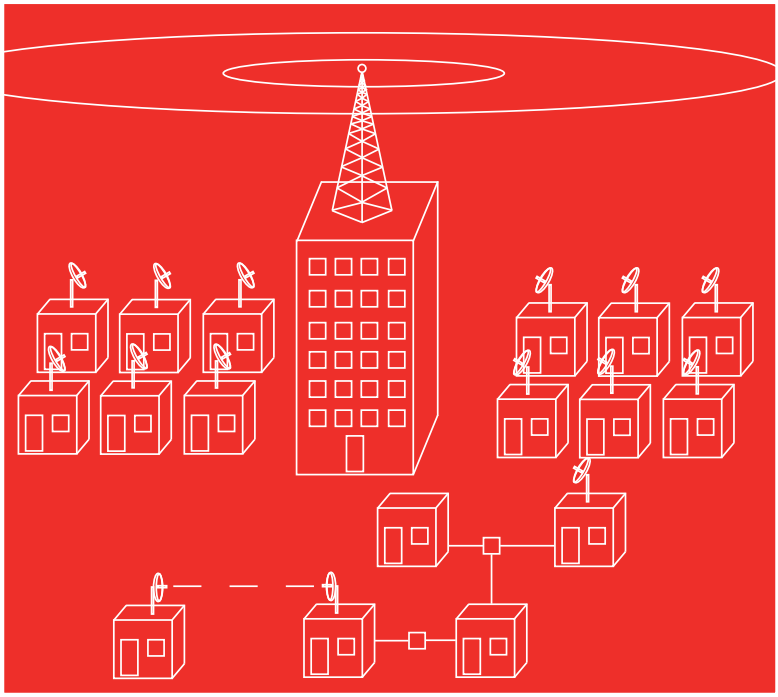
de transmissão (no caso das redes wireless é o “ar”), tecnologias (redes, televisão ou telefonia), etc.

Por isso o repetidor é necessário em casos em que é necessário enviar um trecho de cabos de rede mais longe, ou, ampliar a área de cobertura wireless, etc.

CONFIGURAÇÕES NA PRÁTICA

No geral, o modo de operação de um Access Point pode ser configurado na seção Operation Mode. Cada modo de operação exige todo um conjunto de configurações apropriadas. Por exemplo: ao configurar um AP no modo router, você deve realizar configurações relativas a Internet que está ligada na porta WAN, tais como mudar o método de acesso para IP estático, DHCP Cliente, PPPoE ou PPTP, etc.

Nas páginas que se seguem é abordado vários tipos de configurações que podemos fazer, de acordo com o modo de operação do AP.



Capítulo 5 - Configurações Wireless

INTRODUÇÃO

Neste capítulo há uma abordagem prática das mais variadas configurações que podem ser realizadas para que a rede sem fio funcione em sua total plenitude. Usando como referência o Access point Zinwell Zplus G220, iremos explorar a seção Wireless e seus parâmetros. Você pode usar o que está sendo dito a respeito de cada tipo de configuração no seu AP, não importando a marca e modelo, uma vez que elas valem para todos.

Vale ressaltar que o menu, sua disposição e quantidades de itens presentes podem variar de acordo com a marca e modelo do AP. Mas, as explicações sobre os tipos de configurações são válidas para todos. Por exemplo: ao falarmos do canal do AP (Channel number), estamos explicando um parâmetro que possui um significado global, ou seja, seu modo de configuração, utilidade e significado é o mesmo em qualquer AP.

MENU WIRELESS

Ao clicar na seção wireless, abre-se um menu contendo vários links divididos por tipo de configuração. Cada link abre uma página onde é possível fazer os ajustes e salvar. Nos exercícios que se seguem, são abordado os seguintes itens: Basic Settings, Advanced Settings, Security, Access Control, WDS settings, Site Survey e Connecting Profile.

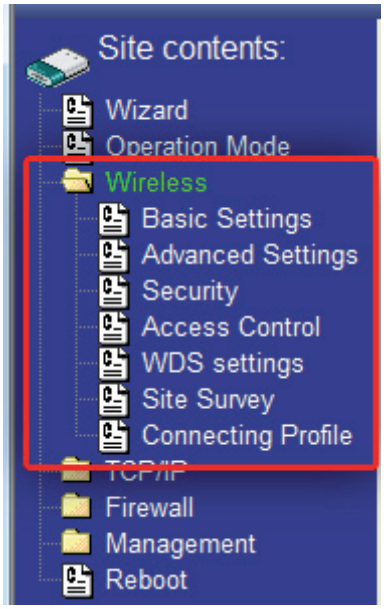


Figura 05.1: menu Wireless.

BASIC SETTINGS

Como se dá para perceber pelo nome, aqui realizamos as configurações básicas da rede sem fio. Em uma rede cabeada, as configurações básicas seriam a preparação do cabo par trançado (sua montagem) e conexão entre as placas de rede e hub/switch. No caso das redes sem fio, configuramos a banda e canal usados, modo e nome da rede, etc.

Band

Configura a banda de operação do AP e a freqüência, ou seja, o padrão de conexão. No geral, você poderá encontrar as bandas A, B e G. O mais comumente é a utilização da banda B ou G ou a combinação das duas (B+G).

A configuração da banda irá definir os padrões de equipamentos/dispositivos que podem ser utilizados:

- **2.4GHz (A):** Somente equipamentos/dispositivos do padrão IEEE 802.11a. Até 54Mbits/s. Trabalha na freqüência de 5GHz;
- **2.4GHz (B):** Somente equipamentos/dispositivos do padrão IEEE 802.11b. Até 11Mbits/s. Trabalha na freqüência de 2,4GHz;
- **2.4GHz (G):** Somente equipamentos/dispositivos do padrão IEEE 802.11g Até 54Mbits/s. Trabalha na freqüência de 2,4GHz;
- **2.4GHz (B+G):** Permite equipamentos/dispositivos do padrão IEEE 802.11b e IEEE 802.11g simultaneamente. É o modo conhecido como misto. Apesar de permitir dispositivos de dois padrões, quando um dispositivo IEEE 802.11b se comunicar com um IEEE 802.11g, a velocidade máxima será de 11Mbits/s.

A mais popular é a banda B, mas, se tiver a opção B+G (uma rede mista), para um melhor desempenho, selecione-a. No geral, você não irá encontrar disponível a configuração para o padrão IEEE 802.1a, pois, ele perdeu terreno para os padrões IEEE 802.1b e IEEE 802.1g.

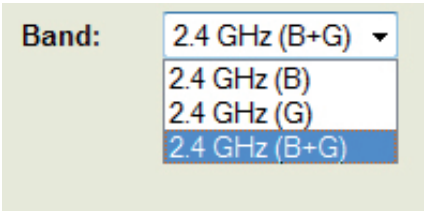


Figura 05.2: band.

Mode

Configura o modo com que o Acess point irá operar. Independente de você configurar o Acess Ponit como router, bridge, ou outro modo, essa configuração, no geral, deve ser feita.

Suponhamos que tenha configurado-o como bridge. Então, nesses parâmetros devemos configurar como o bridge irá se comportar.

As opções de configurações, normalmente, são:

- **AP:** configura-o como um ponto de acesso, onde ele irá interligar todos os nós da rede e intermediar a suas comunicações;
- **Client:** aqui, como o nome sugere, ele será cliente de algum outro AP principal, por exemplo. Essa opção é usada por exemplo, no modo de operação Wireless ISP, ou seja, quando estiver usando o AP para acessar a Internet via à rádio de algum provedor;
- **WDS:** são siglas das palavras em inglês Wireless Distribution System. Deve ser configurado quando se for interligar APs para se ampliar a área de cobertura de uma rede, ou seja, quando um AP for configurado como repetidor. O AP repetidor deve estar clonando o endereço MAC do principal e ambos devem ser configurados para utilizar o mesmo canal (Channel Number). O repetidor deve estar na área de cobertura do principal, e ele irá estender essa área. No geral, esse modo é usado por provedores de acesso à Internet via à rádio, e, só funciona o acesso ao serviço oferecido, que é a internet. Os micros envolvidos não podem ser comunicar entre si;
- **WDS + AP:** esse é o modo WDS combinado com o modo AP. Basicamente é o mesmo modo anterior (WDS) com a diferença de que os clientes podem se comunicar entre si.

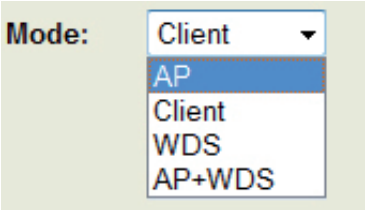


Figura 05.3: Mode.

Network Type

Esse item fica disponível para uso somente quando modo cliente (client) for usado. Define o tipo de rede (Network Type). O padrão é infrastructure (infraestrutura), e é usado, basicamente, quando for interligado ao AP um router ou até mesmo outro AP. O modo AD HOC é utilizado para estabelecer ligação entre computadores, somente.

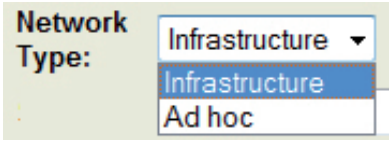


Figura 05.4: Network Type.

SSID

SSID são Siglas das palavras em inglês: Service Set Identifier. Nada mais é do que o nome da rede configurada no Access Point em questão, a sua identificação. Quando um micro detecta uma rede wireless, esse é o nome exibido. Por isso, ele é muito importante. Se haver muitas redes sem fio em uma mesma área de cobertura, o nome é a principal forma de diferenciar uma da outra.

É possível usar até 32 caracteres no nome. Algo muito importante que devemos dizer: O SSID é case-sensitive, o que significa que ele diferencia letras maiúsculas de minúsculas. Ou seja, “s” (minúsculo) é diferente de “S” (maiúsculo).

O ideal é usar nomes que identifiquem a rede, que tenham algo a ver com aquilo que ela se propõem. Suponhamos que uma faculdade chamada “Vencer” cria uma rede sem fio para acesso dos alunos à internet. O SSID pode ser simplesmente Vencer, VencerNet (sempre com muita atenção ao uso de letras maiúsculas e minúsculas), etc.

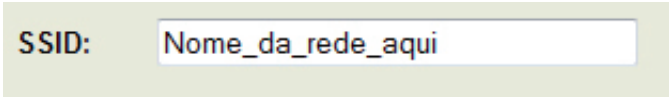


Figura 05.5: SSID.

Channel Number

Como sabemos, as redes sem fio funcionam através de ondas de rádio. O padrão 802.11b e 802.11g funcionam dentro da freqüência de 2.4 GHz, e são divididas em 11 canais de transmissão, que é uma banda estreita de freqüência utilizável para uma comunicação.

Isso que dizer que cada canal irá utilizar uma determinada banda de freqüência. Por exemplo: canal 1= 2,412GHz; canal 2= 2,417GHz; canal 3= 2,422GHz, canal 4= 2,427GHz; canal 5= 2,432GHz; canal 6= 2,437GHz; canal 7= 2,442GHz; canal 8= 2,447GHz; canal 9= 2,452GHz; canal 10= 2,457GHz; e canal 11= 2,462GHz.

Por esse motivo dois APs, em uma mesma rede, não podem utilizar o mesmo canal, a não ser que um determinado AP esteja configurado para ser repetidor de um outro. Aí, nesse caso, ambos devem usar o mesmo canal.

Não é possível configurar um canal se o modo escolhido for Client, ou seja, essa configuração é válida somente para os modos AP, WDS e AP + WDS.

Se sua rede for ter apenas um AP, não é necessário trocar o canal, sequer precisa se preocupar com esse parâmetro. Troque de canal apenas se a latência da rede estiver alta, pois, isso pode ser provado por interferências e a troca de canal pode ajudar.

É interessante se fazer constar que dispositivos tais como transmissores de redes Bluetooth, telefones sem fio de 2,4 GHz, microondas, e outros, podem causar interferência em uma rede sem fio. Por isso, evite, se possível, esses equipamentos próximos do ponto de acesso.

ADVANCED SETTINGS

Esse item do menu está relacionado à configurações avançadas, que irão interferir diretamente no funcionamento da rede sem fio. No geral, não é necessário alterar essas configurações para que a rede funcione, e, jamais modifique alguma coisa se não tiver certeza do que está fazendo. A seguir comentamos os parâmetros mais comuns.

Authentication Type

É o tipo de autenticação. As opções são Open System (Significa “Chave Compartilhada”. Não irá usar criptografia), Shared Key (Significa “Chave Compartilhada”. Utiliza uma chave estática WEP 64/128 bits. Receptor e transmissor compartilham a chave de segurança) e Auto (Faz seleção/detecção automaticamente). Sugestão: deixe em Auto;

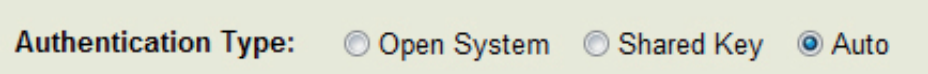


Figura 05.6: Authentication Type.

Fragment Threshold

Configura o limite de fragmentação. Serve para configurar o tamanho máximo, em bytes, que será o limite a ser enviando (dados) sem ocorrer fragmentação. Acima do valor indicado, ocorre a fragmentação dos dados, onde ele passa a ser enviado em vários pacotes menores. Na dúvida, deixe o valor 2346, que é o padrão.

Figura 05.7: Fragment Threshold. O valor entre parênteses é o máximo e mínimo permitido.

RTS Threshold

O padrão, geralmente, é que esse valor seja maior que o Fragment Threshold. De qualquer forma, observe que na própria página de configuração há os valores recomendados (e os permitidos de serem configurados).

Figura 05.8: RTS Threshold. O valor entre parênteses é o máximo e mínimo permitido. Observe que o valor mínimo permitido é maior que o valor máximo do parâmetro Fragment Threshold.

Esse parâmetro serve para configurar o valor máximo, que ao ser ultrapassado irá ocorre a requisição de RTS (Request-to-sent) e CTS (Clear-to-send). Ele serve para resolver o problema de estações que conseguem enxergar o AP, mas, não enxergam outras estações.

Funciona assim: sempre que uma estação (qualquer uma) iniciar uma transmissão, antes, ocorre o envio de um pacote RTS ao AP, que é uma solicitação para ocorrer a transmissão. Estando tudo pronto para a transmissão, o AP retorna um pacote CTS, e a transmissão de dados será iniciada. Esse sistema só será utilizado se o tamanho do pacote exceder o valor especificado;

Beacon Interval

Ajuste de Intervalo de marcação. É um pacote enviado a todos os dispositivos da rede para indicar a sua disponibilidade bem como sua celeridade. É usado pelo AP para sincronizar a rede.

O valor indicado representa milissegundos (ms), e indica de quanto em quanto tempo será enviado o “pacote beacon”. O valor padrão é 100, e no geral pode-se usar valores de 20-1024 ms.

Figura 05.9: Beacon Interval.

ACK Timeout

ACK é uma forma reduzida de acknowledge, que em uma rede, é um sinal de confirmação. Basicamente, é o tempo de espera de um pacote.

Suponhamos que um AP esteja aguardando o recebimento de um pacote de um nó qualquer. Se for recebido dentro do tempo limite, ele envia um sinal de confirmação do recebimento. Caso não receba, ele ficará aguardando. Caso o tempo seja “estourado”, o AP não irá mais aceitá-lo.

Figura 05.10: acknowledge Timeout.

Por isso, deve se ter cuidado ao configurar esse item. Valores altos farão o AP aguardar um tempo desnecessário (caso o pacote não seja enviado), e valores muito baixos o farão “desistir” rápido demais (antes mesmo do pacote ser entregue por completo).

Para distância pequenas (uma rede em uma ou duas salas, por exemplo), você pode deixar o valor padrão, que é 0 (zero). Para distâncias maiores (imóveis interligados, por exemplo, ou se a rede começar a ter problemas de comunicação, coloque um valor que pode ser no máximo 255.

Client Expired Time

É o tempo de expiração de um cliente. Configura um tempo (em segundos) que um cliente pode ficar ocioso (sem atividade). Passado esse tempo, o AP irá desconectá-lo.

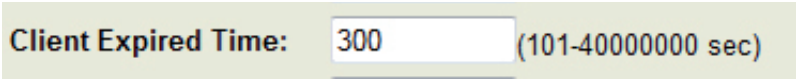


Figura 05.11: Client Expired Time.

MTU Size

MTU são siglas de Maximum Trasmit Unit (unidade máxima de transmissão). Aqui configuramos o tamanho dessa unidade. Basicamente configura o tamanho máximo do pacote ethernet (protocolo) que um microcomputador poderá enviar. O padrão é 1500 bytes.

Ao enviar um dado de um micro para outro, ele será dividido, pelo protocolo TCP/IP (muito usado em redes), em diversos fragmentos ("pacotes"), que serão re-montados no micro destino. O MTU é o maior tamanho possível que esses fragmentos podem ter, pra que possam percorrer todo o caminho até chegar ao destinatário.

Figura 05.12: MTU size.

Data Rate

É a velocidade de transmissão de dados na rede. Os valores são: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 38 e 54MB. O padrão é auto, e você deve deixá-lo, principalmente se a rede conter dispositivos do padrão IEEE 802.11b e IEEE 802.11g, por exemplo.

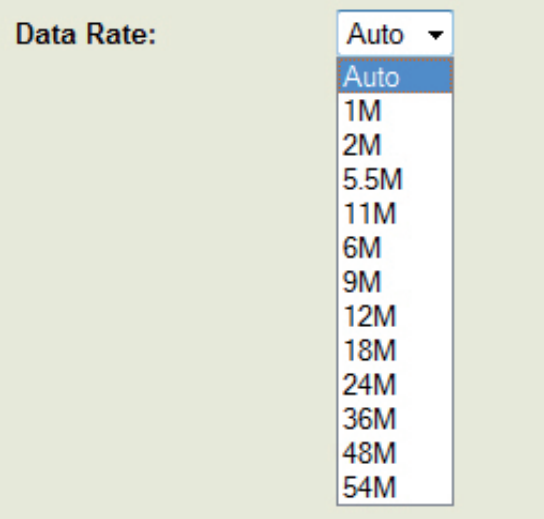


Figura 05.13: Data Rate.

Preamble Type

Defini o tipo de preâmbulo. Preamble é uma seqüência de bits, que durante a transmissão de dados, irá sincronizar emissor e receptor. Ele é necessário, pois, atua na detecção de erros. São duas as opções de configurações: Short Preamble (preâmbulo breve) ou Long Preamble (preâmbulo longo).

Quando usar cada um deles:

- **Long Preamble:** se a rede tiver muito tráfego; em ambientes com muita interferência; ou em casos de dúvida, selecione esse padrão;

Short Preamble: se a rede tiver um tráfego muito pequeno; em ambientes com o mínimo de interferência; quando haver na rede nós que utilizem uma interface wireless do padrão 802.11b, e se observado problemas de sincronização.

Figura 05.14: Preamble Type.

Broadcast SSID

Siginifica Emitir/Enviar SSID. Essa é uma opção interessante, e uma ótima dica de segurança. Se você deixar o Broadcast SSID desabilitado, o nome da rede sem fio não será enviado junto como o sinal e, dessa forma, não será exibido ao ser feito uma procurar por redes disponíveis.

Isso é indicado somente em ambientes onde os usuários são os mesmos, não mudam (nesse caso basta informar manualmente o nome da rede às pessoas autorizadas a ingressar nela). Lugares onde sempre há novas pessoas para usar a rede, como aeroportos, faculdades, etc, essa técnica não deve ser usada.

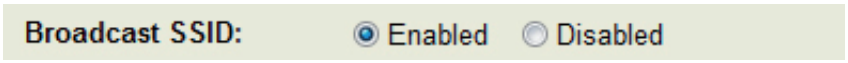


Figura 05.15: Broadcast SSID.

A configuração padrão é Enabled, onde o nome da rede é enviado. Para não enviar, basta escolher Disabled.

IAPP

IAPP são siglas de Inter-Access Point Protocol. É um protocolo coordenado por um grupo de empresas, cujo objetivo é garantir a interoperabilidade (podemos definir como a habilidade do hardware e/o software trabalharem em conjunto) entre equipamentos de fabricantes diferentes.

O protocolo IAPP defini como será a comunicação entre esses os pontos de acesso, permitindo o controle da comunicação entre os clientes (qualquer nó conectado à rede, cuja comunicação é mediada pelo(s) AP(s)) da rede.

A configuração padrão é Enabled, e é muito importante deixar dessa

forma, principalmente se na rede são usado equipamentos de diferentes fabricantes.

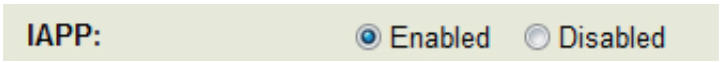


Figura 05.16: IAPP.

802.11g Protection

Esse item é importante em redes que tenha usuários que usem interfaces do padrão IEEE 802.11b e IEEE 802.11g. O padrão IEEE 802.11g possui um mecanismo de segurança que garante o funcionamento de redes sem fio nessas condições, sem que haja interferências/erros entre os usuários IEEE 802.11b e IEEE 802.11g.

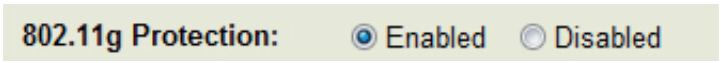


Figura 05.17: 802.11g Protection.

Block WLAN Relay

Configuração que permite isolar os clientes. Através dessa função é possível bloquear pacotes entre clientes se fio. Isso quer dizer que será impedido que os clientes se vejam, se comuniquem diretamente entre si. A configuração padrão é Disabled, onde os clientes poderão “conversar” um com outro. Se escolher Enabled, isso não será permitido.

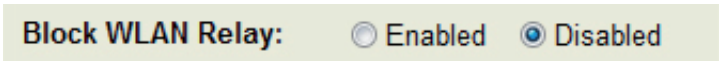


Figura 05.18: Block WLAN Relay.

Turbo Mode

O modo tudo permite uma transferência de dados que ultrapassa os 54Mbits/s, chegando aos 108Mbits/s. Mas, para que ocorra esse aumento,

de fato, é necessário que as interfaces (que devem ser do padrão 802.11g) envolvidas tenham esse modo embutido, ou seja, devem dar suporte a ele. Além disso, ao usar esse modo, ocorre uma drástica diminuição da área de cobertura da rede.

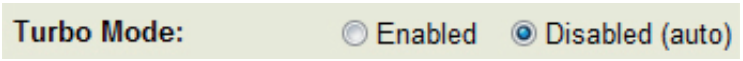


Figura 05.19: Turbo Mode.

Transmit Power (OFDM) e Transmit Power(CCK)

Através dessas configurações podemos ajustar a potencia do sinal de acordo com a distância do receptor.

OFDM são siglas das palavras em inglês Orthogonal Frequency-Division Multiplexing, e, CCK são siglas de Complementary Code Keying. Ambos são técnicas de modulação.

A modulação nada mais é que uma técnica, uma forma de inserir as informações (que são transportadas na rede) no sinal de radiofreqüência. Explicando de forma simples, é a modulação que defini como transportar os nossos dados, pela rede, usando as ondas de rádio. Ela permite que permite que estas informações/dados sejam transportadas inseridas nos parâmetros de amplitude, freqüência ou fase da portadora.

Modulação não é uma técnica empregada somente em redes sem fio. Em qualquer sistema de transmissão de dados, haverá algum tipo de modulação sendo empregado. Não existe somente esses dois tipos (OFDM e CKK), e sim vário tipos (técnicas) de modulação, onde citamos:

Modulações em fase:

- **PSK:** Phase Shift Keying;
- **QPSK:** Quadrature Phase Shift Keying;
- **DQPSK:** Differential QPSK.

Modulação em amplitude:

- **QAM:** Quadrature Amplitude Modulation;

Modulações em Freqüência:

- **FSK**: Frequency Shift Keying;
- **GFSK:** Gaussian Frequency Shift Keying.

Espalhamento Espectral:

- **DSSS:** Direct Sequency Spread Spectrum;

Existem várias outras técnicas de modulação, mas, citamos somente essas apenas para enriquecer a obra. Caso tenha se interessado pelo assunto, procure na própria Internet. Vá ao site Google (www.google.com.br) e procure por modulação, "técnicas de modulação" ou “modulation techniques”. Ficará surpreso com a quantidade de informação disponível.

De acordo com diversas literaturas técnicas, a OFDM é uma modulação em freqüência, o que dá pra perceber até pelo nome (Orthogonal Frequency-Division Multiplexing), enquanto a CCK é uma técnica de Espalhamento Espectral.

O OFDM possui a propriedade de dividir a transmissão de um sinal em vários sub-canais ortogonais entre si, garantindo que não haja interferência entre eles. Cada um desses sub-canais utiliza uma freqüência diferente e transporta apenas alguns bits do sinal original. Isso garante uma alta taxa de transmissão e resistência a interferências.

A técnica de modulação CCK é uma variação da CDMA (Code Division Multiple Access). O CDMA é uma técnica de multiplexação empregada em telefonia móvel. Basicamente, o CKK trabalha com a variação do sinal para decodificação da informação. Pode ser empregada para altas taxas de bits.

Não iremos nos aprofundar muito nas técnicas de modulações, pois, isso fugiria do escopo desta obra (isso é um assunto para estudantes de engenharia elétrica, por exemplo). Vamos voltar agora aos assuntos mais

práticos (e voltar ao tema do livro, que é montagem de redes wireless), e falar sobre as configurações possíveis de serem feitas em seu AP. Iniciemos explicando o que significa as siglas dbm na frente de cada parâmetro.

As siglas dbm está relacionada com uma medida muito importante, o decibel (dB). Explicando de forma bem simples, o decibel é uma unidade que pode ser usada para medições em acústica, física e eletrônica. As suas medidas são de forma relativa, algo semelhante a porcentagem (%).

Uma grande aplicação do decibel está em sua vida todos os dias, o tempo todo: a intensidade de um som.

Já o dBm siginifica dB miliwatt. É uma forma de medida absoluta. 0 (zero) dBm é definido como 1mW (mili watts) de potência. É uma medida usada comumente para expressar a potência de um equipamento de transmissão, que é o caso do AP.

Existe uma equivalência entre dBm e a potência de transmissão. Veja alguns exemplos:

- 5 dBm = 32 mW;
- 16 dBm = 40 mW;
- 17 dBm = 50 mW;
- 18 dBm = 63 mW;
- 19 dBm = 79 mW;
- 20 dBm = 100 mW;
- 21 dBm = 126 mW;
- 22 dBm = 158 mW;
- 23 dBm = 200 mW;
- 24 dBm = 250 mW;

- 25 dBm = 315 mW;
- 26 dBm = 400 mW;
- 27 dBm = 500 mW;
- 28 dBm = 631 mW;
- 29 dBm = 794 mW;
- 30 dBm = 1 Watt;
- 40 dBm = 10 Watts;
- 50 dBm = 100 Watts;
- 60 dBm = 1000 Watts.

Para aumentar a área de cobertura de uma rede sem fios, uma das alternativas é aumentar a potência de transmissão. Mas, isso pode causar aumento temperatura do AP. Por isso, sempre que configurar esse item, aumentando a potência, observe se realmente houve aumento da cobertura da rede, se o AP está aquecendo muito (o que pode provocar seu travamento) e veja se o resultado final vale à pena.

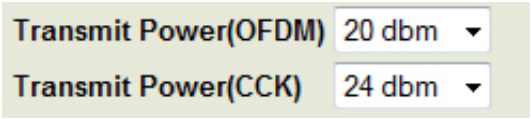


Figura 05.20: Transmit Power (OFDM) e Transmit Power(CCK).

SECURITY

Vamos agora abordar um tema de grande importância em sua rede: a segurança. Há duas formas principais de se configurar técnicas de segurança na rede. A primeira é através do uso de criptografia e chave de acesso. A segunda é configurando o firewall, que é abordado no capítulo 07.

As configurações de criptografia e chave de acesso à rede ficam, geralmente, em um link Security (na seção Wireless). Caso o caminho para se chegar a esses itens seja diferente, em seu AP, basta dar uma procurada rápida e você irá encontrá-la facilmente. Elas visam dar proteção à rede contra o acesso de pessoas não autorizadas.

Figura 05.21: Wireless Security Setup no AP Zinwell Zpluz G220.

Como podemos perceber na imagem 05.21, a primeira opção é a Authentication Type, já explicada neste capítulo (ver anteriormente).

WEP, WPA (TKIP), WPA2 (AES) e WPA2 Mixed

Em Encryption, selecionamos o tipo de criptografia a ser usado. As opções são: None (não utiliza nenhuma criptografia), WEP, WPA (TKIP), WPA2 (AES) e WPA2 Mixed. Vejamos o que significa essas letrinhas:

- **WEP:** Wired Equivalent Privacy;
- **WPA:** Wi-Fi Protected Access;
- **TKIP:** Temporal Key Integrity Protocol;
- **AES:** Advanced Encryption Standard.

O padrão de encriptação WEP é um dos primeiros que se tem notícias a ser usado em redes sem fio, sendo parte do padrão IEEE 802.11 (portanto, são usados por produtos desse padrão) que foi validado em 1999. Apesar de ser muito usado até os dias de hoje, principalmente em uma tentativa de se manter compatibilidade entre todos os nós, ele possui muitas vulnerabilidades e falhas, o que permite que hackers façam ataques bem sucedidos à rede, captura de mensagens e até autenticação na rede.

Graças a todas essa falhas e vulnerabilidades, foi criado (em 2003) o WPA, como forma de corrigir todas as falhas do WEP e permitir uma maior segurança da rede. Desse modo, ele é na verdade um WEP melhorado. Tanto que ele pode ser chamado por WEP2, e portando, se referem a mesma coisa, que é a primeira versão do WPA. No geral, pode-se usar o WPA em redes que possuam WEP. O mecanismo para a criação de chaves de cifra dinâmicas e para a autenticação é o TKIP.

Já existe a segunda geração do WPA, chamada de WPA2, e que possui um nível de segurança ainda maior, o suficiente para ser usado, por exemplo, por organismos governamentais, onde o nível de segurança deve ser muito elevado. Isso graças ao AES, que é mecanismo para a criação de chaves de cifra dinâmicas e autenticação. Ele é compatível com produtos que suporte o WPA.

Ao configurar o padrão de encriptação, observe se há a opção WPA2 Mixed. O que ela faz é combinar TKIP com AES, permitindo que dispositivos que utilizem o padrão WPA possa se comunicar com dispositivos que utilizem o padrão WPA2.

Se escolher o padrão WEP, o próximo passo é criar as chaves de acesso, bastando para isso, no nosso exemplo, clicar no botão Set WEP Key.

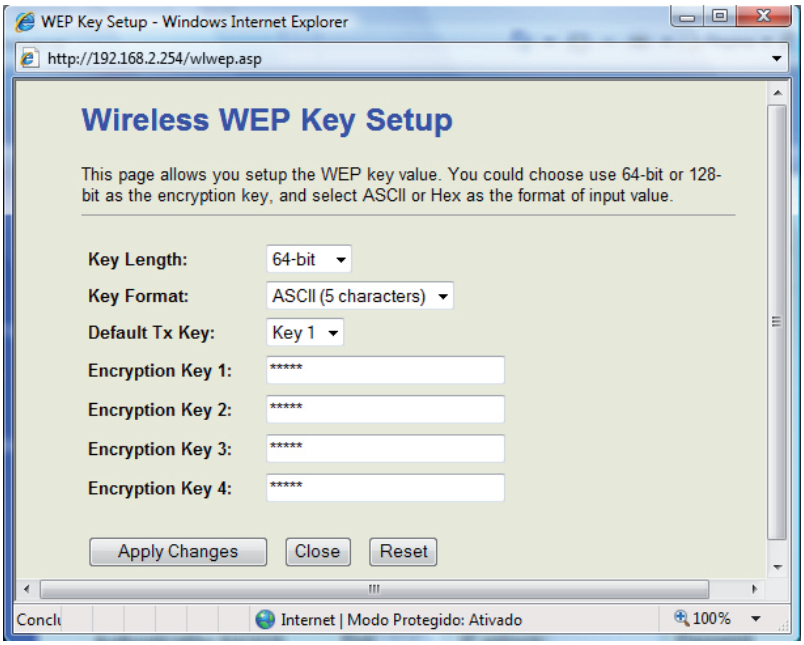


Figura 05.22: Wireless WEP Key Setup. Aqui, configuramos a chave de acesso.

Em Key Length (Comprimento da chave) você deve definir o modo de criptografia, que pode ser de 64 ou 128 bits. Isso terá efeito direto no tamanho da chave:

- **64 bits:** 5 caracteres alfabéticos ou 10 números hexadecimais;
- **128 bits:** 13 caracteres alfabéticos ou 26 números hexadecimais.

Em Key Format definimos o formato da chave: caracteres ASCII (qualquer caractere disponível no teclado, de acordo com a tabela ASCII) ou Hexadecimal (A, B, C, D, E, F, 1, 2, 3, 4, 5, 6, 7, 8, 9 e 0).

No campo Default Tx Key você deve definir qual a chave será a padrão, a que será utilizada normalmente. Observe que você pode digitar até quatro chaves (não é obrigatório digitar as quatros, basta digitar uma).

Nos campos seguintes (Encryption Key 1, Encryption Key 2, Encryption Key 3 e Encryption Key 4) você deve digitar as chaves. Ao terminar, clique em Apply Changes.

Se escolher o padrão de encriptação WPA (TKIP), WPA2 (AES) ou WPA2 Mixed, escolha, em WPA Authentication Mode (Modo de autenticação WPA), o modo Enterprise (RADIUS) ou Personal (Pre-Shared Key).

Se escolher o modo Personal (Pre-Shared Key), você pode digitar a chave no campo Pre-Shared Key. Mas antes, defina o formato da chave em Pre-Shared Key Format:

- **Passphrase:** combinação de letras, caráter de pontuação e números. Pode-se usar uma seqüência de palavras e textos. No geral, é permitido o uso de senhas contendo de 8 a 63 caracteres ASCII;
- **Hexadecimal:** 64 caracteres.

Já a opção Enterprise (RADIUS), é um método onde será utilizado um servidor RADIUS que é um tipo de servidor que irá executar a autenticação e ingresso dos usuários na rede. Ele também permite maior controle e gerenciamento dos usuários. Ao escolher esse modo, digite no campo Port a porta de autenticação com o servidor (o padrão é 1812), em IP address o IP do servidor e em Password a senha de autenticação com o servidor.

ACCESS CONTROL

Quando se fala em Access Control (controle de acesso) estamos nos referindo à possibilidade de controlar o acesso dos usuários à rede. Esse controle, geralmente, se resume a permiti ou não que um (ou mais de um) usuário acesse a rede, ou seja, permitir ou bloquear a sua entrada.

O processo é simples, bastando informar o número MAC do usuário e definir se queremos negar ou permitir sua entrada à rede.

O número MAC (Media Access Control), que pode ser chamado de MAC Adress (Endereço MAC) é um código hexadecimal único, que cada interface de rede possui. Não existem dois números MAC iguais. Por isso, ele é o endereço físico da interface de rede.

É um endereço de 48 bits. Exemplo de um MAC Adress:

00:0e:2e:50:97:5f

Vejamos como bloquear o acesso de um determinado usuário à rede. A primeira providência a tomar é descobrir o seu MAC Adress. Isso pode ser feito através do próprio "Web-Setup" do AP. No modelo que estamos usando como base, basta ir em Basic Settings (na seção Wireless) e clicar no botão Show Active Clients (Mostrar clientes ativos).

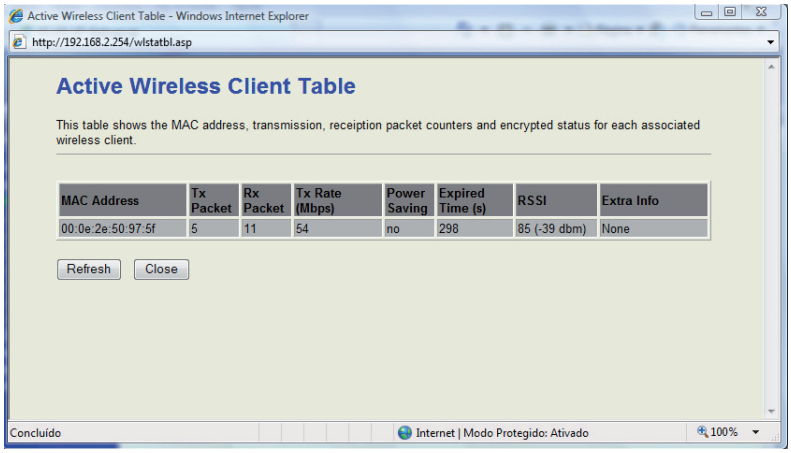


Figura 05.23: Active Wireless Client Table. No momento há somente um cliente ingressado na rede, cujo MAC Adress é 00:0e:2e:50:97:5f.

Uma vez com o MAC Adress anotado, basta ir à página Access Control. Em Wireless Access Control Mode (Modo de controle do acesso à rede sem fio), escolha a opção Deny listed (Negar enumerados). Em Comment (comentário) você pode digitar algum comentário, como um lembrete do motivo pelo qual o usuário em questão está bloqueado, por exemplo. Em MAC Address, digite o endereço MAC anotado no passo anterior. Mas atenção: digite-o sem usar os ":" (dois pontos). No nosso exemplo (00:0e:2e:50:97:5f), deve ser digitado da seguinte forma: 000e2e50975f. Feito isso, clique no botão Apply Changes.

A partir desse ponto, o usuário em questão não conseguirá se ingressar na rede, não importando se há ou não configurado nela algum tipo de criptografia e chave de acesso.

Figura 05.24: usuário bloqueado.

Voltando à opção Access Control Mode, devemos usar a opção Allow listed (permitir enumerados) quando desejamos permitir o acesso de algum usuário (que tenha tido o acesso previamente bloqueado) à rede novamente. Basta selecionar o usuário na lista, escolher Allow listed e clicar em Apply Changes.

WDS SETTINGS

Como sabemos, o modo WDS é configurado quando o objetivo é usar o AP como um repetidor de sinal. Como também já foi dito, quando ele é configurado dessa forma, é necessário também clonar o MAC Adress do AP principal (além ambos estarem configurados para utilizar o mesmo canal - Channel Number).

É exatamente nessa página (WDS settings) que configuramos o AP em que será repetido o sinal. Lembrete: só é possível fazer esses ajustes se o AP já estiver configurado para o modo WDS.

Inicialmente, você precisa saber o MAC do AP que iremos repetir o seu sinal. Para isso, ele deve estar na área de cobertura do repetidor (AP que vai ser configurado como tal). Isso pode ser conseguido até no próprio AP, pois, grande parte dos modelos disponíveis trazem essa informação em uma pequena etiqueta. Mas, outra opção é fazer um rastreamento, de redes ao alcance, no próprio AP que será repetidor.

No modelo que estamos usando como referência, basta clicar em Site Survey (na seção Wireless) e clicar no botão Refresh.

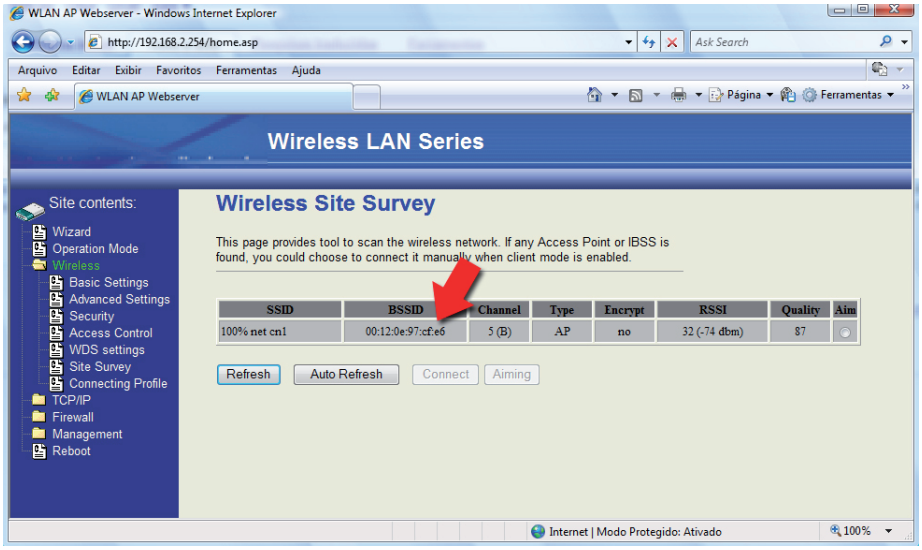


Figura 05.25: AP detectado. Veja o MAC Adress (no campo BSSID) do mesmo. Além dessa informação, há descrito os itens SSID (nome da rede), Channel (canal), Type (Tipo), Encrypt (uso de criptografia), RSSI (potencia do sinal) e Quality (qualidade do sinal captado).

Com o MAC Adress anotado, basta ir a página WDS settings. Ative (selecione) o item Enable WDS. No campo MAC Address digite o MAC, sem os ":" (dois pontos). No nosso exemplo, o MAC é 00:12:0e:97:cf:e6, logo, deverá ser digitado assim: 00120e97cfe6. Em Comment, digite algum comentário, se desejar. Para salvar e finalizar, clique em Apply Changes.

Figura 05.26: WDS Settings.

CONNECTING PROFILE

Ao configurar o AP no modo Wireless ISP (que é o modo utilizado para receber o sinal wireless de um provedor de acesso à Internet, ou seja, esse modo é usado para acessar a Internet), usamos a página Connecting Profile para configurar o AP (que é o AP da empresa. Ele é ligado a uma antena onidirecional) a que devemos nos conectar.

É importante ressaltar que o “AP Wireless ISP” deve estar configurado para o modo cliente. Caso contrário, não irá funcionar. Além disso, é necessário fazer todos os ajustes básicos, tais como os parâmetros de conexão com a Internet (Gateway padrão, Máscara de sub-rede, endereço IP, etc.). Tudo isso é abordado no capítulo 06.

Para configurar, você precisará do SSID e do BSSID (MAC Adress) do AP do provedor de acesso à Internet. Ele pode ser obtido tal como foi demonstrado anteriormente, na página Site Survey.

Com esses dados anotados vá à página Connecting Profile Settings. Ative

o item Enable connecting profile. No campo SSID, coloque o nome da rede. Em BSSID coloque o endereço MAC, sem digitar os ":" (dois pontos). Para confirmar, clique em Apply Changes. Feito isso, o AP do provedor irá aparecer na lista de preferência.

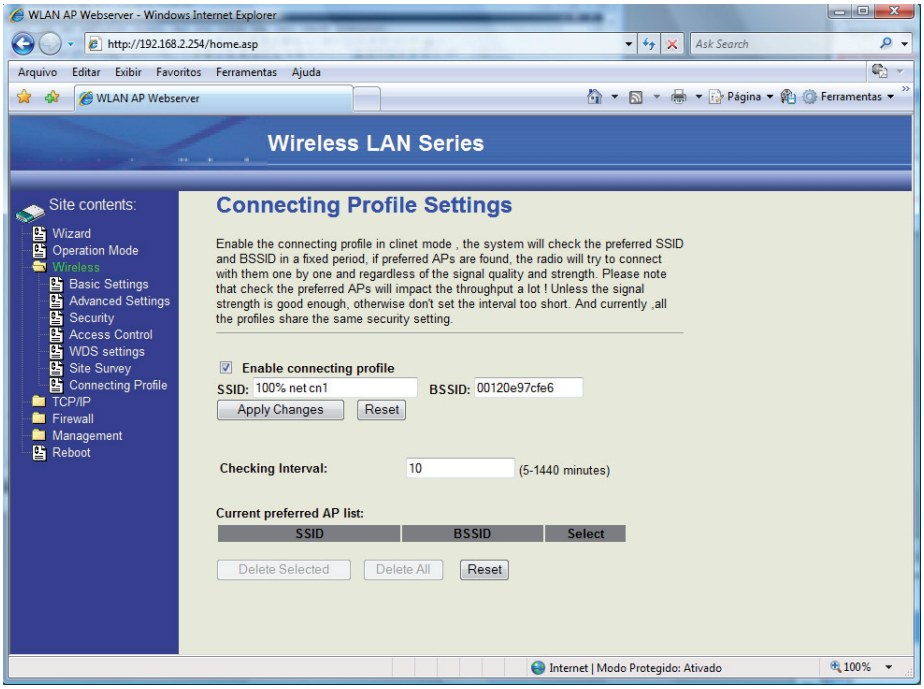
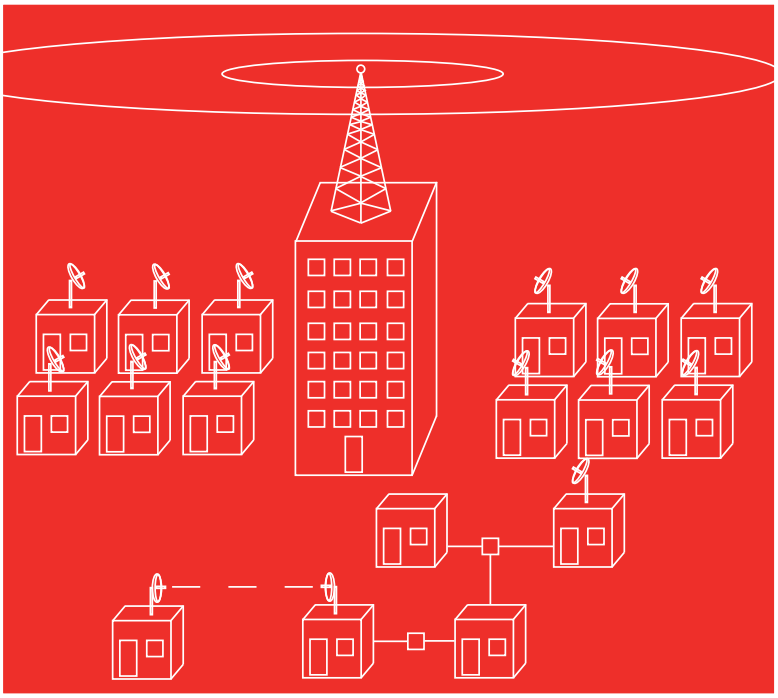


Figura 05.27: Connecting Profile Settings.



Capítulo 6 - Configurações de TCP/IP

PROTOCOLO TCP/IP

Quando se fala em TCP/IP, estamos falando de protocolos usados em redes de computadores. Mas, muitos de vocês podem estar se perguntando: o que é um protocolo? Para evitar atropelos, antes de partir para explicações a respeito de TCP/IP, é necessário entender perfeitamente o que é um protocolo.

Consultando o dicionário, encontramos o seguinte significado para protocolo:

Protocolo

s.m. (gr. Protokollon).

1. Registro de atos públicos.

2. Formulário de regula os atos públicos.

3. Deliberação diplomática.

4. Conjunto das disposições de um tratado entre nações.

5. Conjunto de normas a serem observadas em cerimônias oficiais.

6. Fig. Formalidade, etiqueta.

Fonte: dicionário Larousse Cultural

De todos os significados, destacamos: Conjunto das disposições, Conjunto de normas, Formalidade e etiqueta. Iremos voltar a comentar alguns desses significados, e você entenderá o por quê deles poderem ser usados em nossa explicação.

Voltando às redes de computadores, vamos usar como exemplo a Internet (a maior de todas as redes). Como sabemos, ela é composta por milhares de computadores espalhados por todo o mundo. Existem computadores de plataformas diferentes (MAC, PC, etc) e com sistemas operacionais diferentes (Windows, Linux, FreeBSD, etc). Perceba que mesmo sendo

plataformas e sistemas operacionais diferentes, eles conseguem se comunicar um com outro.

Um usuário de um PC com Windows pode enviar um e-mail que passará por outros computadores (servidores) que podem ser de outra plataforma (como o Linux) e chegará ao destino, que é o computador do destinatário (que para ilustrar, digamos que seja um MAC).

Não importa a plataforma, sistema operacional ou até idioma do destinatário, ele conseguirá receber e ler o seu e-mail. E mais do que isso: podemos usar programas de comunicação instantânea (que nos permiti conversar através de áudio, vídeo ou texto, em tempo real, com outros usuários da Internet), abrir páginas web que estão hospedadas em servidores que nem sabemos qual plataforma, idioma ou sistema operacional usa, etc.

Poderíamos dizer que computadores de plataformas diferentes “falam” línguas diferentes. Por exemplo: poderíamos dizer que o MAC “fala” chinês enquanto um PC “fala” inglês. Se eles “falam” línguas diferentes, como é possível um se comunicar com o outro na grade rede? Isso só será possível se todos eles “falarem” em uma mesma linguagem. É nesse ponto que entra os protocolos. São eles que ditam todas as normas, disposições e regras para a comunicação entre computadores. É ele que controla e permite a conexão e comunicação ou transferência de dados entre dois computadores.

Portando, voltando a nosso hipotético exemplo, quando um MAC que “fala” o idioma chinês for se comunicar com um PC que “fala” o idioma inglês, ele não irá usar o idioma chinês ou o inglês, e sim a “linguagem” do protocolo, ou seja, ele seguirá as normas do protocolo.

Existem vários tipos de protocolos, onde citamos:

- **TCP/IP:** Transfer Control Protocol;
- **POP:** Post Office Protocol;
- **POP3:** Post Office Protocol version 3;
- **IMAP:** Internet Message Access Protocol;

- **IMAP4:** Internet Message Access Protocol version 4;
- **SNMP:** Simple Network Management Protocol.

O TCP/IP é o protocolo mais comum e mais usado em redes (inclusive na Internet). Ele é formado por um conjunto de protocolos. O próprio nome já nos remete a dois deles:

- **TCP:** Transmission Control Protocol (Protocolo de Controle de Transmissão);
- **IP:** Internet Protocol (Protocolo de Internet).

A arquitetura do TCP/IP é baseada em um modelo de camadas, sendo quatro ao total. A quarta camada é a mais próxima do usuário. E a camada mais baixa (primeira camada) é mais próxima da máquina. Veja na imagem 06.1 uma representação da arquitetura do TCP/IP.

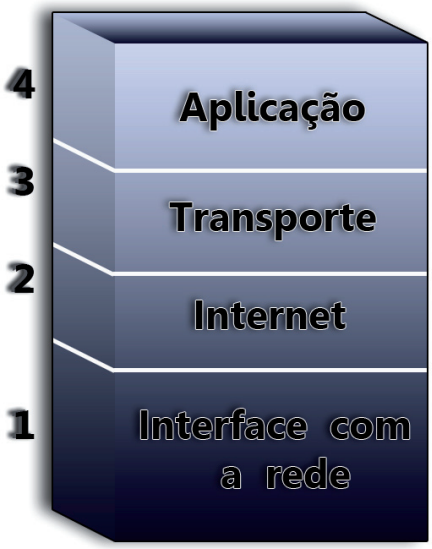


Figura 06.1: arquitetura TCP/IP.

Cada camada contém um determinado conjunto de protocolos. E cada camada possui uma função bem definida. Ou seja, cada camada irá pegar os pacotes de dados e fazer aquilo ao qual ela é programada para fazer. Ao terminar o "serviço", ela entrega o pacote para a camada logo abaixo, que também exerce uma função bem específica. Ao tratar os dados, ela, mais uma vez, envia o pacote para a camada seguinte (abaixo). Esse processo vai ocorrendo até o pacote ser enviado à rede, seja através de cabos ou do "ar". Perceba que acabamos de ilustrar um processo de envio de um pacote. Quando ocorre o recebimento de um pacote, ele deverá passar por cada camada (iniciando pela primeira, que é a Interface com a rede) até chegar ao programa do usuário (graças à camada aplicação).

Vejamos, finalmente, para quê serve cada camada e os protocolos mais comuns envolvidos:

- **Aplicação (Quarta camada):** essa é a última camada, e é ela que lida diretamente com os softwares do usuário. Por isso dissemos que ela é a "mais próxima do usuário", pois, é a camada que trabalha diretamente com o os softwares (como o Word, Excel, calculadora, jogos, etc, etc.). Portanto, aqui haverá protocolos de aplicação, ou seja, aqueles usados pelos programas. Exemplos: HTTP (Hypertext Transfer Protocol. É usado para transferir dados pela Web), SMTP (Simple Mail Transfer Protocol. Usado para envio de e-mails), FTP (File Transfer Protocol. Utilizado para transferência de arquivos a um servidor), entre outros;

- **Transporte (Terceira camada):** o protocolo da camada de aplicação irá pegar os dados requisitados pelo programa e enviar para a camada abaixo dele, que é a camada de transporte. É nesse estágio que os dados são divididos em vários pacotes ordenados, cujo conteúdo de cada um é verificado para se evitar erros. Um tipo de protocolo muito comum que atua nessa camada é o TCP (Transmission Control Protocol). É ele que é responsável em enviar os dados de forma correta, sem erros e na seqüência exata. Um outro tipo de protocolo que pode atuar nessa camada é o UDP (User Datagram Protocol). A diferença entre o TCP, é que o UDP prioriza a velocidade em liberar os pacotes. Não é realizado um controle tal como ocorre no TCP, e não é garantia de que os pacotes cheguem ao destino. Mas, devido ao seu modo de

funcionamento, ele é extremamente eficaz em vários setores. Exemplo: transmissão de áudio e vídeo ao vivo pela Internet;

- **Internet (Segunda camada):** uma vez cada pacote estando preparados, a camada de transporte os envia para a camada Internet. Nessa camada quem entra em ação é o protocolo IP (Internet Protocol) cuja função é adicionar em cada pacote recebido o endereço IP do computador que está enviando e o endereço IP do computador que vem receber. Então, ele trabalha com endereçamento. Feito isso, o pacote é enviado para a camada Interface com a rede;

- **Interface com a rede (Primeira camada):** essa é camada mais baixa (número 1). Ela irá preparar os pacotes, digamos em uma "linguagem de máquina". É ela que trata os dados para serem enviados para o meio de transporte, que pode ser cabos de fibra óptica (e portando, os dados devem ser transportados em meios luminosos), cabos de cobre (pulsos elétricos) ou até mês pelo "ar" (radio freqüência). Um tipo de protocolo muito comum que atua nessa camada é o Ethernet (na verdade, ele é um conjunto de protocolos, e possui três camadas: LLC - Controle do Link Lógico -, MAC - Controle de Acesso ao Meio - e Física. Não iremos entrar em detalhes a respeito desse protocolo, pois, o objetivo aqui é explanar somente o TCP/IP). Os pacotes a serem enviados pela rede, a partir daqui, recebem o nome de quadros.

LAN INTERFACE SETUP

Agora que já conhecemos o protocolo TCP/IP, vamos partir para a prática e abordar algumas configurações possíveis de serem feitas em um Access Point. Iniciemos pelas configurações dos parâmetros da rede local sem fio.

No menu do roteador Zinwell Zplus G220, encontramos a seção TCP/IP, que possui o link LAN Interface. Clicando nele chegaremos à página LAN Interface Setup (Interface de configuração da LAN).

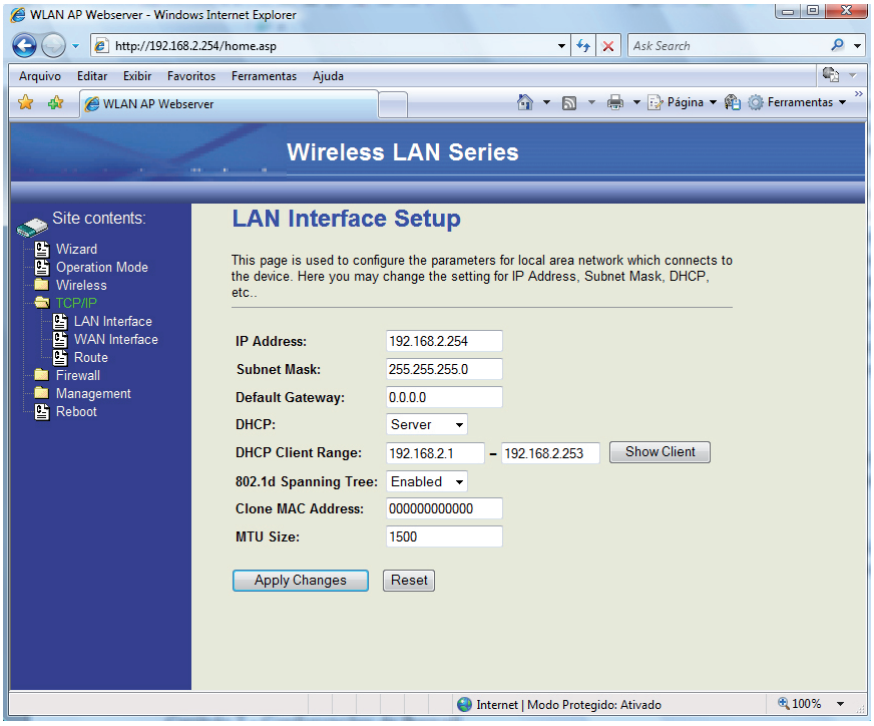


Figura 06.2: LAN Interface Setup.

Na seqüência abordamos os parâmetros disponíveis.

IP Address

A primeira opção é a IP Address (endereço IP). Através dela podemos configurar o IP do Access Point. Todo Access Point Possui um IP que vem configurado de fábrica. E é este IP que usamos para acessar o seu “Web-Setup”.

Acontece que podemos mudar esse IP. Use um IP na mesma faixa de IPs usada em DHCP Client Range (ver mais abaixo). Porém, o IP do AP é reservado somente para ele. Desse modo, reserve para o AP um IP que

esteja antes ou depois da faixa de IPs selecionada para o DHCP Client Range. Exemplo:

Reservado ao DHCP Client Range:

192.168.2.2 - 192.168.2.253

Desse modo, o IP do AP pode ser, por exemplo:

192.168.2.1 ou 192.168.2.254

Existe uma faixa de IPs que podem ser usadas em redes locais (sem fio ou não). Que são elas:

- **Classe A:** de 10.0.0.0 à 10.255.255.255;
- **Classe B:** de 172.16.0.0 à 172.31.255.255;
- **Classe C:** de 192.168.0.0 à 192.168.255.255.

Atenção: é preciso tomar muito cuidado ao local onde configura o IP do AP. Fazemos isso, no geral, na seção TCP/IP, na página LAN Interface, em Configurações da LAN, ou algo parecido.

O cuidado que se deve tomar é que você encontrará outros campos “IP Address” para serem configurados. Por exemplo: na página WAN Interface. Mas acontece que nessa página, o IP Address se refere ao IP fornecido pelo provedor de acesso à Internet, que geralmente é o IP de algum outro AP ou roteador, por exemplo.

Subnet Mask

Configura a máscara de sub-rede. Esse item deve ser configurado de acordo com a faixa de IPs usada no item anterior (IP Address). Cada faixa de IPs (classe) terá uma máscara de sub-rede que pode ser usada. Dessa forma, temos:

- **Classe A:** 255.0.0.0;
- **Classe B:** 255.255.0.0;

- **Classe C:** 255.255.255.0.

São sempre essas, e não podem ser trocadas. Se você usar uma faixa de IPs da classe A, a máscara de sub-rede deve ser 255.0.0.0, e não 255.255.0.0 ou 255.255.255.0.

Outro detalhe é que máscaras de sub-redes são formadas por apenas dois números: 0 e 255, apenas.

Default Gateway

Uma das definições para Gateway é aquele dispositivo usado para conexão com a Internet e que, compartilha e fornece esse acesso com outros computadores.

Esse dispositivo pode ser, inclusive, um microcomputador (que tenha acesso e compartilha o acesso à Internet).

Essa é a definição empregada em redes. Sempre que, ao configurar IP, servidor DNS, etc, e, for solicitado o 'gateway padrão', saiba que o que está pedido é o IP do dispositivo usado para prover acesso à Internet.

Se você possui um roteador para acessar à Internet banda larga (Velox, Speed, etc), é possível ligá-lo ao AP (na porta WAN) e compartilhá-la na rede sem fio. No campo Default Gateway, devemos informar o IP desse roteador.

O roteador, tal como o AP, possui um numero IP, que também é usado para acessar o seu "Web-Setup".

DHCP

DHCP são siglas de Dynamic Host Configuration Protocol. O que ele faz é configurar dinamicamente os endereços IPs de cada micro que entrar na rede. Dessa forma, não é necessário configurar manualmente os endereços IP (bem como máscaras de sub-rede) dos micros envolvidos.

Para que o AP funcione como um servidor DHCP basta selecionar a opção Server.

DHCP Client Range

Uma vez o AP configurado para atuar como um servidor DHCP, o próximo passo é definir a faixa de IPs que ele pode usar para os clientes que se ingressarem na rede.

Use a mesma faixa de IP usada em IP Address (IP do Access Point), respeitando o IP reservado ao AP.

Observe que em DHCP Client Range há dois campos. O primeiro você digita o IP inicial e no segundo o IP final. A partir daí o AP usará os IPs, dentro dessa faixa indicada, para fornecer aos clientes.

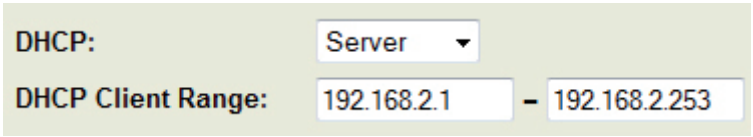


Figura 06.3: exemplo de configuração do AP como servidor DHCP.

802.1d Spanning Tree

O 802.1d Spanning Tree é um protocolo muito importante que deve ser habilitado quando sua rede tiver bridges/switches.

Uma de suas grande utilidade é trabalhar na definição dos melhores caminhos para a transmissão de dados na rede, atuando diretamente nos seguimentos separados por bridges ou switches. Isso evita que dados sejam transportados por caminhos com eficiência baixa (onde, por exemplo, a entrega dos dados será mais demorada), ou pior, que os dados fiquem em um processo chamado de loop (fica “dando voltas”), onde eles ficam sendo transportados sem conseguir chegar ao destino, o que acaba congestionando a rede. Essa situação pode acontecer principalmente porque muitos APs podem integrar redes sem fio com cabeada (ou seja, eles possuem a função de hub/switche).

Figura 06.4: 802.1d Spanning Tree habilitado.

Clone MAC Address

Através dessa opção, podemos copiar o MAC Adress de outro dispositivo. Suponhamos que você vai ligar um roteador na porta WAN do AP para compartilhar a Internet banda larga através da rede sem fio. É necessário digitar nesse campo o MAC do roteador, sem usar os ":" (dois pontos).

Essa opção também está presente em todos os tipo de acesso WAN: Static IP, DHCP Client, PPPoP e PPTP.

WAN INTERFACE

Só é possível configurar os parâmetros da seção WAN Interface quando o AP estiver no modo Router ou Wireless ISP.

Nessa página configuramos os parâmetros da Internet que está chegando ao AP, seja uma banda larga ADSL (um cabo ligado à porta WAN. O AP deve suportar o modo router) ou através do recebimento da Internet através de ondas de rádio (Wireless ISP). Isso quer dizer que não importa se a internet chega através de cabos ou por uma rede wireless, é nessa página que iremos configurar o AP para receber o sinal e distribuí-lo entre os usuários, via cabo (no caso do Wireless ISP), sinal de rádio ou ambos (no caso de receber a Internet via porta WAN).

E se você ligar um roteador ADSL na porta WAN, também pode usar essa página para configurá-lo. Mas, qual a vantagem de usar o AP em modo router, recebendo o sinal da Internet de um outro router pela porta WAN? A resposta é muito simples: quando o seu objetivo for apenas distribuir a Internet via ondas de rádio para um determinado grupo de clientes, sem que eles possam se comunicar diretamente entre si.

WAN Access Type

Aqui selecionamos o tipo de acesso WAN. Por exemplo: suponhamos que você utilize conexão ADSL. Nesse caso você deverá escolher o tipo de acesso PPPoE.

Ao escolher um determinado tipo de acesso, haverá logo abaixo todas os parâmetros específicos do tipo em questão, que devem ser configurados. Vejamos, na seqüência, um resumo de cada um.

Static IP

Esse modo pode ser usado, por exemplo, quando você configurar um cliente Wireless ISP.

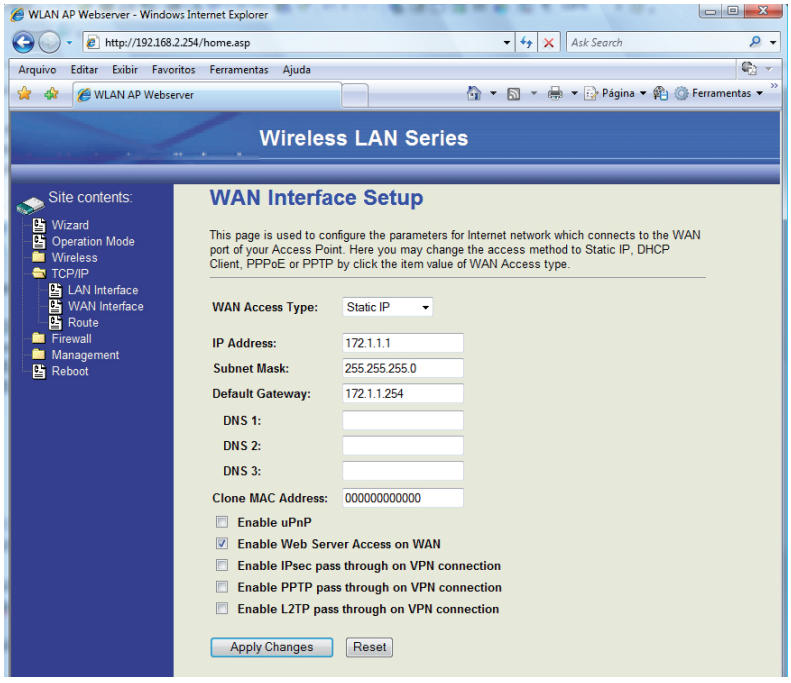


Figura 06.5: configurações de Static IP.

Vejamos, passo a passo, para que serve cada parâmetro:

1 - IP Address: esse IP não é o IP do Access Point, e sim um IP fornecido pelo provedor de acesso à Internet e que o AP irá se conectar. É preciso ter muita atenção em cada tipo de configuração, pois, muitos técnicos menos experientes se perdem ao meio de tantas configurações. Se configurar deforma errada o AP não vai funcionar;

2 - Subnet Mask: é a máscara de sub-rede. Digite uma máscara de acordo com a classe de IPs usada em IP Address;

3 - Default Gateway: esse dado também é fornecido pelo provedor de acesso à Internet. É o IP do dispositivo que irá fornecer o acesso à Internet ao AP. Aqui é necessário fazer mais uma importante ressalva. Você não pode configurar, em um mesmo dispositivo, dois Gateway padrão. Caso contrário ele ficará simplesmente "perdido" e não funcionará. Desse modo, se tiver configurando uma WAN interface, não indique um Gateway padrão nas configurações da interface LAN;

4 - DNS: logo abaixo há os campos DNS (Domain Name System). Trata-se de um servidor que converte nomes em IPs e localiza websites na Internet. Quando você digita o endereço de um site no browser, os servidores DNS são responsáveis em localizar (pelo IP do site) onde ele se encontra, em qual servidor disponível na Internet. Esse dado também é fornecido pelo provedor de acesso à Internet;

DHCP Client

Já o modo DHCP Client fornece os IPs automaticamente. Também pode ser usado para configurar um Wireless ISP, desde que o provedor de acesso à Internet forneça suporte e isso.

No caso, deve ser digitado nos campos DNS o IP fornecido pelo provedor. Ou ativar a opção Attain DNS Automatically para que o servidor DNS seja detectado automaticamente.

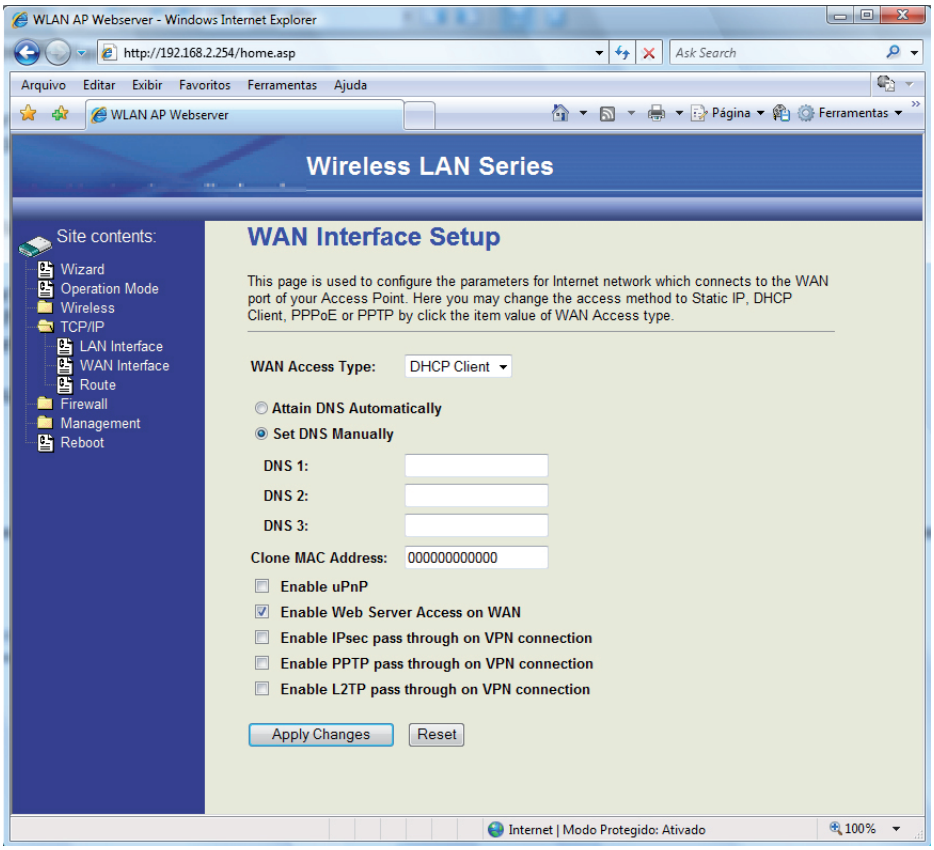


Figura 06.6: configurações de DHCP Client.

PPPoE

Essas siglas significam Point-to-Point Protocol over Ethernet. Esse protocolo é o mais usado para conexão de Internet banda larga (ADSL). É ele que estabelece a sessão e autenticação (através do fornecimento do nome de usuário e senha).

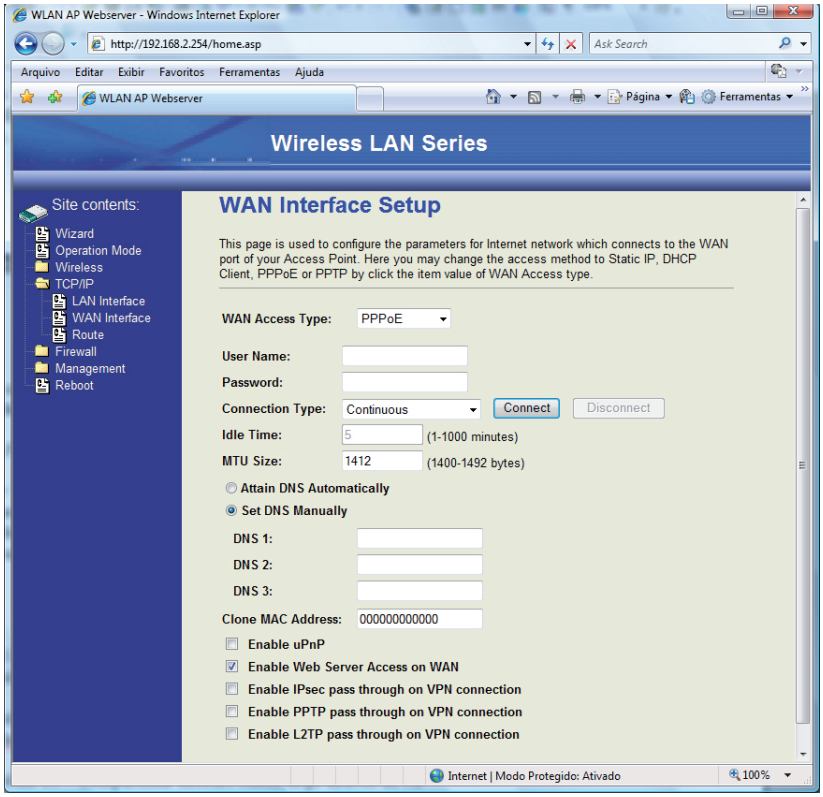


Figura 06.7: configurações de PPPoE.

Vejamos os principais parâmetros:

1 - User Name: nome de usuário criado pelo provedor de acesso à Internet;

2- Password: senha de acesso. Você já deve estar cadastrado em um provedor para ter esses dados;

3 - Connection Type: aqui define-se o tipo de ligação. As opções são: Contínuos (Modo Contínuo. Fica ligado permanentemente), Connect on Demand (Conecta de acordo com a demanda. Conecta automaticamente quando o usuário necessitar acessar à Internet) e Manual (o usuário conecta manualmente);

4 - DNS: configura um servidor DNS.

PPTP

PPTP são siglas de Point to Point Tunneling Protocol (Protocolo de Tunelamento Ponto a Ponto).

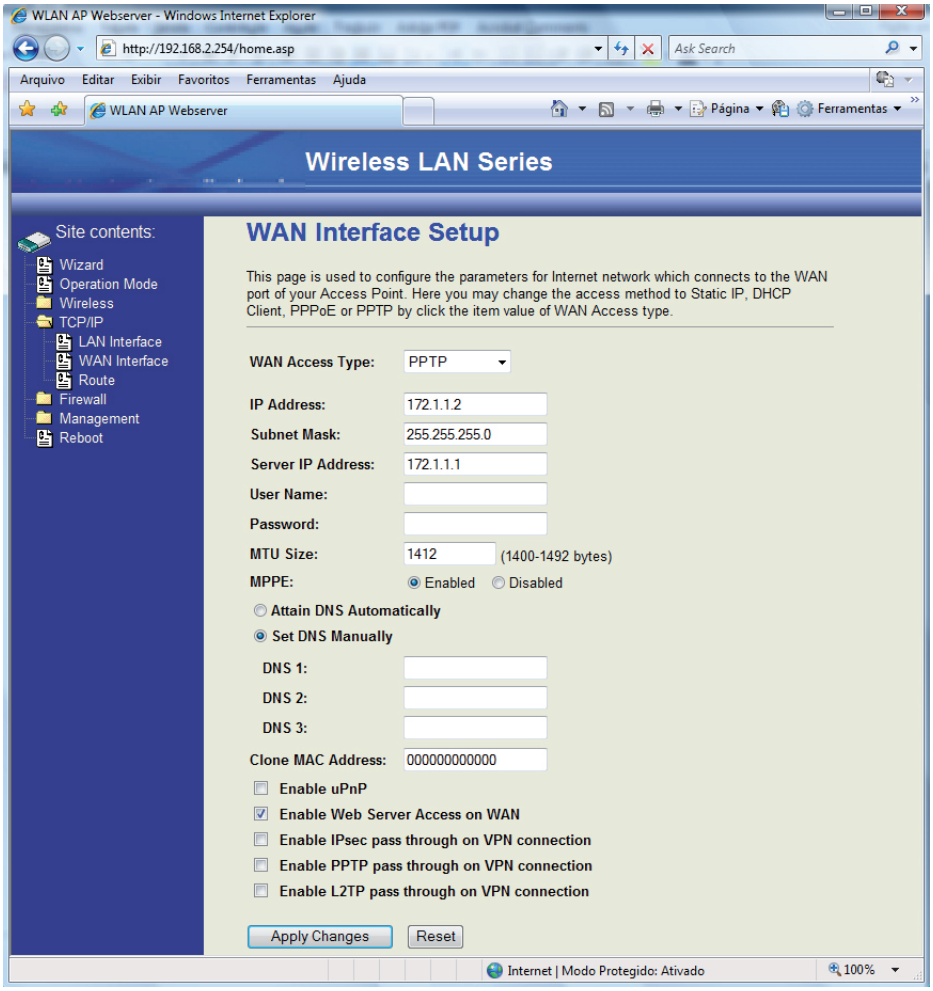


Figura 06.8: configurações de PPTP.

Todas as configurações citadas anteriormente, em PPPoE, são realizadas nesse tipo. A diferença é que, ao usar PPTP, haverá alguns parâmetros extras, onde citamos:

1 - IP Address: fornecido pelo provedor de acesso à Internet;

2 - Subnet Mask: de acordo com a faixa de Ips usada;

3 - Server IP Address: é o endereço do servidor PPTP fornecido pelo provedor.

ROUTING SETUP

É possível fazer ajustes nessa página somente se o AP estiver configurado para o modo Router ou Wireless ISP. Ela é usada para editar o protocolo de roteamento dinâmico ou editar rotas estáticas. O roteamento é um processo que objetiva definir qual será os melhores caminhos por onde será enviado os pacotes até que eles cheguem ao destino.

Existem dois tipos de roteamento usados pelos dispositivos roteadores:

1 - Roteamento estático: utiliza rotas fixas, definidas pelo administrador. Sua alteração requer intervenção humana;

2 - Roteamento dinâmico: são conhecidos também por adaptativos. São utilizados protocolos de roteamento que irá definir as rotas. Esses caminhos são atualizados/mudados dinamicamente, sempre que necessário.

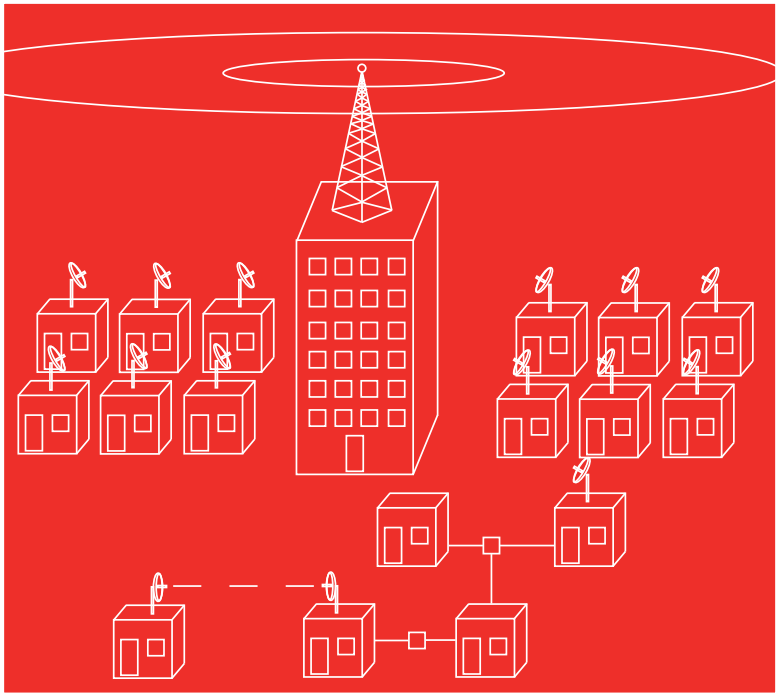
Ao acessar a página Routing Setup (na seção TCP/IP) você encontrará diversos parâmetros possíveis de se configurar. Entre eles, citamos:

1 - Disable NAT: a palavra NAT significa Network Address Translation. É um protocolo que garante o correto encaminhamento de pacotes da rede local à Internet. Não o desabilite;

2- Enable Dynamic Route: deve ser habilitado. É esse parâmetro que irá ativar o roteamento dinâmico;

3 - Enable OSPF Route: as siglas OSPF sigfinicam Open Shortest Path First. É um protocolo de roteamento criado para substituir o protocolo RIP (ver a seguir). Quando um roteador suporta os dois protocolos (OSPR e RIP), o que ganha em questão de preferência é o OSDF. Entre as vantagens, citamos que com esse protocolo a velocidade de convergência é muito maior. Além disso, ele possui a capacidade de escolher pelos caminhos que estão realmente funcionando, além de conseguir testar a comunicação com outros roteadores. Para usá-lo, você deve ativar o roteamento dinâmico (Enable Dynamic Route);

4 - RIP: são siglas de Routing Information Protocol. Também é um protocolo de roteamento, conforme dito, muito embora seja menos eficiente do que o OSPF. Só para citar um exemplo, e para que você entenda o porque dele ser menos eficiente, o protocolo RIP define o caminho a ser percorrido tendo como base a distância até o receptor, sem considerar as condições e desempenho desse caminho. Existe duas versões lançadas: RIP1 e RIP2.



Capítulo 7 - Firewall

O QUE É UM FIREWALL?

O firewall é um sistema de proteção aplicado a computadores e redes. Existe desde os firewalls pessoais (para proteção de um único computador) até os corporativos (para proteção de redes corporativas).

Ele é um mecanismo que atua entre a rede interna e a externa (qualquer outra rede ao qual ela está ligada, incluindo a internet), monitorando o tráfego de dados que entra e o que sai.

Dessa forma, ele protege a rede contra acessos não autorizados (invasão) de qualquer espécie (pessoas não autorizadas, vírus, trojans, etc), além de monitorar a saída de dados, como a tentativa de conexão efetuada por programas maliciosos que, porventura, esteja na maquina de algum usuário.

No caso de firewalls pessoais, ele atua diretamente entre o computador do usuário e a rede externa, que pode ser desde qualquer rede local ao qual ele está conectado até a Internet. Também monitora o tráfego de dados que entra e que sai. No caso dos dados que sai, estamos dizendo qualquer tipo de tentativa de conexão e/ou envio de alguma informação para redes externas. Se um programa não autorizado tentar se conectar com a Internet, por exemplo, o usuário é imediatamente avisado, ficando a seu cargo autorizar ou não tal conexão.

Perceba, dessa forma, que um firewall situa-se entre dois pontos (rede interna e externa), como se fosse um “escudo”, uma barreira, um “muro”. Inclusive, o próprio termo faz alusão a um tipo de parede que é usada, por bombeiros, em casos de incêndios, que é chamada de corta-fogo (firewall), para evitar o alastramento das chamas. Essa é a origem do nome firewall usado para proteger nossos computadores.

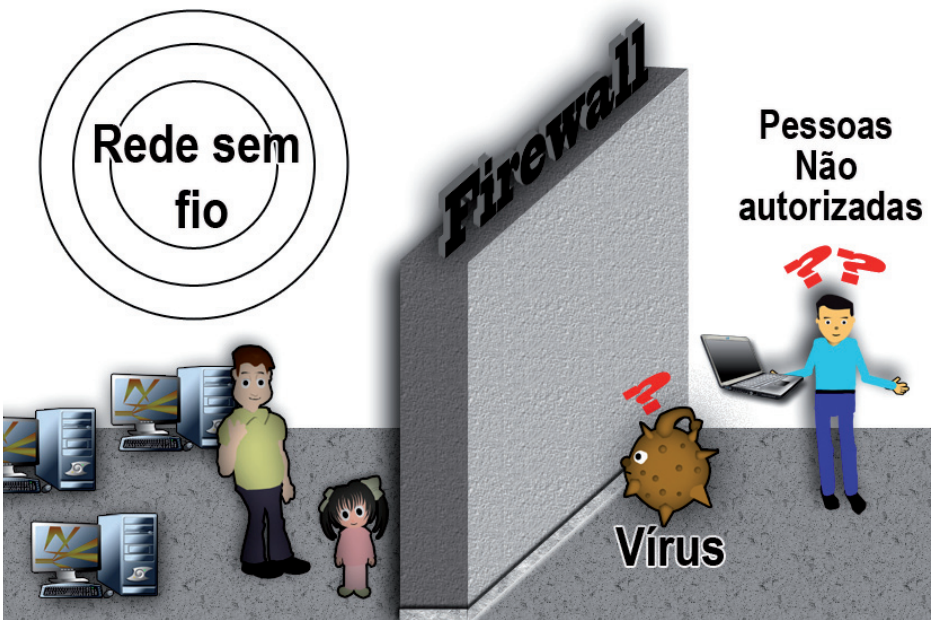


Figura 07.1: nessa imagem temos uma representação de um firewall. Observe que o muro impede que pessoas não autorizadas, vírus (e seus variantes) acessem a rede.

Tipos de firewall

Podemos classificar os firewalls em dois tipos bem definidos: os softwares e os hardwares.

Os instalados em um microcomputador, logicamente, são softwares. Existem aqueles que são destinados a proteção pessoal, já que ele estará agindo em um único computador. Existem também os firewalls que podem ser instalados em um servidor que ficará entre a e rede interna e a externa. Nesse caso, ele passa a proteger uma rede inteira.

Já os firewalls que classificamos como hardwares são dispositivos instalados na rede para prover a sua proteção. Eles possuem uma lógica interna, chamada firmware, que é um software que controla o dispositivo. Ele fica gravado em um chip ROM (memória ROM).

Qualquer Access point ou roteador que se preze possui um firewall embutido. Mais à frente, neste livro, veremos como configurar um firewall de um AP.

Modos de funcionamento

Quanto ao modo de funcionamento dos firewalls, podemos citar dois modos básicos:

- Filtragem de pacotes e;
- Controles de aplicações.

O primeiro modo (filtragem de pacotes) é muito usado em firewalls pessoais, em redes de pequeno ou médio porte. O que ele faz, basicamente, é decidir quais pacotes poderão entrar ou sair da rede. Também é sua função determinar quais computadores da rede poderá ou não se comunicar com a Internet ou outras redes.

Já o modo de controle de aplicações é mais complexo e robusto. São indicados para médias ou grades redes. Anteriormente dissemos que existem firewalls que podem ser instalados em um servidor, que é o caso desse tipo. Na verdade, ele é projetado para ser instalado somente em um servidor, que muitas vezes são chamados de proxy.

Por ser instalado em um servidor, ele irá intermediar a comunicação da rede interna com a externa. Qualquer tentativa de comunicação com uma rede externa deverá, obrigatoriamente, passar pelo firewall, caso contrário não há comunicação. Devido a esse fato, ele é muito mais eficiente do que os do tipo anterior, uma vez que, há um acompanhamento, filtragem e controle muito maior dos pacotes que circulam entre as redes.

Riscos de não usar um firewall

Os riscos que sua rede estará passando por não usar um firewall são vários. Mas, a razão maior de todas está relacionada com a segurança dos dados que circulam em sua rede.

Uma rede desprotegida pode ser alvo de hackers, que poderão capturar informações, comprometendo-as ou usando-as de forma maliciosa.

Ela pode ser alvo de vírus, cavalos-de-tróia, entre outras “pragas” virtuais. Um cavalo-de-tróia é um programa que entra no computador do usuário como algo “útil” e “inofensivo”. Por exemplo: uma animação qualquer, um joguinho, etc. Mas, ao ser ativado (aberto pelo próprio usuário), entra em ação a sua face nociva, agindo sem que o usuário perceba (pois, o grande truque do cavalo-de-tróia está no fato de que a animação ou o joguinho, citado como exemplo, irão funcionar normalmente. É apenas um disfarce, que inclusive, pode ser qualquer outro). Entre as coisas que ele pode fazer, citamos a captura de tudo aquilo que é digitado no teclado e o posterior envio dessa informação à Internet (para que o seu criador a receba).

Um firewall consegue bloquear portas que podem ser usadas por todas essas “pragas”, além de bloquear programas suspeitos.

Além da segurança dos dados, outro risco eminente é de pessoas não autorizadas conseguirem acessar a rede e obterem, a partir dela, acesso à Internet. A partir daí eles podem usá-la apenas para ter o acesso, de fato, ou pior, para iniciar ataques à partir de sua rede.

CONFIGURANDO O FIREWALL DE UM AP

Vamos deixar a teoria de lado e demonstrar como configurar um firewall de um Access Point. O texto a seguir se baseia no AP Zinwell Zplus G220, mas, você pode usar o que está explicado a respeito e cada parâmetro para configurar outros modelos.

Essas configurações são realizadas na seção Firewall do menu que se encontra à esquerda da página. Ao clicar sobre ele irá abrir o menu dessa seção, onde cada link o levará a uma página, onde é realizado um tipo de configuração bem específica. Leia a seguir o que podemos configurar em cada página e as funções de cada parâmetro.

Port Filtering

Nessa página configuramos o Filtro de portas. Ele faz um controle de todos os pacotes, e, quando ocorre alguma tentativa de conexão que busca uma porta que esteja configurada como bloqueada, a comunicação será impedida.

Figura 07.2: Port Filtering.

As portas de comunicação são “canais” que permitem a comunicação de programas e serviços com a rede (seja uma rede local, ou seja, a própria Internet). Todo e qualquer programa que deseja estabelecer algum tipo de comunicação em rede, precisa usar uma porta.

Vamos a um exemplo bem prático e talvez muito comum em seu dia-a-dia: a navegação na web. O protocolo usado para navegar na web é o HTTP. Desse modo, quando você abre o seu browser e digita no campo URL o endereço de algum site, o que irá acontecer nesse momento é que o browser irá se conectar na porta 80 no servidor HTTP onde a página se encontra. E por que a porta 80? Porque essa é a porta padrão para o protocolo HTTP.

Outro exemplo bem típico é a transferência de arquivos locais (que estão

no seu computador) para um servidor remoto. Isso pode ser feito usando o protocolo FTP (File Transfer Protocol - Protocolo de Transferência de Arquivos). Quando é usado um programa de FTP (AbleFTP, JaSFtp, Core FTP, WS_FTP Home, CoffeeCup Direct FTP, entre outros exemplos) para transferir arquivos para o servidor, ele se conecta com a porta 21 do servidor FTP.

Cada programa e/ou serviço utiliza uma determinada porta (que já é definida por padrão). Por isso é possível utilizar vários programas ao mesmo tempo acessando a rede ou a internet (browers, Chat, transferência de arquivos via FTP, etc.) sem que os pacotes enviados para cada um se percam no meio de tanta conexão, correndo o risco de um pacote ser enviado para o programa errado.

São 65.536 portas TCP e UDP que podem ser usadas. Apesar de cada programa ou serviço ser associado, por padrão, a uma determinada porta, elas podem ser mudadas (um programa ou serviço que utiliza uma porta “x” pode ser configurado para usar a porta “y”, por exemplo), muito embora isso envolva alguns ajustes que devem ser realizadas para que tudo funcione. A seguir listamos algumas portas para seu conhecimento:

- **21:** FTP;
- **22:** SSH;
- **23:** Telnet;
- **25:** SMTP;
- **42:** WINS;
- **53:** DNS;
- **80:** HTTP;
- **110:** POP3;
- **118:** SQL Services;

- **137:** NetBIOS Name Service;
- **147:** IMAP4;
- **143:** IMAP;
- **443:** HTTPS.

Para ver uma lista completa, visite o site: http://www.iana.org/assignments/port-numbers

Uma porta aberta é aquela que não está bloqueada, e pode ser um canal de entrada para programas maliciosos, como os vírus e trojans. Existem scanners de portas, que são usados, por pessoas que desejam invadir a rede, para rastrear e detectar portas abertas.

Mas, você não pode simplesmente sair bloqueando todas as portas de comunicação existente. Isso causará uma série de erros em diversos programas que usam a rede ou a Internet. Para que um dado programa ou serviço consiga se comunicar com rede ou a Internet, é preciso que a porta usada por ele esteja aberta.

Se você bloquear a porta 80, por exemplo, não será possível navegar na web. Nenhum browser conseguirá acessar as páginas da www.

É necessário que você tenha uma política de segurança e tente sempre estar um passo à frente de eventuais problemas que possam surgir. Veja um grande exemplo: é comum em redes corporativas o bloqueio de portas usadas por programas de chat, tais como o MSN (muito embora as versões recentes consigam se comunicar usando a porta 80, além de existir sites que podem ser usados para que as pessoas conversem com seus contatos do MSN, usando a web).

Resumo de portas usadas pelo MSN:

TCP 1863

UDP 1863

UDP 5190

UDP 6901

TCP 6901

Outra conduta muito aplicada é o bloqueamento das portas usadas por programas P2P (Peer-to-Peer), que são programas de compartilhamento de arquivos.

Quando algum usuário instala esses tipos de softwares, ele passa a ter acesso a programas, músicas, vídeos, e todo tipo de arquivo que estão em máquinas de outros usuários (que também possuam o mesmo programa instalado em seus computadores) ao redor do globo terrestre, formando uma espécie de “rede comunitária virtual”. E no geral, como o usuário passa a fazer parte da rede, ele também passa a oferecer esse tipos de dados (que estão em uma pasta pré-selecionada), para que outros usuários tenham acesso. Alguns exemplos:

KaZaA:

TCP 1214

UDP 3855

UDP 17437

TCP 3855

TCP 17437

Kazaa

TCP 1214

UDP 1214

TCP 3048

UDP 3048

Emule

TCP 4661

TCP 4662

TCP 4711

UDP 4672

UDP 4665

No caso dos programas de compartilhamento de arquivos (P2P), eles são uma das grandes portas de entrada para vírus e hackers. Por isso muitos administradores de redes sempre já possuem essa preocupação em bloquear as portas usadas por eles. Dessa forma, mesmo se algum usuário da rede instalá-los, eles não funcionarão.

Sempre ao bloquear alguma porta, procure observar se não ocorrerá algum problema na rede. Por exemplo: alguns programas não conseguirem se conectar na Internet, não enviarem e-mail, etc. Em caso de erros, basta desbloquear a porta e verificar se o erro persiste. Na própria Internet há muita informação das portas usadas pelos programas.

Bloqueando uma porta

Vejamos, passo a passo como bloquear uma porta:

1 - Na página Port Filtering, marque o item Enable Port Filtering (denied list) – Ativar Filtro de portas;

2 - Em Port Range, especifique a porta a ser filtrada. Observe que há dois campos (pra digitar) separados por um sinal de "-" ou "~". Basta digitar o numero dd porta duas vezes, uma em cada campo;

3 - Em Protocol, selecione o protocolo: as opções são Both (ambos), TCP ou UDP;

4 - Em Comment, você pode inserir um pequeno comentário. Pode ser, por

exemplo, um pequeno lembrete do motivo pelo qual a porta em questão está bloqueada;

5 - Para finalizar e salvar, clique em Apply Changes.

Logo abaixo você verá uma tabela com as portas que estão sendo filtradas. Se clicar em Delete selected, irá apagar a porta selecionada. Se clicar em Delete all, irá apagar todas as configurações realizadas.

IP Filtering

O filtro de IP é um recurso usado para impedir que usuários da rede interna, cujo IPs estão listados, não consigam obter acesso à Internet. Para que isso funcione, obviamente, o microcomputador do usuário deve usar IP fixo. Esse recurso não é muito seguro, quanto o filtro de endereço MAC (ver a seguir), uma vez que os próprios usuários podem modificar seu endereço IP.

Para configurá-lo, faça o seguinte:

1 - Na página IP Filtering, marque o item Enable IP Filtering (denied list) – Ativar Filtro de IP;

2 - No campo Local IP Address, digite o IP do usuário. Digite respeitando todos os pontos. Por exemplo: digite 192.168.0.2, e não 19216802;

3 - Em Protocol, selecione o protocolo: as opções são Both (ambos), TCP ou UDP;

4 - Em Comment, você pode inserir um pequeno comentário;

5 - Finalmente, clique em Apply Changes.

Logo abaixo haverá uma tabela com os IPs que estão sendo filtrados.

MAC Filtering

Esse filtro faz a mesma coisa que o IP Filtering, ou seja, impede o acesso dos usuários listados à Internet, porém, com uma eficiência muito maior.

Mas ele faz mais do que isso. Como ele bloqueia o endereço físico de uma interface (seja interface wireless ou placas de rede cabeada), qualquer dispositivo que tiver o MAC listado terá o acesso á Internet bloqueado.

Além disso, como o IP é um endereço lógico e facilmente configurável, o usuário poderá mudá-lo facilmente. Já um MAC Adress é um dado gravado em um chip ROM, que apesar de existir recursos para regrava-lo e mudá-lo, um usuário comum não conseguirá mudá-lo.

Para configurá-lo, siga os passos:

1 - Na página MAC Filtering, marque o item Enable MAC Filtering (denied list) – Ativar Filtro de MAC;

2 - No campo MAC Address, digite o MAC do usuário/dispositivo. Digite-o sem usar dos ":" (dois pontos). Por exemplo: se o MAC for 00:12:0e:97:cf:e6, digite 00120e97cfe6;

3 - Em Comment, você pode inserir um pequeno comentário;

5 - Clique em Apply Changes.

Logo abaixo haverá uma tabela com os MACs que estão sendo filtrados.

Port Forwarding

Port Forwarding em português significa redirecionamento de portas. Com este recurso é possível que usuários externos (da Internet) consigam acessar um computador de uma rede local que esteja atrás de um router. Isso quer dizer que, com esse esquema é possível estabelecer comunicação com um computador que está em uma rede local, partindo de qualquer ponto do mundo, usando a Internet.

Antes de continuarmos falando sobre Port Forwarding, é imprescindível abordamos alguns assuntos correlacionados: IPs privados e públicos e NAT.

Como sabemos, as redes internas usam IPs chamados "privados" (ou reservados, "não-roteáveis"). Eles não são válidos na Internet. Os IPs

reservados para Internet são os públicos (“roteáveis”). Um exemplo de IP público: 200.234.201.101.

O gateway (por enquanto vamos usar esse nome genérico, mas, saiba que pode ser router, AP, Firewall, etc) consegue um IP válido na Internet, devido a sua conexão com o provedor de acesso à Internet. É como se o provedor “emprestasse” um IP válido ao router, para que possamos nos conectar na Internet.

Mas, cada computador da rede ainda possui IP privado. Como fazer para que eles acessem à Internet? Isso é possível graças ao NAT (Network Address Translation), que é um recurso que deve estar habilitado no gateway.

O que o NAT faz, basicamente, é fazer um mapeamento onde consta o IP interno e a porta local do computador.

Dessa forma, quando um determinado pacote sair da rede interna para à Internet, ele terá um IP válido (que é o IP que o gateway pegou emprestado do provedor) e levará consigo uma referência a esta porta e IP. Quando o pacote chegar ao destino, o computador que receber saberá para onde retornar a resposta, pois, ele sabe o IP (que é um IP válido), e possui a referencia de quem enviou.

Por outro lado, se o computador de destino recebesse o pacote contendo como remetente o IP privado, usado pelo computador na rede local, ele simplesmente não saberia para onde enviar a resposta, pois, IPs privados não são usados na Internet, não existem, não são enxergados.

Explicando de forma mais simples, o que o NAT faz é pegar os pacotes oriundos da rede interna e deixá-los preparados para serem enviados pela Internet, de tal forma que sejam recebidos corretamente no remetente. Além disso, o remetente também terá total condição de enviar a resposta corretamente.

Cadê o Port Forwarding?

Como dissemos, esse recurso permite que um computador remoto se conecte a um computador dentro da rede local.

Essa conexão só é conseguida porque nós associamos, antecipadamente, no AP, portas de comunicação a endereços IPs. Por exemplo: podemos associar a porta 2133 ao IP 192.168.2.1, por exemplo. Desse modo, sempre que um computador externo “dizer” ao AP que ele quer se comunicar com a porta 2133, o AP “saberá” que ele deseja se comunicar com o computador cujo IP é 192.168.2.1.

Para que esse esquema funcione sempre, os computadores da rede interna devem usar IPs fixos, caso contrário será necessário mudar as configurações no AP a cada novo ingresso dos computadores à rede, o que é muito inviável.

Algumas observações:

- Só é possível usar esse recurso no dispositivo usado para prover o acesso à Internet. Isso que dizer que se você usa um AP, ele deverá receber diretamente o acesso a Internet (via ADSL ou Wireless ISP), ou, caso tenha um router ligado em sua porta WAN, ele (o AP) deve estar clonando o MAC do router, além de estar perfeitamente configurado e tendo acesso à Internet;
- NAT deve estar habilitado;
- Uma mesma porta não pode ser redirecionada para mais de um computador;
- Você pode associar várias portas a um mesmo endereço IP da rede local;
- Você precisa saber qual é a porta do aplicativo ou serviço que deseja oferecer.

Configuração na prática

Vejamos, então, como realiza a configuração na prática. Para exemplificar, vamos disponibilizar um servidor WEB, que está instalado em um computador de uma rede local, na Internet. Esse servidor é apenas fictício,

serve apenas para ilustrar o nosso exemplo. Para você colocar isso na prática, ressaltamos que o seu servidor WEB (ou qualquer outro serviço) deve estar perfeitamente configurado e funcionando na rede local.

Usaremos a porta 80 (TCP), pois, como já foi dito, essa é a porta usada para navegação na Web. O nosso servidor fictício possui o IP 192.168.2.1. Para configurar, siga os passos:

1 - Na página Port Forwarding, assinale o item Enable Port Forwarding;

2 - Em IP Address, digite o IP do computador local que irá provê o serviço. No nosso exemplo é 192.168.2.1;

3 - Em Protocol, escolha o protocolo. No nosso caso é TCP. Na dúvida, escolha Both (ambos);

4 - Em Port Range, digite a porta. No nosso exemplo é 80;

5 - Em Comment, você pode inserir um pequeno comentário. No nosso exemplo digitamos Web Server;

5 - Clique em Apply Changes.

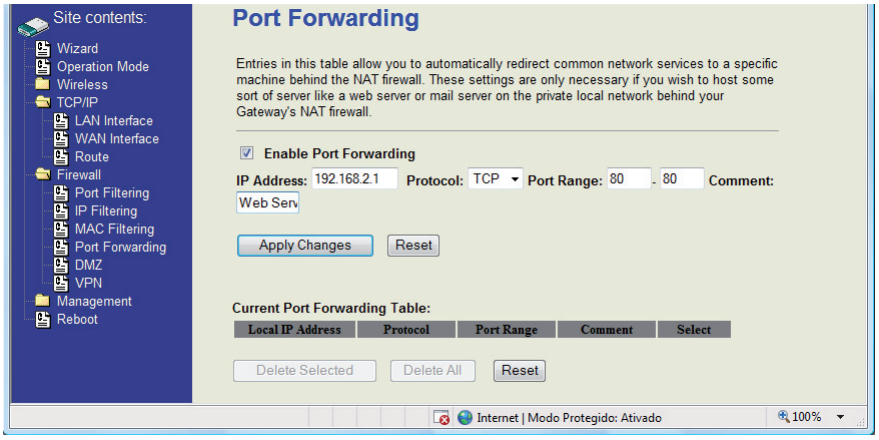


Figura 07.3: configurando um Port Forwarding.

Logo abaixo haverá uma tabela com os Port Forwarding atuais.

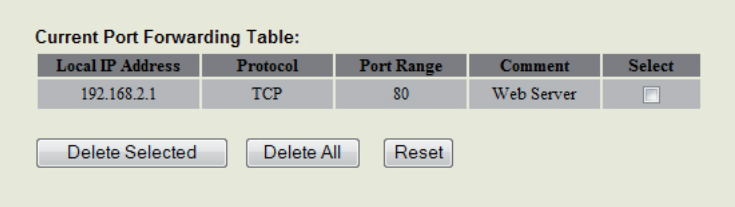


Figura 07.4: Port Forwarding atual.

DMZ

DMZ são siglas de DeMilitarized Zone, que é bom português quer dizer zona desmilitarizada. É um recurso que permite deixar um computador totalmente accessível à Internet. Também é necessário ter NAT ativado.

Ao usar esse recurso, não é permitido usar o Port Forwarding (que deve ser desabilitado). Além disso, ele não torna somente um serviço acessível à Internet, e sim todos os dados do computador podem ser acessados irrestritamente. Não há proteção ao computador exposto.

Não é necessário associar uma porta ao IP, uma vez que o computador é exposto integralmente. Basta informar o IP local. Além disso, um único computador pode ser configurado. O acesso ao computador pela Internet é feito digitando-se no browser o IP público do gateway.

Para configurar um computador:

1 - Na página DMZ, assinale o item Enable DMZ;

2 - Em DMZ Host IP Address, digite o IP do computador local que irá expor à internet;

3 - Clique em Apply Changes.

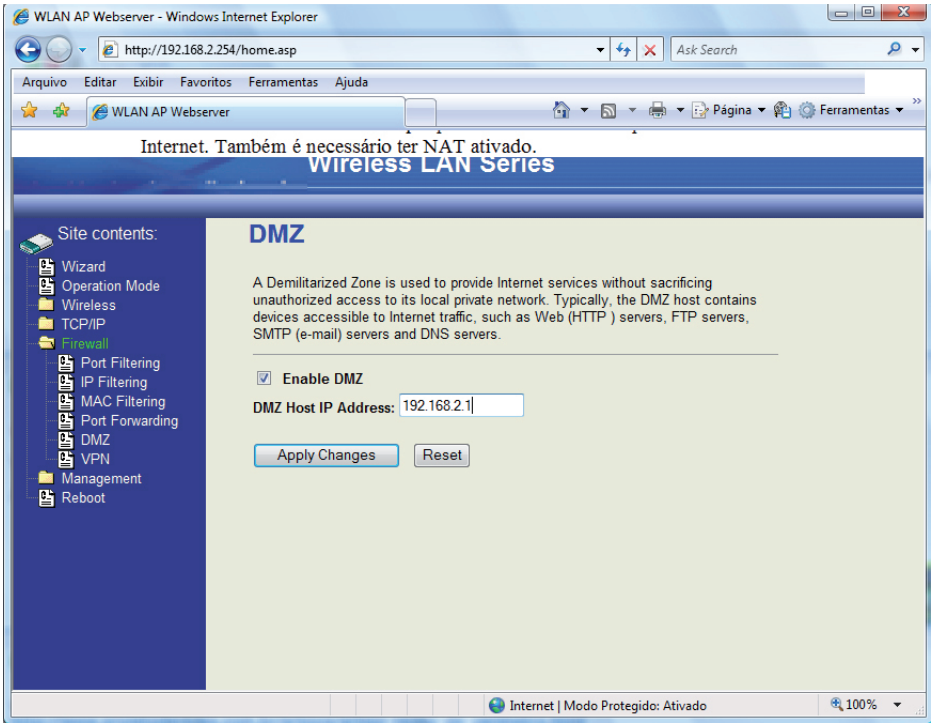
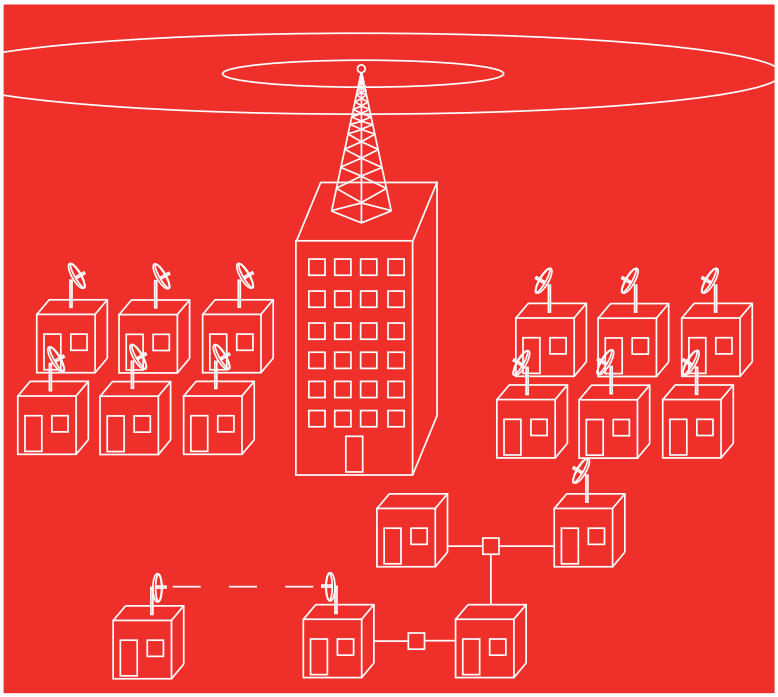


Figura 07.5: configurando um DMZ.



Capítulo 8 - Gerenciamento

INTRODUÇÃO

Até esse ponto do livro vimos como montar e realizar diversos tipos de configurações em redes wireless. Neste último capítulo desta obra é abordado um pouco sobre o gerenciamento de redes sem fio.

O gerenciamento pode ser feito através do próprio “Web-setup” do access point. No menu haverá uma seção dedicada a isso, chamada Management (Gerenciamento).

Podemos definir gerenciar como administrar, regular e manter a integridade física e funcional da rede.

Isso quer dizer que o gerenciamento vai além de configurar a seção Management “Web-setup”. Por exemplo: devemos manter a integridade do AP, fisicamente falando. Se sua rede utiliza dois ou mais AP (repetidores), ou, em conjunto com o AP é utilizado roteadores, cabe a você cuidar e manter esses equipamentos seguros e em pleno funcionamento.

Eles devem instalados em lugares seguros. Evite simplesmente colocá-los de qualquer forma sobre uma mesa, para evitar que ele sofra esbarrões e até seja jogado no chão. Se o modelo em questão não suportar fixação em uma parede (não há os locais para parafusos), então, reserve um lugar seguro, onde ele fique protegido e provendo á todos os nós da rede um bom sinal.

Uma questão muito importante é quanto à sua segurança: existem caixas próprias para a instalação de APs, principalmente naqueles casos em que ele é usado no modo Wireless ISP, sendo instalados junto (ou próximo) ao porte da antena. Essas caixas o protege da chuva, sol e vento. Além de prover uma segurança mínima contra furtos. Se você possui um provedor de acesso á Internet via ondas de rádio, saiba que essas caixas podem ser afixadas junto à base da antena.

Se um AP “queimar” (danificar) ele deve ser substituído. Se a Internet parar de funcionar, deve ser verificado o motivo e posterior solução. Se o tráfego de dados estiver muito pesado, o mesmo deve ser feito, ou seja, averiguar a causa e aplicar uma solução o mais rápido possível.

Quanto às configurações no AP, o quê nos é permitido fazer, em se tratando de gerenciamento, vai depender muito da marca e modelo do AP. Existem desde modelos que nos permitem um gerenciamento básico até modelos que possuem um gerenciamento amplo e completo.

O objetivo deste capítulo é discutir algumas dessas possibilidades. O menu do AP Zinwell Zplus G220 pode ser visto na imagem à seguir. Observe a seção Management.

Figura 08.1: Management.

Password

Não há tópico melhor, para começar a discutir, do que esse. O password do AP, ou seja, a senha que é usada para acessar ao "Web-setup".

Essa senha é de uso imprescindível, indispensável. É o primeiro fator a definir a segurança de toda a rede.

O AP é o centro, o núcleo da rede sem fio. Se qualquer pessoa que conseguir captar o sinal da rede, ter acesso ao "Web-setup" do AP, qualquer outro tipo de configuração de firewall e chave de acesso é totalmente vil, sem sentido e demonstra total ingenuidade a respeito do assunto.

Nem precisa dizer que uma vez "dentro" do "Web-setup", todas as configurações podem ser modificadas, inclusive à favor daquele que fizer as modificações. Um invasor pode, por exemplo, aumentar a força do sinal para que ele consiga navegar melhor, do local onde ele conseguiu captar o sinal wireless.

Ao montar uma rede sem fio, qualquer vizinho seu que tenha um computador contendo uma placa de rede wireless é capaz de captar o seu sinal. E ele pode tentar se conectar à rede (e se ela não tiver criptografia e chave de acesso configurada, ele terá êxito). E se ele conseguir o IP do access point, o acesso pode ser certo.

Vale ressaltar que ao criar uma senha, também é necessário criar um nome de usuário, pois, esses dois dados são solicitados na tentativa de acesso.

Alguns "Web-setup" vêem de fábrica sem senha (e conseqüentemente, sem nome de usuário). Simplesmente não solicitado nenhuma senha nos primeiros acessos, até que o usuário configure uma. Outros possuem senhas padrões (ver manual), algo tipo admin (nome de usuário) e admin (senha).

Para modificar ou inserir uma nova senha, faça o seguinte:

1 - Na seção Management, clique no link password;

2 - Irá abrir a página Password Setup. No campo User Name, digite um nome de usuário;

3 - Em New Password, digite a senha desejada. Repita-a em Confirmed Password;

4 - Para confirmar, clique em Apply Changes.

Figura 08.2: Password Setup.

A partir de agora, sempre que acessar o “Web-setup” será solicitado um nome de usuário e senha.

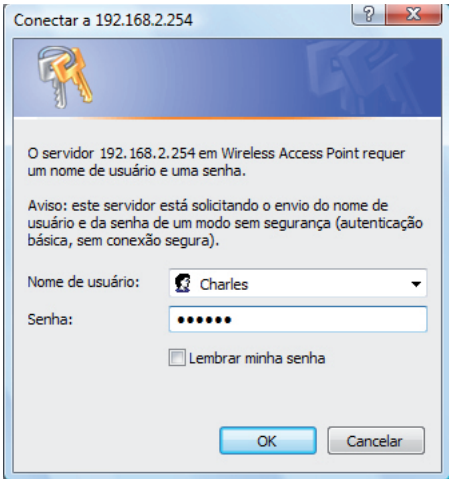


Figura 08.3: digite o nome de usuário e senha.

STATUS

A página de status é o local onde podemos ver as principais configurações e definições atuais do AP. Elas variam de acordo com o modo do ap, já que cada modo possui as suas próprias peculiaridades. Vejamos às informações disponíveis no modo AP - Bridge:

System

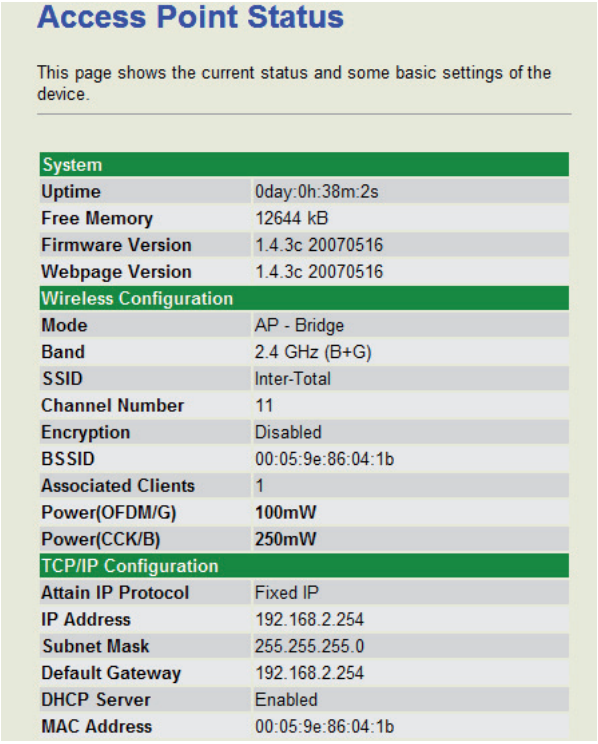
- **Uptime:** define o tempo de atividade. Mostra quanto tempo o AP está ligado, em dias, horas, minutos e segundos;
- **Free Memory:** exibe a memória livre d sistema;
- **Firmware Version:** versão atual do firmware gravado na memória ROM do AP;
- **Webpage Version:** define a versão do “Web-setup”.

Wireless Configuration

- **Mode:** exibe os modos do AP e o tipo de rede;
- **Band:** Mostra a banda de operação e frequencia usada atualmente pelo AP;
- **SSID:** o nome da rede;
- **Channel Number:** canal de transmissão usado;
- **Encryption:** se usado algum tipo de criptografia, é mostrada qual é nesse campo;
- **BSSID:** MAC Adress do AP;
- **Associated Clients:** número de clientes associados, ingressados na rede;
- **Power(OFDM/G):** exibe potência do sinal OFDM;
- **Power(CCK/B):** exibe potência do sinal CCK.

TCP/IP Configuration

- **Attain IP Protocol:** exibe se é usado IP fixo ou dinâmico;
- **IP Address:** IP atual do access point;
- **Subnet Mask:** máscara de sub-rede usada;
- **Default Gateway:** mostra o IP do gateway padrão;
- **DHCP Server:** a condição atual, ou seja, habilitado ou desabilitado;
- **MAC Address:** exibe o MAC do access point.



Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:38m:2s
Free Memory	12644 kB
Firmware Version	1.4.3c 20070516
Webpage Version	1.4.3c 20070516
Wireless Configuration	
Mode	AP - Bridge
Band	2.4 GHz (B+G)
SSID	Inter-Total
Channel Number	11
Encryption	Disabled
BSSID	00:05:9e:86:04:1b
Associated Clients	1
Power(OFDM/G)	100mW
Power(CCK/B)	250mW
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
DHCP Server	Enabled
MAC Address	00:05:9e:86:04:1b

Figura 08.4: status (modo AP – Bridge).

TIME ZONE

Nessa página é possível acertar a data e hora. As configurações são bem simples. Acompanhe na prática:

1 - No campo Year (ano) digite o ano atual;

2 - Em Month (Mês) digite o número correspondente ao mês;

3 - Em Day (dia) digite o dia do mês;

4 - No campo Hour (hora) digite a hora. Em Min (minutos) coloque os minutos e em Sec (segundos) os segundos);

5 - No item Time Zone Select (Fuso horário) devemos escolher o fuso horário de acordo com o nosso país. Para o Brasil é (GMT-03:00)Brasília;

6 - A opção Enable NTP client update deve ser selecionada caso deseje que a data e hora seja acertada através de um servidor público NTP (ver capítulo 03, no tópico Wizard);

7 - Clique em Apply Changes para aplicar e salvar.

Figura 08.5: Time Zone.

LOG

Em questões de gerenciamento, essa página é extremamente útil. O objetivo principal dela é exibir os clientes que se ingressaram e os que saíram da rede. Isso é conseguido graças ao endereço MAC que cada placa wireless possui.

Você pode facilmente montar em uma tabela (usando algum programa específico, como o Excel) contendo os nomes de todos os clientes da rede, associados aos seus respectivos endereços MAC. A partir daí, é possível ter um pequeno acompanhamento de todos os seus ingressos à rede.

Voltando à questão de invasão, se uma pessoa conseguir acessar a rede de forma não autorizada, o seu endereço MAC também estará registrado. Desse modo, essa página de Logs torna-se útil na tarefa desse tipo de detecção.

Uma vez detectado algum usuário não autorizado à rede, basta anotar o seu endereço MAC e bloqueá-lo, conforme já demonstramos anteriormente neste livro.

A questão de segurança é tão importante, que vamos abrir um parêntese para comentar mais um assunto relacionado. Muitas vezes pode ocorrer o ingresso de pessoas não autorizadas à rede, não por uma invasão de fato, mas, sim porque algum usuário (que possui a sua autorização para acesso) forneceu-lhe os dados necessários para acesso. Nesse caso, ele consegue entrar na rede sem fio e usar tudo a que um usuário autorizado tem direito. Mas, o endereço MAC dele também será listado. Basta bloqueá-lo.

Para ativar essa função:

1 - Selecione o item Enable Log;

2 - Logo abaixo, escolha entre wireless only (Apenas sem fio) ou system all (todo o sistema);

3 - Clique em Apply Changes para aplicar e salvar.

Para ver os logs clique no botão Refresh.

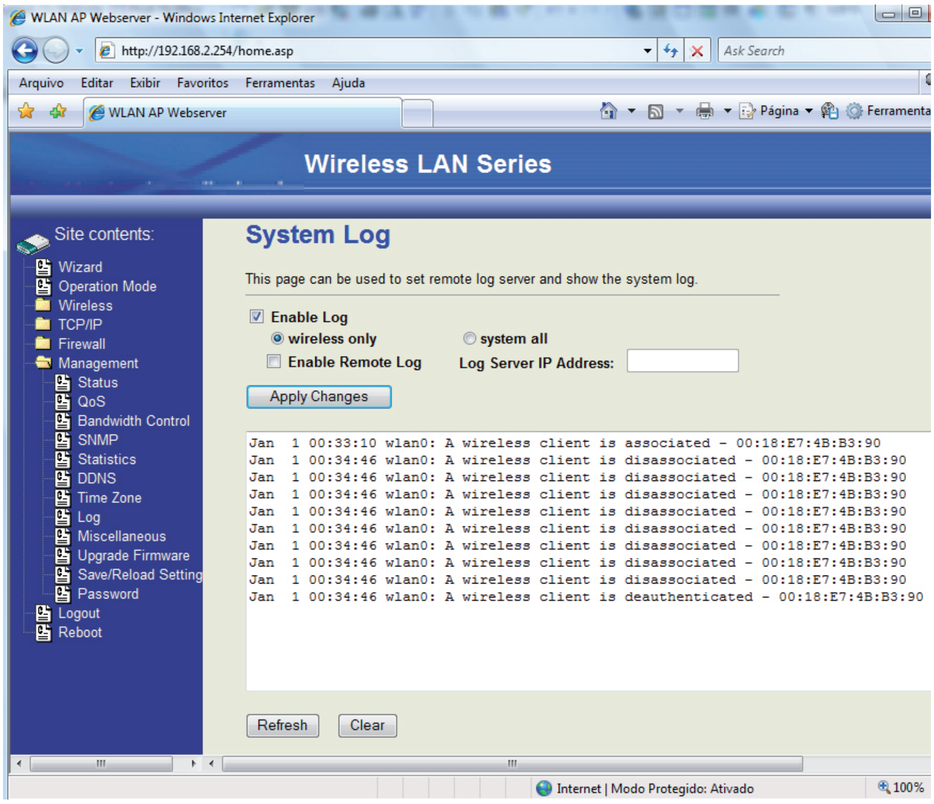


Figura 08.6: Log.

UPGRADE FIRMWARE

Fazer um upgrade do firmware do Access point é atualizar a versão desse firmware, logicamente por uma mais recente.

Você pode atualizá-lo por vários motivos. Por exemplo: para que ele tenha novas funcionalidades (em termos de hardware o AP pode dar suporte a certos tipos de configurações, mas, que ainda não podem ser realizadas no

"Web-setup".), para que ele fique no seu idioma (por exemplo: o AP está no idioma inglês e você deseja atualizá-lo para o português), etc.

A primeira coisa a saber é que os procedimentos de atualização do firmware de um AP pode mudar de acordo com a marca e modelo. Dessa forma, a consulta do manual é insubstituível. Esse é um caso que não vale à pena tentarmos explicar uma forma, uma maneira "padrão" de como proceder para atualizar. Não existe "receita de bolo" para esse caso.

É preciso estar atento quanto à memória livre: observe, através do manual, se o seu modelo de AP exige uma certa quantidade de memória livre (do AP). Caso afirmativo, e a memória livre não for suficiente, experimente desativar alguns funções, ou, até resetar o AP (se for o caso).

Além disso, um detalhe importante, é que durante o processo de upload dos dados para o AP (durante o processo de gravação), ele não pode ser desligado da tomada. Isso pode causar problemas sérios, uma vez que os dados ficaram gravados pela metade. O ideal é deixá-lo, pelo menos durante esse processo, ligado a um nobreak, pois, caso ocorra uma interrupção temporária da energia elétrica, o seu computador e o AP continuam ligados.

Por fim, a versão atualizada do firmware é conseguida diretamente no site do fabricante. Consulte a manual para saber o endereço (URL) correto.

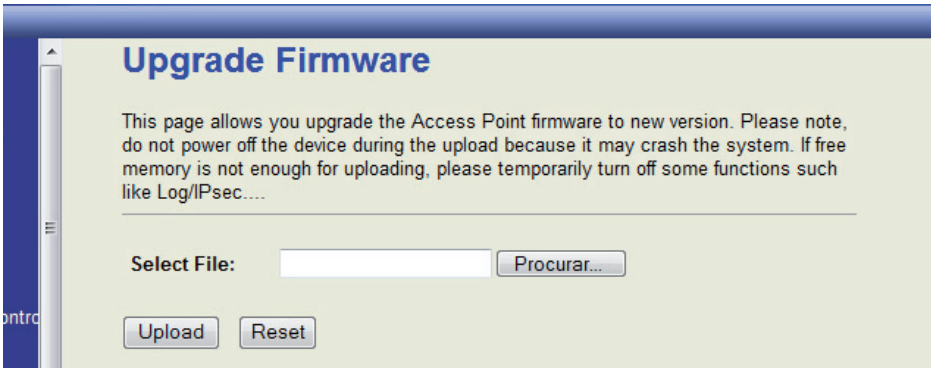


Figura 08.7: Upgrade Firmware.

Vamos explicar para que servem as opções na página Upgrade Firmware:

1 - A opção Select File é onde você deve digitar o caminho para o arquivo do firmware no seu HD. Caso queira fazer uma procurar, basta clicar no botão procurar. Irá abrir a janela Escolher arquivo, onde você pode navegar normalmente pelas pastas até chegar ao local onde se encontra o arquivo;

2 - O botão Upload serve para enviar o arquivo do seu HD para a memória ROM do access point;

3 - O botão Reset apaga as informações inseridas no campo Select File, ou seja, as informações do local onde se encontra o arquivo.

Nota geral: para gravar o firmware na ROM do AP, é necessário conectá-lo ao computador onde se encontra o arquivo do firmware (que você fez o download da Internet) usando um cabo do tipo par trançado. Consulte o manual para saber todos os procedimentos necessários.

STATISTICS

Páginas de estatísticas. Nessa página é possível acompanhar os pacotes enviados e recebidos na rede sem fio, redes Ethernet e WAN.

São duas as informações:

- **Sent Packets:** pacores enviados;
- **Received Packets:** pacotes recebidos.

Para atualizar os dados da página, clique no botão Refresh.

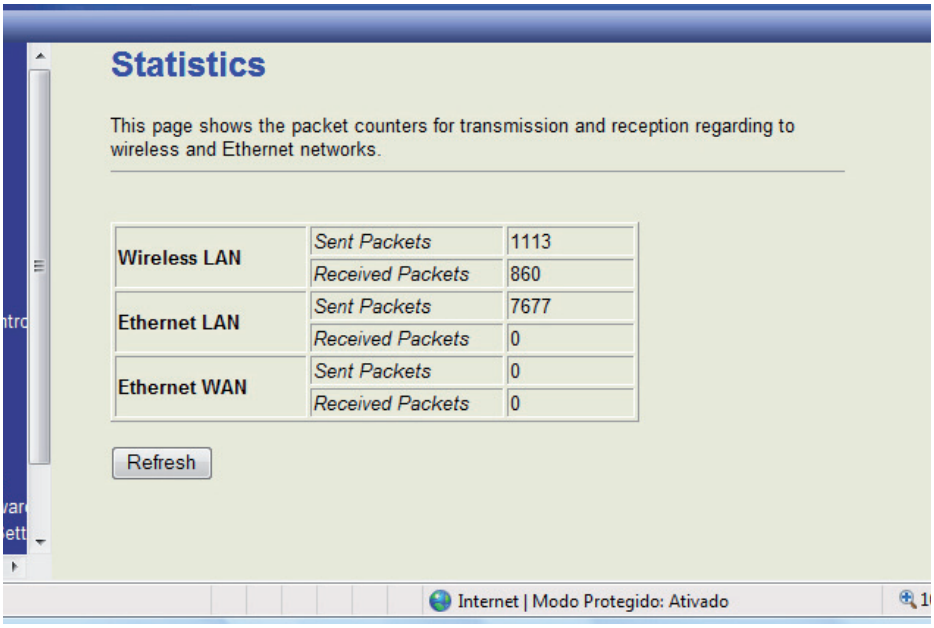


Figura 08.8: Statistics.

DDNS

No capítulo passado explicamos o funcionamento de Port Forwarding, onde, após a sua correta configuração, é possível acessar recursos disponíveis em um computador que esteja em uma rede local. Para que isso funcione é necessário que o gateway (mais uma vez vamos usar esse nome "genérico", pois, isso pode ser aplicado a um router, AP, firewal, etc) tenha um IP válido na Internet. E ele tem, graças ao servidor de acesso à Internet ao qual ele se conecta.

Mas, há um problema grave nisso: o IP recebido pelo gateway é válido, mas, é um IP dinâmico. Isso quer dizer que ele muda o tempo todo. A cada nova conexão que for feita, um novo IP será cedido ao gateway.

Se o IP muda o tempo todo, é necessário informar o novo IP para todos os usuários que quiserem acessar o recurso disponível no computador local. O que torna o uso do recurso muito inviável.

E isso vale também para o uso do DMZ, afinal, o IP do gateway é dinâmico.

É nesse ponto que entra o DDNS (Dynamic Domain Name System). É um serviço fornecido por diversas empresas, algumas gratuitas, outras pagas.

O que ele faz é criar um nome de domínio que passará a representar o IP (válido) da conexão do usuário. Com o serviço DDNS é possível acessar o gateway (ou os serviços oferecidos por ele) a partir da internet, sem se preocupar com IP.

Funciona assim: primeiro o usuário se cadastra no serviço e cria um nome de domínio e faz as devidas configurações necessárias no site. Uma vez cadastrado ele terá um nome domínio e senha. Com esses dados, ele realiza a configuração na área DDNS do gateway, informando o site que oferece o serviço, o nome do domínio, senha e e-mail. Pronto, tudo já estará funcionando.

Sempre que o gateway se conectar com a Internet, ele fará uma conexão com o serviço DDNS para informar o seu novo IP. Desse modo, não importa quantas vezes o IP mude. O nome do domínio criado será sempre o mesmo, e, ele irá fazer referencia o IP do gateway válido no momento em que ele estive conectado. Sempre que mudar o IP do gateway, essa informação é automaticamente atualizada na empresa que fornece o DDNS.

Vejamos como realizar a configuração:

1 - Na seção Management, clique no link DDNS;

2 - Na página Dynamic DNS Setting, marque (para ativar) o item Enable DDNS;

3 - Em Service Provider, selecione o servidor DDNS. O que recomendamos aqui é o DynDNS (www.dyndns.com);

4 - Em Domain Name, digite o nome de domínio criado;

5 - No campo User Name/Email, digite o nome de usuário que você criou ao abrir a conta no serviço DDNS;

6 - Em Password/Key, digite a senha que você criou ao abrir a conta no serviço DDNS;

7 - Clique em Apply changes.

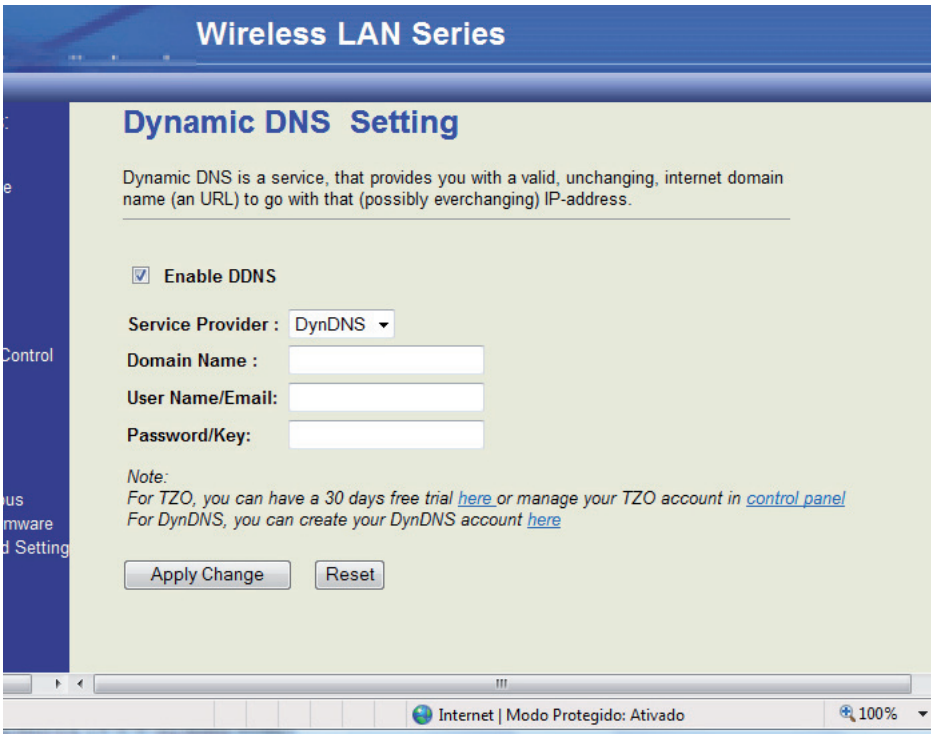


Figura 08.9: Dynamic DNS Setting.

MISCELLANEOUS

A palavra Miscellaneous em português significa miscelânea. Para quem não conhece, esse terno significa misturado, variado, diversos, misto.

Dessa forma, o que encontramos na página Miscellaneous Settings (definições diversas) é uma área onde podemos realizar algumas

configurações variadas, tais como HTTP Port (porta que será usada para o protocolo HTTP. O padrão é 80), RSSI Interval (Configuramos o intervalo em minutos), RSSI (Received Signal Strength Indicator – Indicação da força do sinal), Ping Interval (intervalo para o ping), etc.

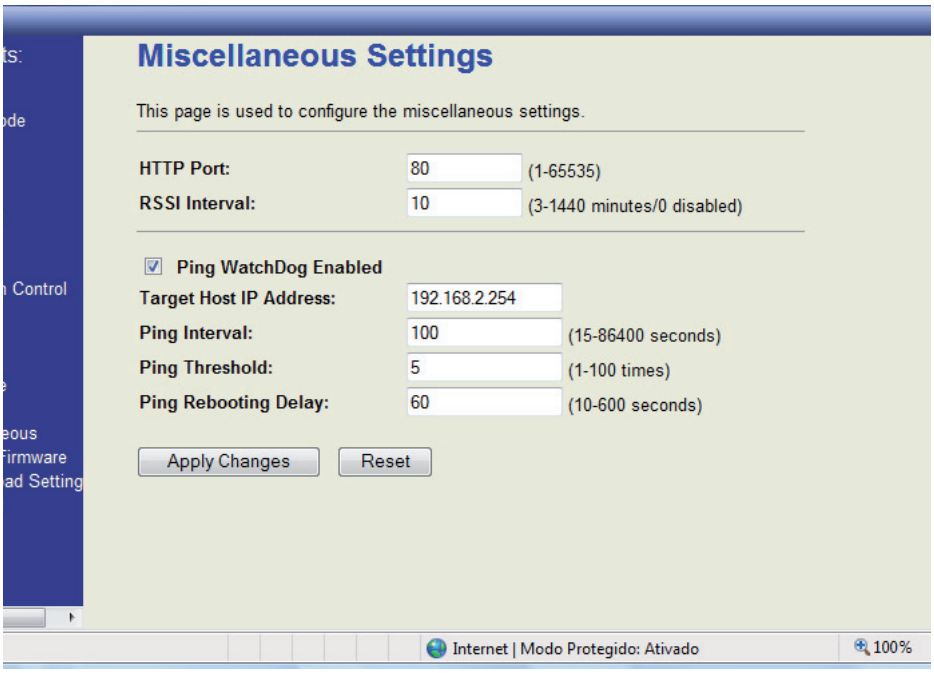
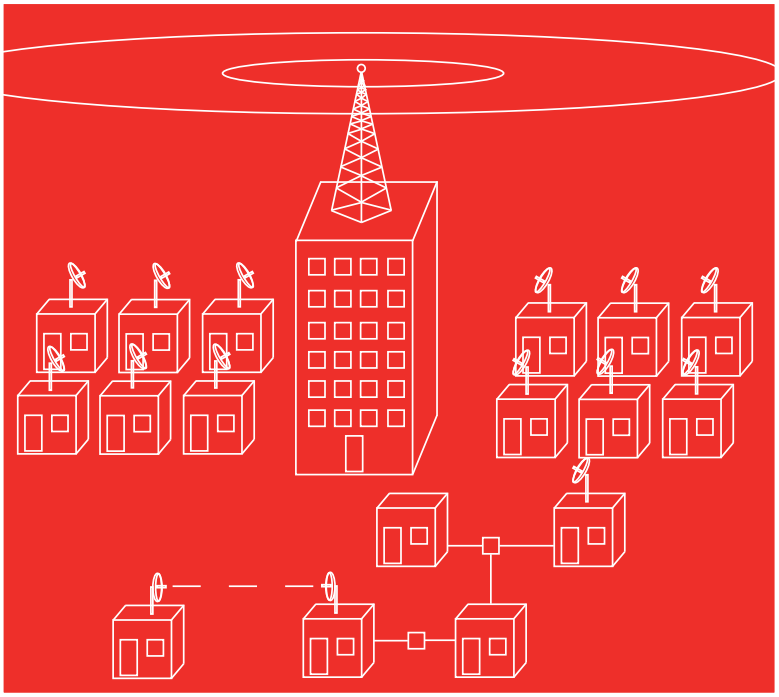


Figura 08.10: Miscellaneous.



Capítulo 9 - Bônus: Introdução ao Mikrotik

INTRODUÇÃO

É importantíssimo eu te dizer o seguinte: Este capítulo é apenas um bônus, ou seja, um capítulo extra que estou te dando de presente.

Além disso, este capítulo é apenas uma introdução para você conhecer o assunto e, a partir daí, poder dar passos maiores.

Procurei fazer uma introdução bem caprichada, para que você possa entender exatamente o que é Mikrotik, como baixá-lo, como instalá-lo e acessá-lo, como navegar por entre suas opções e tudo que você precisa saber sobre licenciamento. A partir daí, caso tenha interesse no assunto, é procurar livros e cursos completos sobre Mikrotik.

Espero que você consiga por em prática tudo que eu demonstrar nas páginas seguintes.

Avante rumo ao sucesso.

O QUE É MIKROTIK?

A melhor forma de começar este capítulo é justamente respondendo algumas dúvidas que muitos iniciantes em MikroTik possuem. É muito comum dúvidas tais como:

O que é MikroTik?

O que podemos fazer com ele?

Onde conseguir o sistema?

Entre várias outras perguntas. Iniciantes, ou até mesmo estudantes intermediários, possuem muitas dúvidas acerta do assunto.

ENTÃO, O QUE É MIKROTIK?

MikroTik é uma empresa que fica situada na Letônia. Letônia é uma república que faz limite com a Rússia, Estónia, Bielorrússia, Lituânia e com o mar Báltico. A seguir vemos a Letônia no mapa.

Figura 09 .1: Letônia no mapa.

A capital de Letônia é Riga. O seu idioma oficial é o letão. Letônia em letão pronuncia-se “Latvija”.

A MikroTik foi fundada em 1995 e é especialista no desenvolvimento de produtos wireless e roteadores.

Seus produtos são muito utilizados em áreas como conexões sem fio, provedores de acesso a internet sem fio (internet via rádio) e administração de redes.

: o site oficial da MikroTik é: www.MikroTik.com/.

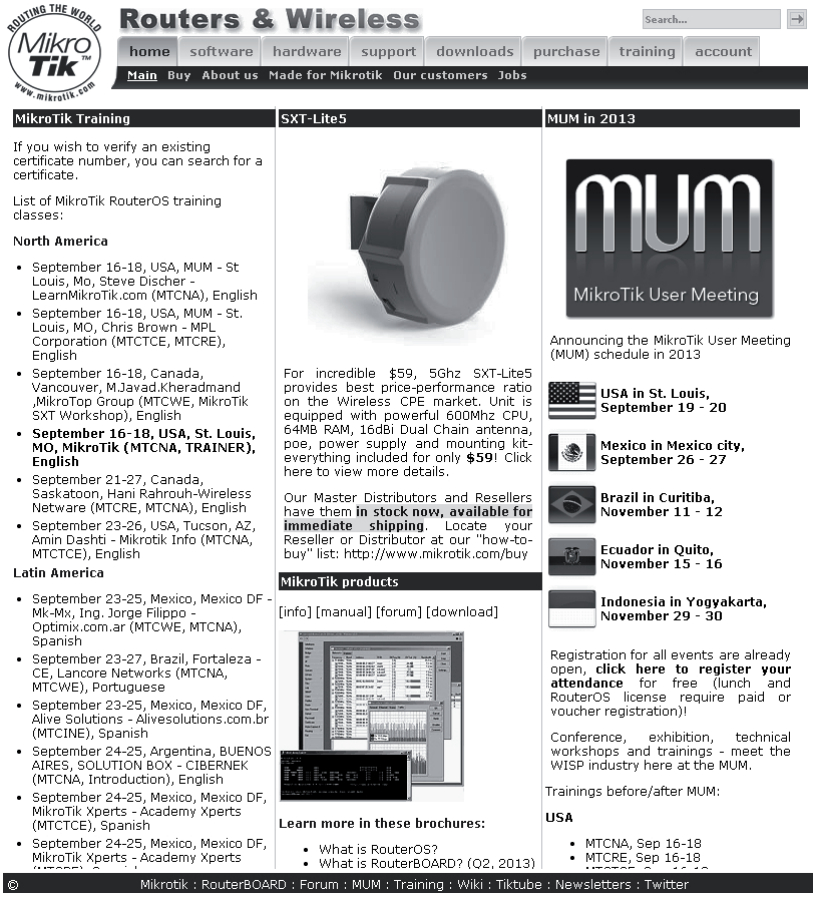


Figura 09.2: site oficial da MikroTik.

Agora que já sabemos o que é MikroTik, onde está localizada, ano de fundação e o que ela faz, vamos conhecer sobre o sistema operacional. Leia o tópico seguinte.

O QUE É MIKROTIK ROUTEROS?

Li em alguns lugares que MikroTik é o sistema operacional. Na verdade, o sistema operacional desenvolvido pela empresa MikroTik é o MikroTik RouterOS.

Portanto, já respondendo a pergunta do tópico, MikroTik RouterOS é um excelente sistema operacional desenvolvido tendo como base o Linux.

MikroTik RouterOS pode ser instalando em roteadores ou em computadores e servidores da plataforma x86.

Computadores e servidores x86 são os PCs (Personal Computer) que conhecemos, que possuem na grande maioria algum sistema operacional da família Windows ou Linux. Graças a essa vantagem, podemos dimensionar nossos próprios roteadores, usando hardwares compatíveis. Inclusive, ao dimensionar um roteador baseado em PC podemos montá-lo dentro de uma caixa hermética.

O MikroTik RouterOS pode ser baixado no próprio site oficial da MikroTik : www.MikroTik.com/.

 : devido à grande estabilidade e cartela de recursos, MikroTik RouterOS é referência mundial quando o assunto é sistema para servidores e roteadores.

O QUE É MIKROTIK ROUTERBOARD?

MikroTik RouterBoard são hardwares criados pela própria empresa MikroTik. Esse tipo de equipamento já vem de fábrica com o sistema MikroTik RouterOS instalado. No geral são roteadores e equipamentos de rádio frequência.

Roteadores RouterBoard podem ser comprados com as seguintes características básicas:

- **Com case:** ele virá instalado dentro de uma case própria. Ou seja, terá a aparência semelhante à um hub, roteador ou switch;
- **Sem Case:** é a placa avulsa que pode ser montada dentro de uma caixa hermética.

O QUE PODEMOS FAZER COM MIKROTIK ROUTEROS/ MIKROTIK ROUTERBOARD

O que podemos fazer com MikroTik RouterOS e/ou MikroTik RouterBoards? Essa pergunta talvez seja uma das mais esperadas por você.

Todos querem saber ou conhecer as características e qualidades, funcionalidades e vantagens, enfim, tudo o que podemos montar e configurar.

Explanei a seguir uma lista de funcionalidades, vantagens, o que podemos configurar com sistema MikroTik:

- Exige poucos recursos de hardware;
- Opções de backup;
- Permite atualizações;
- Permite disponibilizar roteadores dedicado;
- Montagem de redes wireless. Suporta equipamentos dos padrões 802.11a/b/g/n;
- HotSpot. Você pode fornecer acesso controlado (com usuário e senha) à internet em ambientes diversos como hotéis, convenções, escolas, restaurantes, cafeteria, etc;
- SP/WISP. Montagem de servidores via rádio;
- Permite autenticação Radius;
- Possui interface de gerenciamento amigável;
- Controle de banda, por usuário ou máquina;
- Gerenciamento de usuários;
- Balanceamento de links. Você pode usar vários links de acesso à internet (dedicado ou não) de forma balanceada;

- Evita congestionamento do link com balanceamento de carga entre os usuários. Mesmo se um usuário da rede fizer excessivos downloads, a rede não fica congestionada;
- Configurações ponto a ponto (tipo matriz filial);
- Firewall, para dar maior segurança à rede;
- Recursos de Segurança WEP, WPA e WPA2;
- Acesso e gerenciamento remoto através da web, Telnet, SSH, WinBox Gui, Mac-telnet;
- Bridge;
- Web Proxy;
- Servidor PPPOE;
- Redes Virtuais (VPN);
- NAT;
- DHCP;
- QoS;
- Filtros HTTP, P2P, entre outros;
- E etc;

Como vemos, o MikroTik RouterOS nos prover muitas possibilidades. Ele oferece muito recursos e pode ser utilizado em diversas situações, desde pequenas redes sem fio locais até serviços de internet via rádio. É estável, robusto e com excelente nível de gerenciamento.

DOWNLOAD DO SISTEMA MIKROTIK ROUTEROS

Vamos ao download do sistema MikroTik RouterOS. Para isso, siga as instruções:

1 - Acesse o endereço eletrônico:

http://www.MikroTik.com/

2 - Ao acessar, você verá a página oficial da empresa MikroTik;

3 - Clique em downloads;

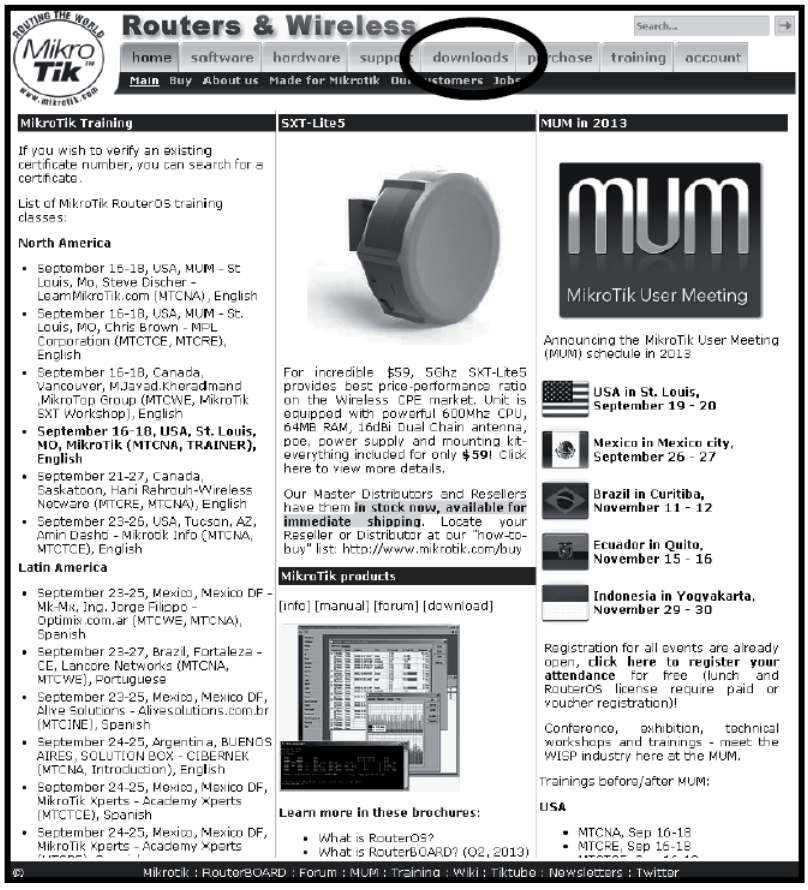


Figura 09.3: opção downloads.

4 - Você a página de downloads, onde bem no topo está escrito: “Download MikroTik software products”;

Figura 09 .4: página de downloads.

5 - Para instalar em um computador PC, clique na opção x86. Você verá as versões disponíveis, e em cada versão as opções de instalação;

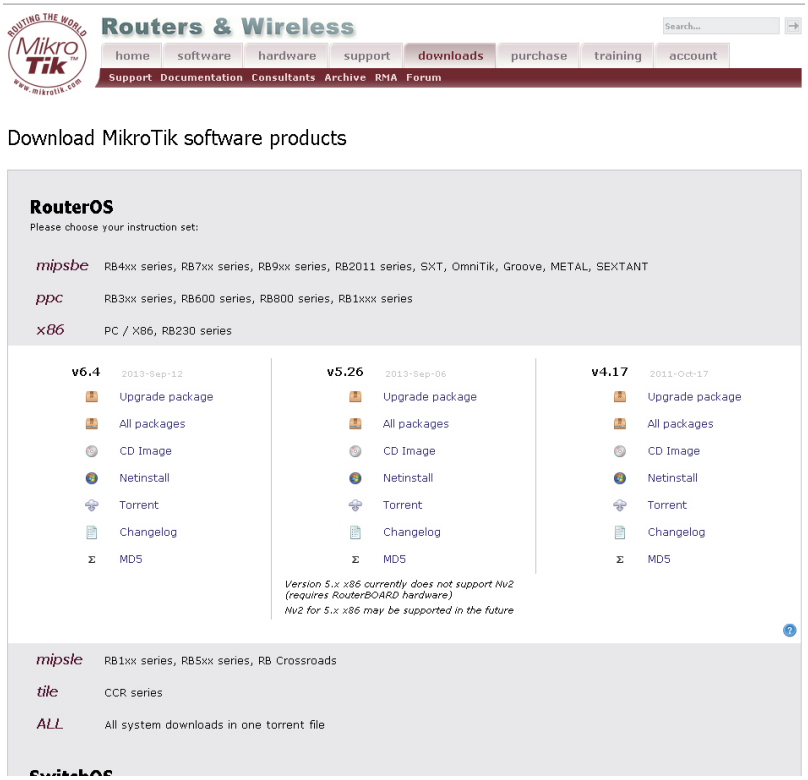


Figura 09.5: versões e opções de instalação.

6 - O nosso interesse por hora é obter a imagem "*.iso" para instalação do sistema em um computador PC. Indico a versão mais atual. Clique em CD Image;

7 - Faça o download em uma pasta de sua escolha. Ao final do download é necessário proceder com a gravação da imagem em um CD. Para isso, leia o tópico seguinte.

GRAVAÇÃO DA IMAGEM .ISO EM UM CD

Agora que já temos o arquivo "*.iso" basta gravá-lo em um CD virgem. Neste tópico farei um resumo bem breve (bem breve mesmo. Gravar CD/

DVDs é uma tarefa bem simples.) como gravar esse arquivo no CD usando o software de gravação de CDs e DVDs Nero Express. É um software muito conhecido, por isso optei por ele. Mas, você pode seguir as orientações que dou aqui e usar o software de sua preferência.

A gravação da imagem "*.iso" é fácil, é necessário apenas ficarmos atentos com a forma de gravar. Escrevi este tópico justamente para evitar erros. Para gravar faça o seguinte:

1 - Coloque um CD virgem na unidade de gravação;

2 - Vemos a pergunta: O que você gostaria de gravar? Selecione logo abaixo a opção Imagem do disco ou projeto salvo.

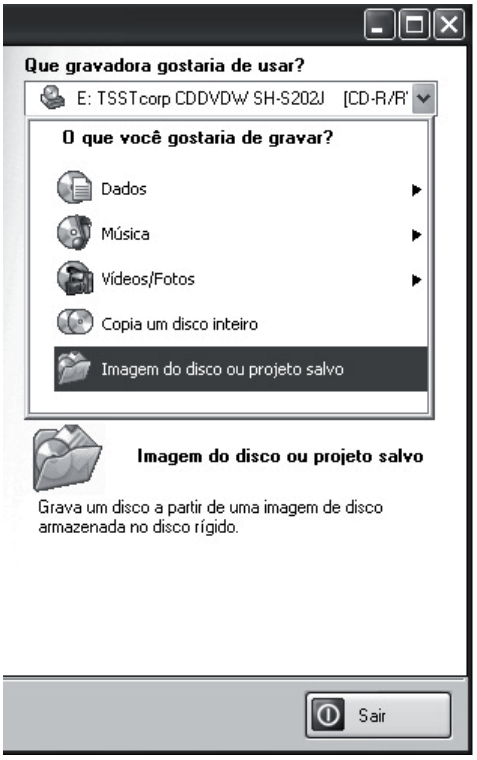


Figura 09.6: Clique na opção Imagem do disco ou projeto salvo.

3 - Irá abrir a janela Abrir. Na opção Arquivos do tipo, selecione Arquivos de Imagem (*.nrg, *.iso, *.cue);

Figura 09.7: selecione Arquivos de Imagem.

4 - Em Examinar, selecione a pasta onde você fez o download do arquivo *.iso;

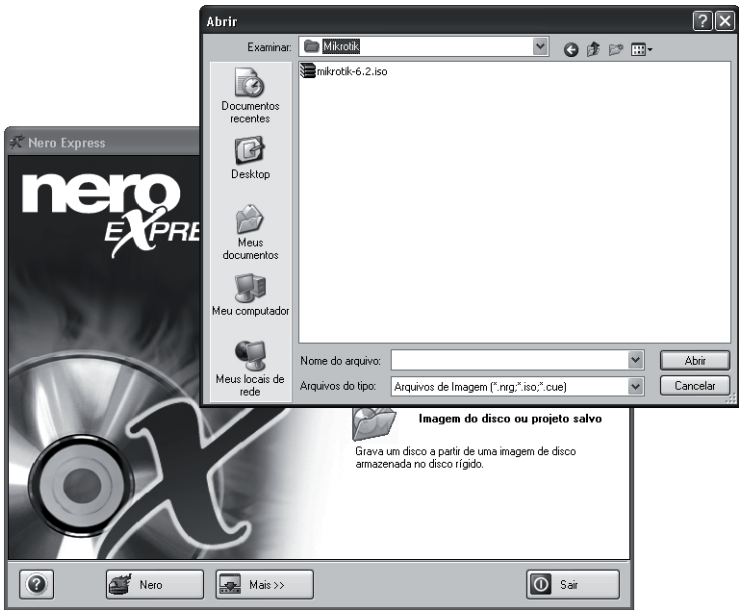


Figura 09.8: selecione onde fez o download do arquivo.

5 - Selecione o arquivo e clique no botão Abrir;

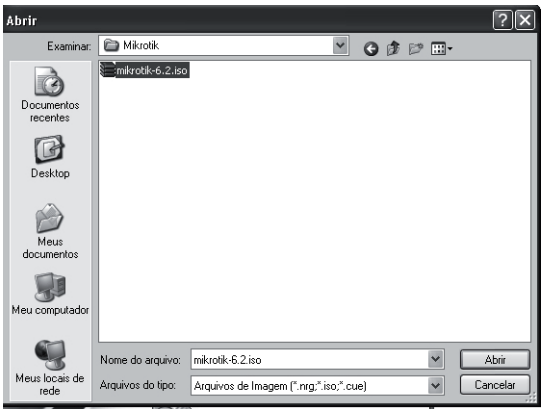


Figura 09.9: selecione o arquivo e clique no botão Abrir.

6 - Veremos uma janela com informações do Arquivo de imagem, drive de destino (unidade de gravação) e número de cópias. Verifique se está tudo correto e clique no botão Avançar;

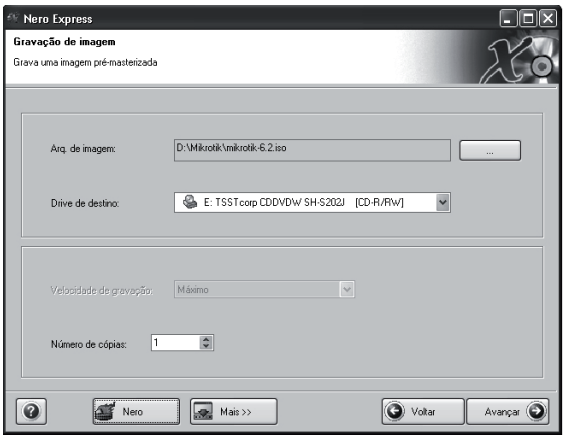


Figura 09.10: se estiver tudo correto clique em Avança.

7 - A gravação irá iniciar;

Figura 09.11: processo de gravação.

8 - Ao término clique no botão OK.

Figura 09.12: clique em OK.

9 - Neste ponto a gravação foi completada com sucesso. O Nero pode ser fechado.

Pronto, o CD está preparado para ser usado na instalação do MikroTik RouterOS. Mas, antes de instalar é indispensável averiguar se o hardware do computador PC é compatível. Para isso, vamos ao tópico seguinte!

HARDWARES SUPORTADOS

Antes de instalar o MikroTik RouterOS é indispensável verificar a lista de hardwares suportados. Você precisa verificar se o hardware do computador PC onde vai instalar o MikroTik RouterOS é compatível com o sistema.

Para fazer essa verificação, siga as etapas:

1 - Acesse o endereço eletrônico: http://wiki.MikroTik.com/wiki/Supported_Hardware

2 - Você verá a página Supported Hardware.

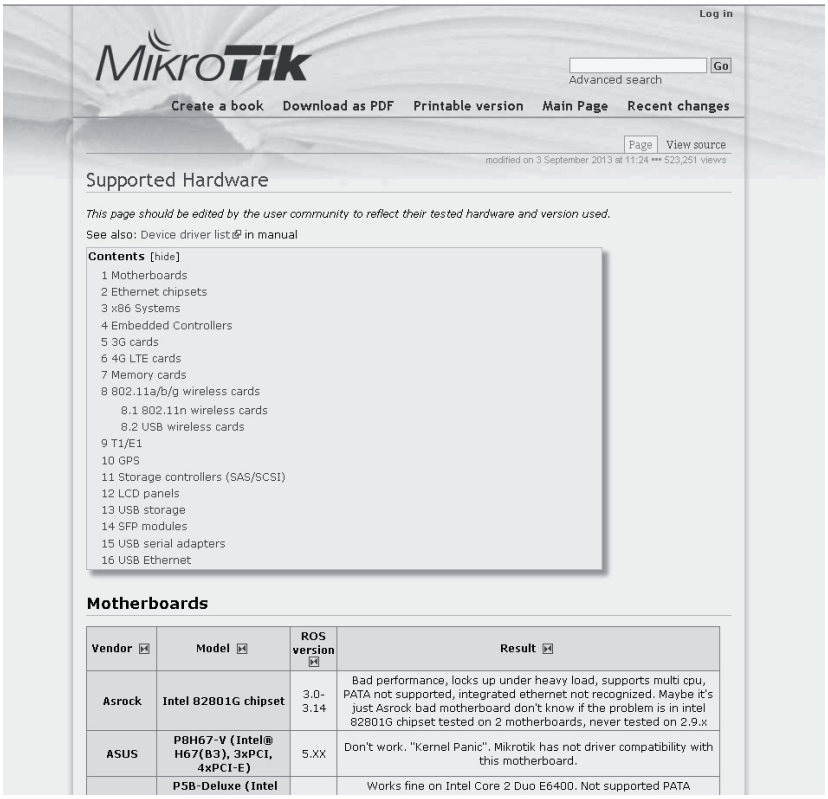


Figura 09.13: Página Supported Hardware.

3 - Esta página mantém a lista atualizada com comentários. É útil e recomendo que sempre acesse-a para manter-se informado. Principalmente se você for trabalhar na área.

INSTALAÇÃO PARA TESTES E ESTUDO COM MÁQUINA VIRTUAL

O que fazer se você desejar instalar o MikroTik RouterOS apenas para estudos e testes e não possui um computador PC que poderia ser usado especificamente para a instalação?

Para contornar essa situação facilmente o que indico é que use algum aplicativo que forneça recursos de criação de máquinas virtuais. São aplicativos que possibilitam que você instale vários sistemas operacionais dentro do Windows. Com isso, você pode usar uma máquina virtual para instalar o MikroTik RouterOS dentro do Windows.

Dois nomes bem conhecidos que posso mencionar são:

- **Microsoft Virtual PC:** http://www.microsoft.com/pt-br/download/details.aspx?id=3702
- **Oracle Virtual Box:** http://www.oracle.com/technetwork/pt/server-storage/virtualbox/downloads/index.html

Se por algum motivo as URLs que citei estiverem "quebradas" ou desatualizadas, acesse a página inicial (home) de cada site (Microsoft e Oracle respectivamente) e use seus mecanismos de busca para encontrar os referidos softwares.

Outras opções de download:

- http://www.baixaki.com.br/download/microsoft-virtual-pc.htm
- http://www.baixaki.com.br/download/virtualbox.htm
- http://www.google.com.br/

Não irei entrar em detalhes à respeito da instalação desses programas. Vejamos apenas um resumo da instalação, configuração e uso do Microsoft Virtual PC:

1 - Faça o download do programa;

2 - Execute o instalado e siga os procedimentos até o fim;

3 - Ao término, vá ao menu Iniciar – Todos os Programas - Microsoft Virtual PC. Você verá uma janela semelhante à mostrada na figura;

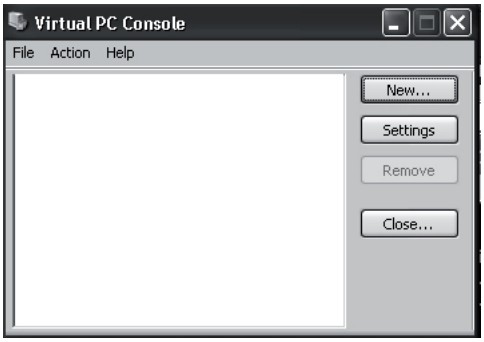


Figura 09.14: janela inicial do Microsoft Virtual PC.

4 - Clique no botão New. Irá abrir a janela do Wizard;

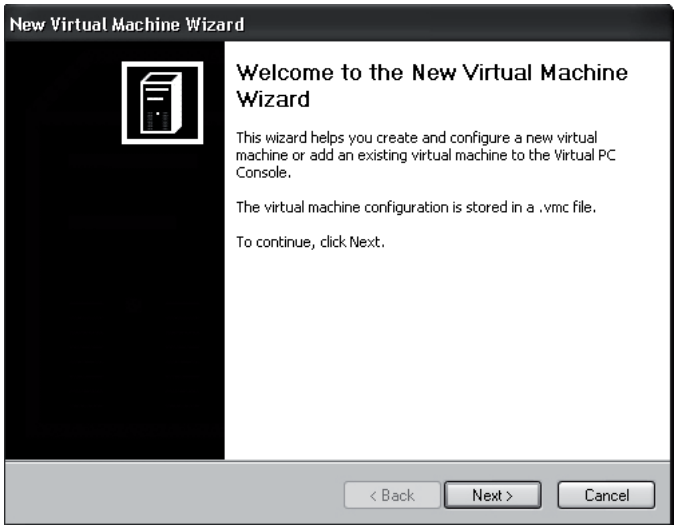


Figura 09.15: Wizard.

5 - Clique no botão Next>. Na janela seguinte, mantenha selecionada a opção Create a Virtual Machine. Clique no botão Next>;

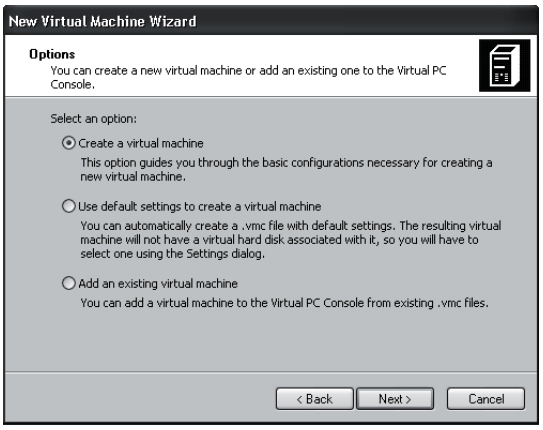


Figura 09.16: clique em Next>.

6 - Na janela seguinte, clique no botão Browser e selecione onde deseja criar a máquina virtual. Além disso, digite um nome para a máquina virtual. Clique no botão Next>;

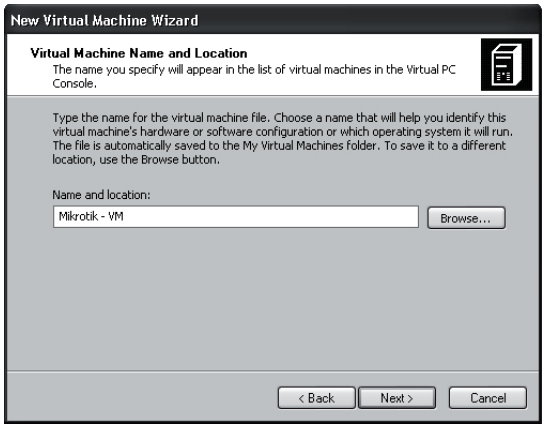


Figura 09.17: Nome e Local.

7 - Na janela Operation System, deixe a opção Other selecionada e clique no botão Next>;

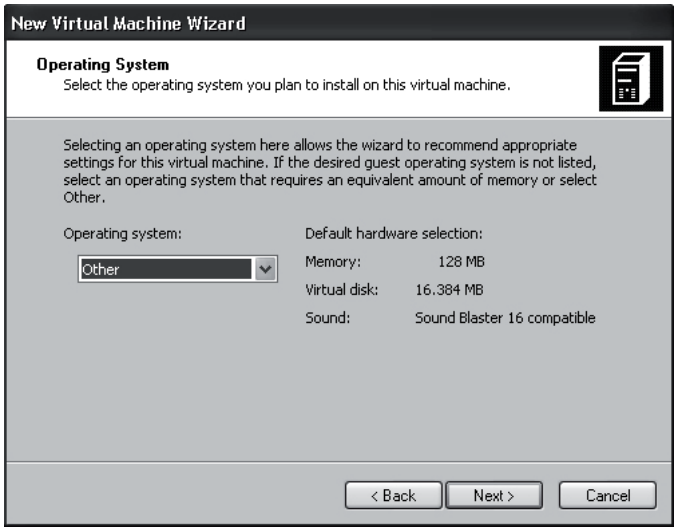


Figura 09.18: Deixe como está e clique em Next>.

8 - Na janela seguinte podemos configurar a quantidade de memória RAM. Geralmente é indicado 128 MB. Clique no botão Next>;

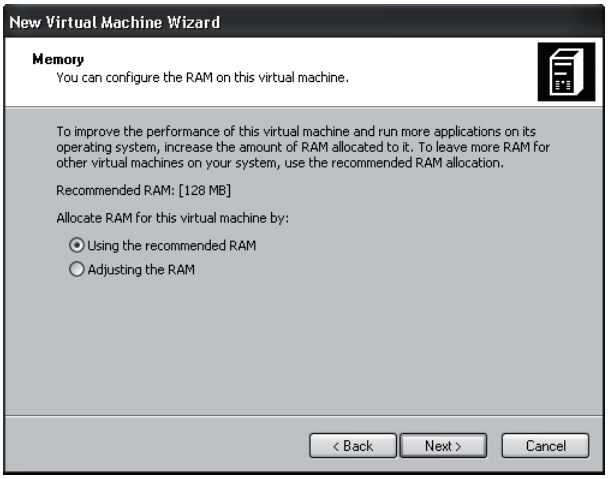


Figura 09.19: Clique em Next>.

9 - Na janela seguinte, selecione a opção A New virtual Hard Disk. Clique no botão Next>;

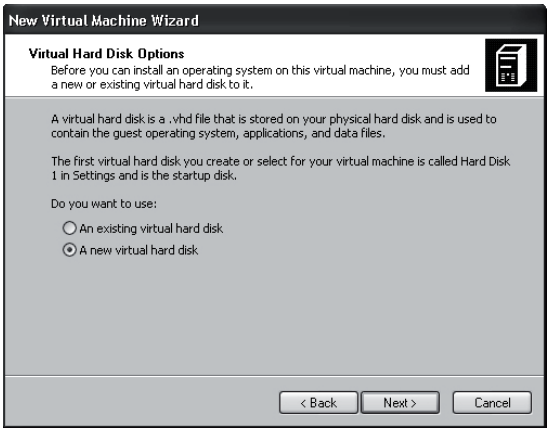


Figura 09.20: selecione a opção A New virtual Hard Disk e clique em Next>.

10 - Na janela seguinte você pode configurar o tamanho, em MB, do disco virtual. O tamanho indicado geralmente é mais que suficiente. Por isso, apenas clique em Next>;

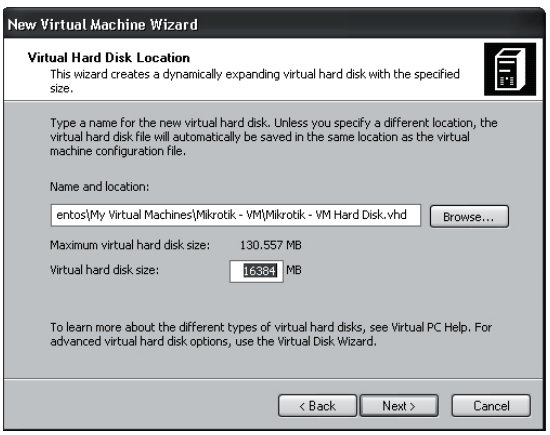


Figura 09.21: Clique em Next>.

11 - Na janela seguinte clique no botão Finish.

Figura 09.22: Clique em Finish.

Pronto, o Microsoft Virtual PC está instalado. Vá ao menu Iniciar o inicie-o. Ao abrir o programa você verá uma janela semelhante à mostrada na figura.

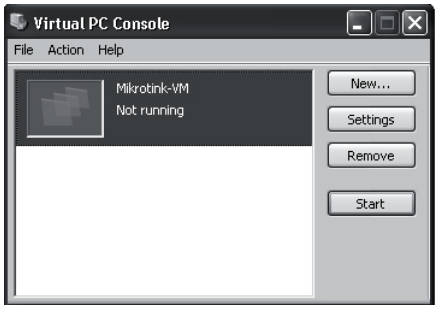


Figura 09.23: Máquina virtual criada.

Para iniciar a máquina virtual você pode clicar com o botão direito do mouse sobre ela e clicar em Start. Você verá uma janela semelhante ao prompt de comando.

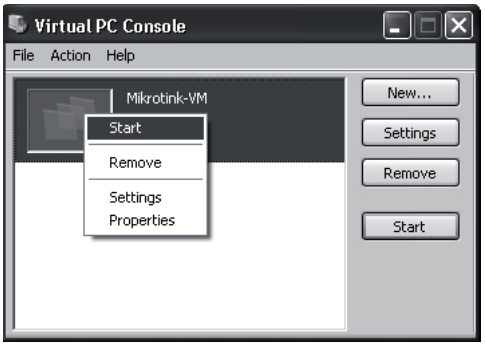


Figura 09.24: clique com o botão direito do mouse sobre a máquina virtual e clique em Star para iniciar.

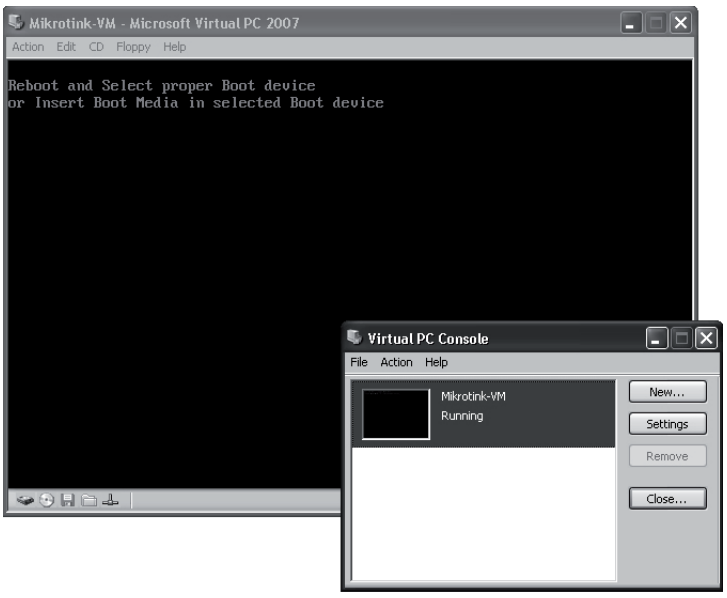


Figura 09.25: aqui vemos uma janela semelhante ao prompt de comando. A máquina virtual já está funcionando.

Caso não seja encontrada nenhuma unidade “bootável”, você verá a mensagem conforme mostrada na figura seguinte.

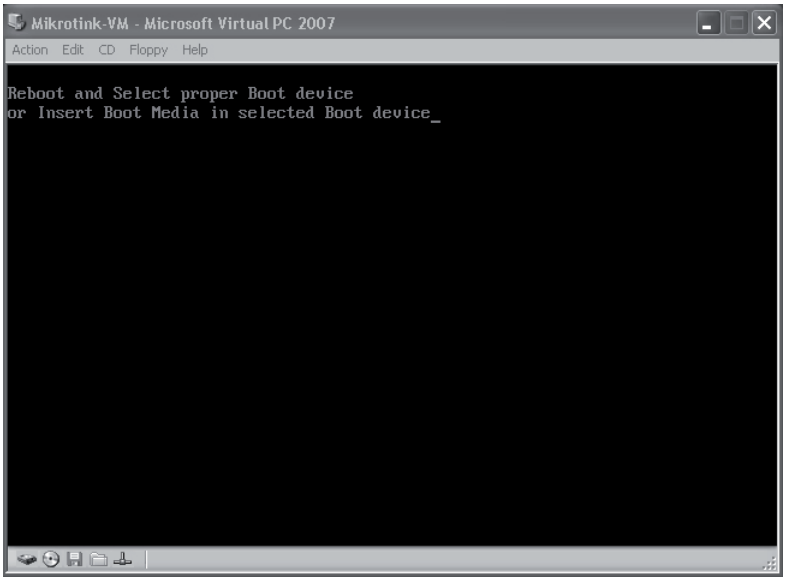


Figura 09.26: não foi encontrada nenhuma unidade “bootável”.

Nesse caso, você pode colocar o CD de instalação do MikroTik RouterOS na unidade de CD. Se não iniciar automaticamente, pressione alguma tecla do teclado ou dê um “re-boot” pelo menu Action – Reset.

A partir deste ponto você poderá instalar o MikroTik RouterOS. As etapas de instalação são as mesmas do tópico seguinte.

INSTALAÇÃO PASSO A PASSO

Finalmente vamos à instalação. O objetivo deste tópico, além de mostrar a você um passo a passo da instalação do MikroTik RouterOS, é levar até você a possibilidade de praticar o que está sendo ensinado. O ideal é que leia este tópico pondo em prática o que é mostrado. Se você não tiver um computador PC que possa ser usado para instalar o sistema a partir do zero, use uma máquina virtual como mencionei anteriormente.

Antes de irmos à instalação do sistema, vou falar um pouco sobre o hardware que seu PC vai precisar. O MikroTik RouterOS tem poucas exigências de hardware. O mínimo de memória RAM livre que o PC precisa ter é 32MB. E de HD é 64MB. É necessário ter suporte a barramentos como o PCI e/ou PCI-X para instalação de interfaces. Você pode obter mais detalhes em:

http://wiki.MikroTik.com/wiki/Manual:RouterOS_features

Como vemos, qualquer computador PC que você montar (desde que o hardware seja compatível) irá ter hardware mais que suficiente. Eu digo isso levando em consideração a prática que tenho na montagem de PCs. Hoje, você não encontra pentes de memória RAM novos que tenha somente 32 MB. E muito menos um HD novo com somente 64 MB de espaço.

Outro detalhe é que para montar um servidor completo é necessário duas placas de redes. Uma placa vai receber a internet através do seu modem por exemplo. E outra placa vai fazer comunicação com a rede. A montagem de um servidor completo é um assunto que considero bem avançado, capaz de render um livro inteiro.

Vamos à prática! Para instalar o MikroTik RouterOS faça o seguinte:

1 - Certifique-se de que o primeiro boot que está configurado no setup do seu computador seja na unidade de CD/DVD;

2 - Coloque o CD na unidade e ligue e/ou reinicie o computador (ou a máquina virtual);

3 - Ao dar o boot no CD a instalação será carregada e o seu HD será reconhecido;

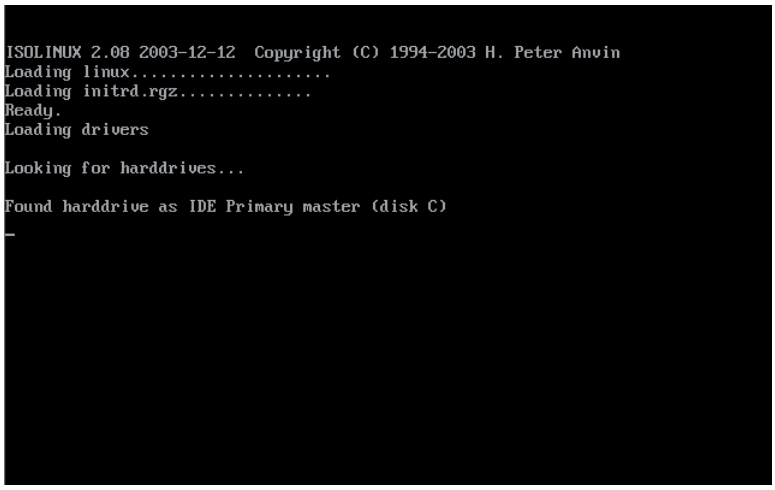


Figura 09.27: Carregamento da instalação.

4 - Em seguida já abre a tela onde devemos selecionar os pacotes a serem instalados. Esses pacotes podem ser instalados mais tarde. Mas, como a instalação ocupa pouco espaço, e por motivos didáticos, sugiro que selecione todos os pacotes;

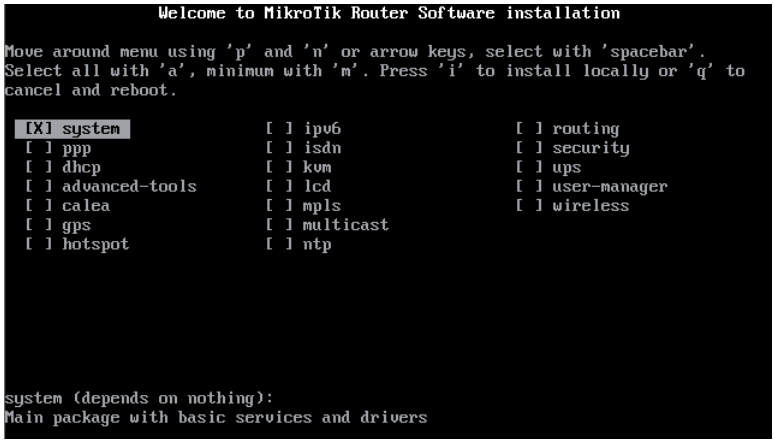


Figura 09.28: Selecione os pacotes.

5 - Para interagir nessa tela você pode usar as seguintes teclas:

- **P:** move para cima;
- **N:** move para baixo;
- **Setas direcionais do teclado:** movem para cima, para baixo, esquerda ou direita;
- **Barra de Espaço:** seleciona (marca) ou desmarca um pacote;
- **A:** marca todos os pacotes;
- **M:** marca somente o pacote mínimo (System);
- **Q:** cancela e dá um reboot;
- **I:** inicia a instalação;

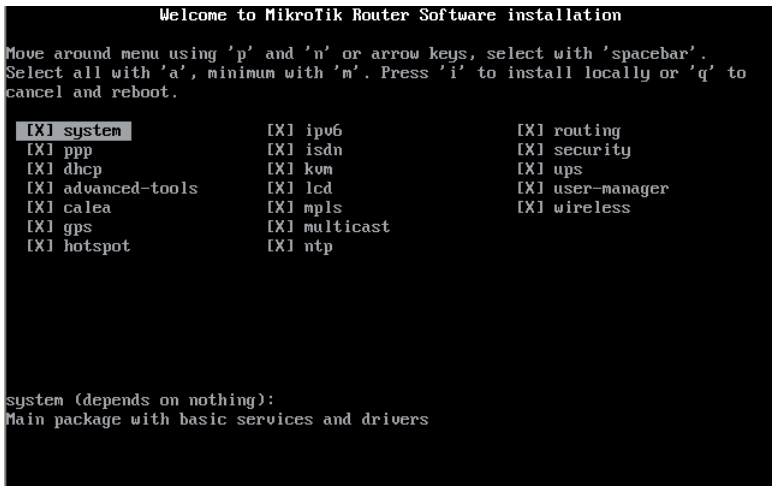


Figura 09.29: Selecionamos todos os pacotes.

6 - Ao selecionar um pacote você verá logo abaixo a descrição dele;

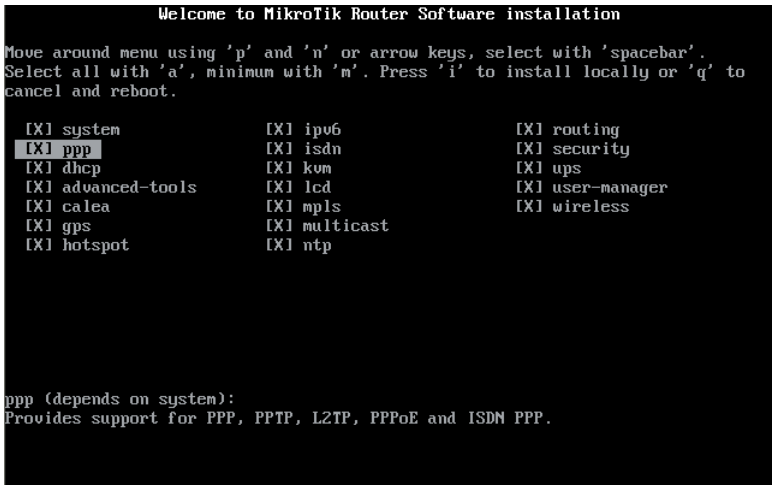


Figura 09.30: descrição de um pacote.

7 - Os pacotes existentes na versão (6.2) que estamos instalando são (veja que disponibilizei a descrição original em inglês):

- **System:** "Main package with basic services and drivers". Pacote principal com serviços básicos e drivers. A instalação desse pacote é obrigatória, podemos selecionar nenhum pacote, mas, esse é obrigatório;
- **PPP:** "Provides support for PPP, PPTP, L2TP, PPoE and ISDN PPP." Fornece suporte a servicos PPP, PPTP, L2TP, PPoE e ISDN PPP;
- **DHCP:** "DHCP client and Server". DHCP cliente e servidor;
- **Advanced-Tools:** "email client, pingers, netwatch and other utilities." Cliente de e-mail, ferramentas de diagnostic entre outros;
- **Calea:** "lawfully authorized electronic surveilance." É um pacote para vigilância eletrônica. Faz vigilância de conexões, mas, é exigido somente nos EUA;
- **GPS:** "Provides support for GPS." Fornece suporte para GPS, ou seja, para criar informações sobre posicionamento e tempo;

- **HotSpot:** “Provides HotSpot.” Para fornecer suporte a HotSpot;
- **IPv6:** “Provides support for IPv6.” Para fornecer suporte a IPv6;
- **ISDN:** “Provides ISDN support.” Para fornecer suporte a conexões ISDN;
- **KVM:** “Provides support KVM virtual machines.” Para fornecer a máquina virtual KVM. KVM são siglas de Kernel-based Virtual Machine. É uma máquina virtual que permite executar vários sistemas operacionais em um host RouterOS. Suporta as principais distribuições Linux e plataforma x86;
- **LCD:** “Provides support for LCD panel.” Para fornecer suporte a painel LCD. Esses painéis são usados para exibir informações do sistema;
- **MPLS:** “Provides support for MPLS.” Para fornecer suporte ao protocolo MPLS (Multi Protocol Label Switching);
- **Multicast:** “Provides support for PIM (platform independent multicast).” Para fornecer suporte a multicast;
- **NTP:** “NTP client and server.” NTP são siglas de Network Time Protocol. Permite obter e sincronizar a hora correta em servidores, roteadores e máquinas em redes;
- **Routing:** “Provides support for RIP, OSPF, and BGP4.” Para fornecer suportes a roteamentos dinâmicos;
- **Security:** “Provides support for IPSEC, SSH and secure connectivity with WinBox.” Fornece suporte para IPSEC, SSH e conectividade segura com WinBox;
- **UPS:** “Provides support for APC UPS.” Esse pacote fornece suporte a no-breaks APC UPS que possui recurso de sinalização inteligente. Essa sinalização inteligente funciona através da ligação de um cabo USB ou RS-232 ao servidor ou roteador. Ele permite que o servidor ou roteador administre o uso da bateria do no-break em caso de queda de energia prolongada. Funciona basicamente assim: caso a energia

caia durante muito tempo e a carga da bateria ficar baixa, o servidor ou roteador irá entrar em modo de hibernação. E quando a energia elétrica voltar o servidor ou roteador sairá do modo de hibernação;

- **User-Manager:** "RouterOS User Manager Test package." É um sistema de gerenciamento de usuário que pode ser usado para: usuário HotSpot, usuário DHCP e PPP e wireless;

- **Wireless:** "Provides support for PrismII and Atheros Wireless Station and AP." Pacote para fornecer suporte intarfeces Prism e Atheros.

8 - Ao selecionar todos os pacotes, pressionamos a tecla "i" para prosseguir com a instalação;

9 - Irá surgir a pergunta: "Do you want to keep old configuration?" Ou seja, você quer manter a configuração antiga. Caso tenha uma instalação do MikroTik RouterOS existente e queira manter a configuração antiga pressione a tecla Y (para "Yes" – Sim). Caso contrário pressione N (para "No" – Não);

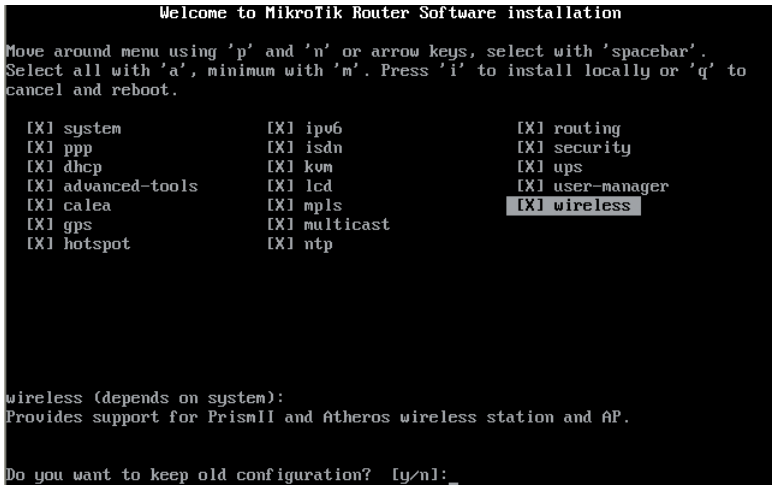


Figura 09.31: pressione Y ou N para continuar.

10 - Irá surgir agora a mensagem "Warning: all data on the disk will be

erased! Continue?" Ou seja, todos os dados do disco onde o MikroTik for instalado serão apagados. Pressione Y para continuar;

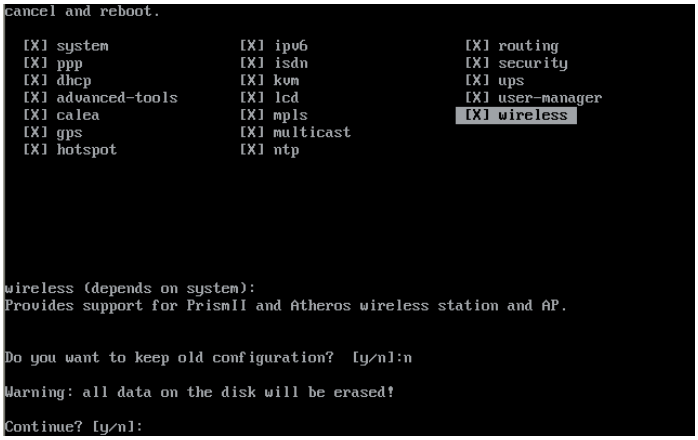


Figura 09.32: pressione Y para continuar.

11 - Será criada a partição. Em seguida ela será formatada;

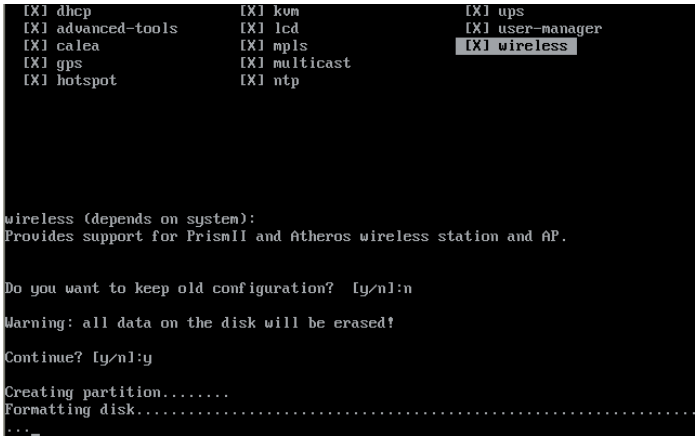


Figura 09.33: criação da partição e formatação.

12 - Os pacotes serão instalados e ao término será solicitado que você

pressione a tecla Enter para dar um reboot. Retire o CD da unidade (para não dar boot nele novamente) e pressione Enter;

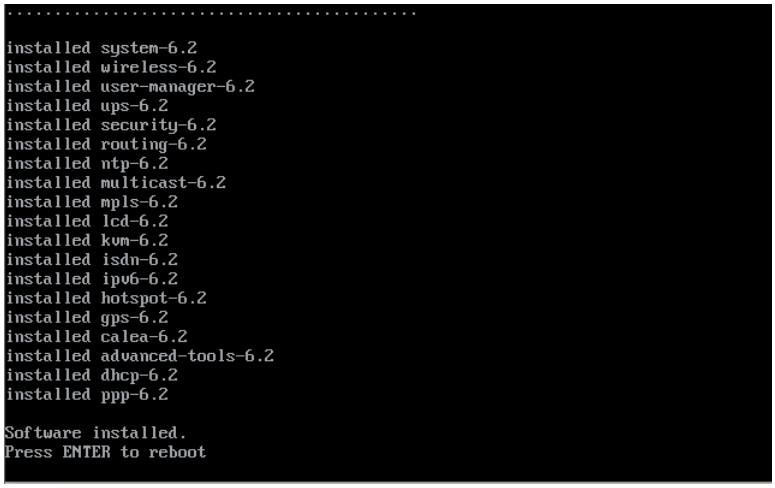


Figura 09.34: Término da instalação dos pacotes. Pressione Enter para reiniciar.

13 - O Sistema irá iniciar;

Figura 09.35: Iniciando o MikroTik RouterOS.

ACESSO INICIAL VIA CONSOLE

Ao terminar de instalar o MikroTik RouterOS já poderemos fazer o primeiro acesso. Logo após o sistema iniciar iremos nos deparar com uma tela solicitando o Login. Use os seguintes dados:

- **MikroTik Login:** admin
- **Password:** deixe em branco

Pressione a tecla Enter para confirmar cada dado.

Figura 09.36: Login e Password.

Em seguida veremos a seguinte mensagem:

“ROUTER HAS NO SOFTWARE KEY

You have xxhxxm to configure the router to be remotely accessible, and to enter the key by pasting it in a Telnet window or in WinBox.

Turn off the device to stop the timer.

See www.mikrotik.com/key for more details.

Current installation "software ID": xxxx-xxxx

Please press "Enter" to continue!”

Essa mensagem diz que o nosso router (que é o nosso PC/Servidor) não possui a licença/chave.

O prazo para inserir essa chave no sistema é de 24 horas. Mas, basta desligar o sistema que a contagem regressiva é pausada.

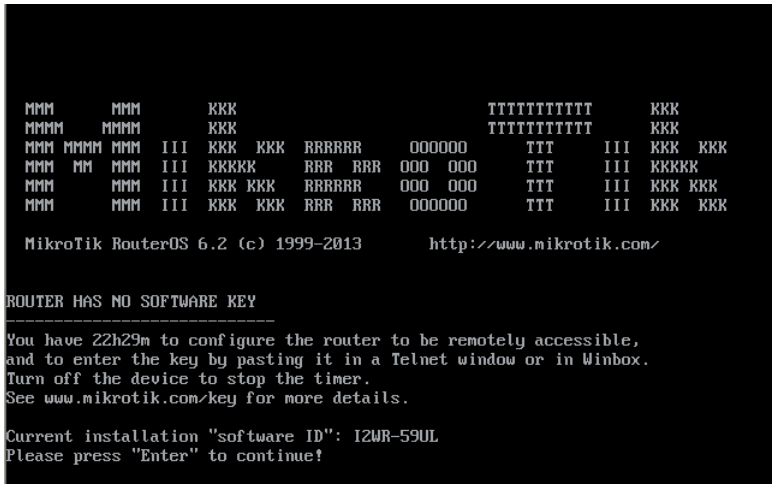


Figura 09.37: aviso sobre licenciamento.

Para darmos sequência pressionamos a tecla Enter. Neste ponto podemos acessar todas as configurações do MikroTik RouterOS. Porém, no console isso é feito através de comandos que digitamos em modo texto. As configurações são acessadas através de um sistema de diretórios hierárquicos. Dessa forma, podemos acessar esses diretórios e navegar através dos caminhos, adentrando pela hierarquia de diretórios ou voltando até chegar à raiz.

Exemplo Prático:

Digitamos:

interface

e pressionamos a tecla Enter.

Agora digitamos:

ethernet

e pressionamos a tecla Enter.

```
[admin@MikroTik] > interface
[admin@MikroTik] /interface> ethernet
[admin@MikroTik] /interface ethernet>
```

Figura 09.38: exemplo de navegação.

Para mostrar uma ajuda a respeito do diretório atual onde estamos podemos digitar o comando:

?

Para voltar um nível para trás basta digitar .. (ponto ponto) e pressionar Enter.

Para voltar para a raiz, independente do diretório onde você se encontra, digitamos / e pressionamos Enter.

WINBOX

O WinBox é um aplicativo para Windows que permite acessar e configurar o MikroTik RouterOS de forma totalmente gráfica.

Ele permite acessar o MikroTik RouterOS através do IP ou do MAC do servidor e/ou roteador onde ele está instalado. Quando fazemos uma instalação nova do MikroTik RouterOS não é configurado um IP para o computador onde ele está instalado. Mas, com WinBox podemos usar apenas o MAC para acesso.

WinBox também pode ser utilizado no Linux. Mas, entenda que ele é um aplicativo executável (*.exe) para a plataforma Windows. Para usar no Linux será necessário usar algum emulador do Linux.

Para usar o WinBox teremos que fazer o seu download no endereço:

http://www.mikrotik.com/download

Ao abrir a página, basta clicar em WinBox e fazer o download.

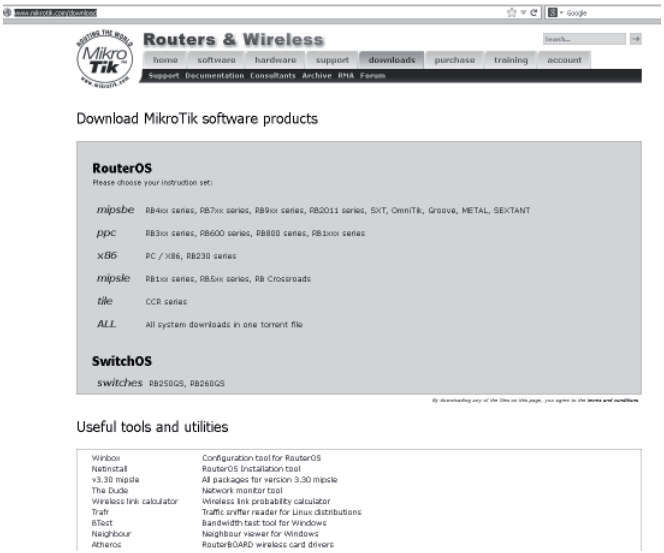


Figura 09.39: Clique em WinBox.

Ao fazer o download basta efetuar um clique duplo no arquivo winbox.exe. Não é preciso instalar, o arquivo já é pronto para uso.

Ao acessar o WinBox você verá a janela inicial, como vemos na imagem.

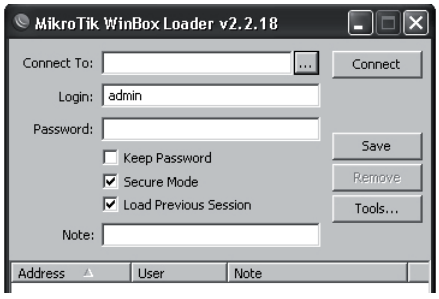


Figura 09.40: Janela Inicial do WinBox.

 : O servidor ou roteador onde está o MikroTik RouterOS que vai acessar via WinBox deve estar no mesmo barramento da rede.

 : Obviamente, o servidor ou roteador onde está o MikroTik RouterOS deve estar ligado. Mas, você não precisa logar nele via console. Apenas ligue o dispositivo e deixe o MikroTik RouterOS carregar.

 : Você pode usar o WinBox para acessar o MikroTik RouterOS que está instalado em uma máquina virtual (mesmo que esteja no mesmo computador onde está o Windows). Para isso, inicie a máquina virtual e em seguida o MikroTik RouterOS.

Na janela do WinBox teremos alguns botões e opções, que são:

- **Connect To:** Clique no botão “três pontinhos” e escolha o MAC ou IP do computador ou roteador onde está o MikroTik RouterOS;
- **Connect:** botão usado para acessar em modo gráfico;
- **Login:** nome do usuário que vai usar para acessar. O padrão é admin;
- **Password:** é a senha. O padrão é deixar em branco;
- **Keep Password:** guarda a senha digitada;
- **Secure Mode:** modo de segurança. Os dados são criptografados;
- **Load Previous Session:** carrega uma sessão anterior;
- **Note:** para digitar uma nota;
- **Save:** salva os endereços (MAC e/ou IP) e dados do usuário;
- **Remove:** remove os endereços (MAC e/ou IP) e dados do usuário que foram salvos;

- **Tools:** possui algumas opções, como exportar ou importar endereços, remover todos os endereços e limpar cache.

O básico que devemos fazer é escolher o MAC ou IP do computador ou roteador que vamos acessar, digitar o nome de usuário e senha (caso haja) e clicar no botão Connect.

Ao carregar, você verá estará conectado via WinBox em modo totalmente gráfico. Pode usar o mouse, claro. Se for uma instalação nova e que não possui licença você verá o aviso que mencionei anteriormente (“ROUTER HAS NO SOFTWARE KEY”). Basta clicar no botão Licence para inserir uma chave de licença ou em OK para com continuar sem licença.

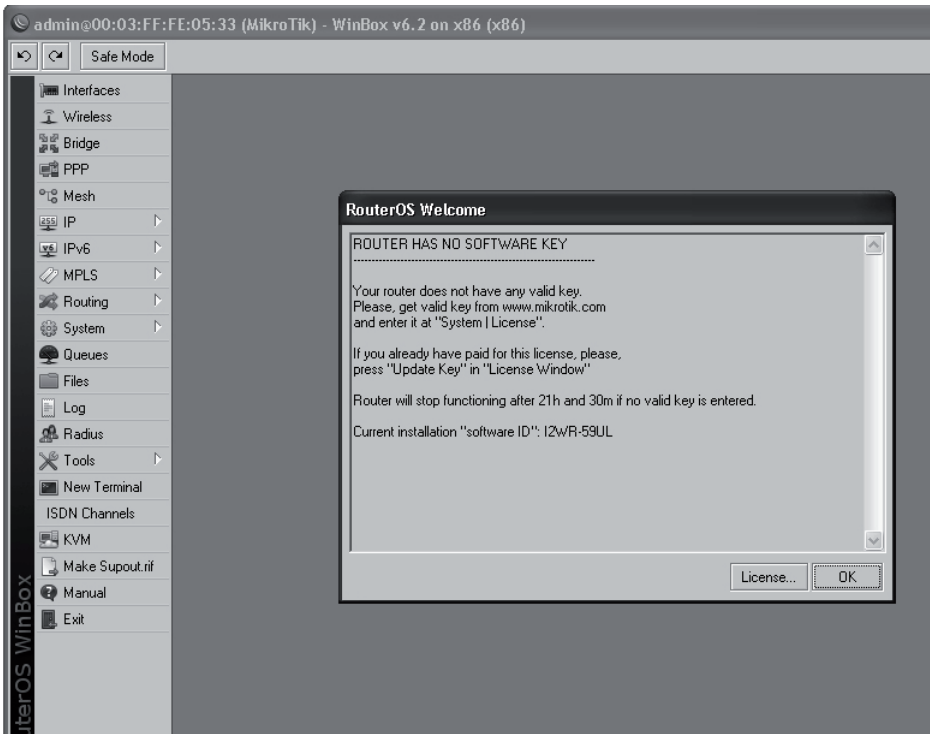


Figura 09.41: Clique em Licence para inserir uma chave de licença ou em OK para com continuar sem licença.

Navegação Básica

Agora que você já acessou o MikroTik RouterOS via WinBox é indispensável começar a se familiarizar com essa interface. Experimente “navegar” pelas janelas, ver os recursos existentes, etc. Para ajudar nesse exercício, deixo algumas instruções:

1 - Na parte superir da janela, na barra de títulos, você verá o usuário logado no momento e o endereço MAC ou IP do computador ou dispositivo onde o MikroTik RouterOS está instalado. Verá também a versão do sistema e a plataforma usada. X86 é computador PC;

Figura 09.42: Informações na barra de título.

2 - Logo abaixo você verá os botões Undo (desfazer), Redo (refazer) e Safe Mode (Modo de Segurança). O modo seguro é um recurso que te permitirá desfazer as configurações caso uma sessão tenha se perdido. Para habilitar esse modo pode-se usar as teclas de atalho Ctrl + X;

Figura 09.43: botões Undo, Redo e Safe Mode.

3 - Na esquerda da janela há um menu com os recursos do MikroTik RouterOS. Ao clicar em quaisquer um deles irá abrir uma guia (ou janela, aba, como queira) onde poderemos proceder com as mais variadas configurações. Cada guia possui os botões Maximizar, Restaurar abaixo e Fechar.

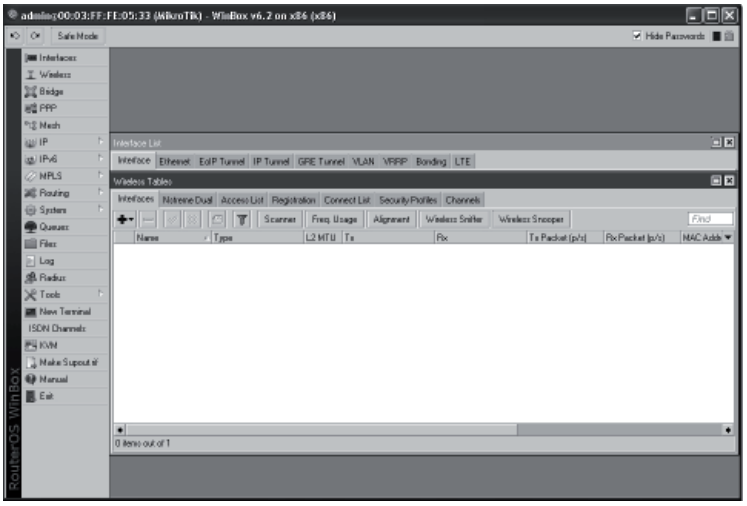


Figura 09.44: Menu à esquerda e Guias no centro.

4 - Ainda no menu à esquerda há o botão Exit para sair do WinBox.

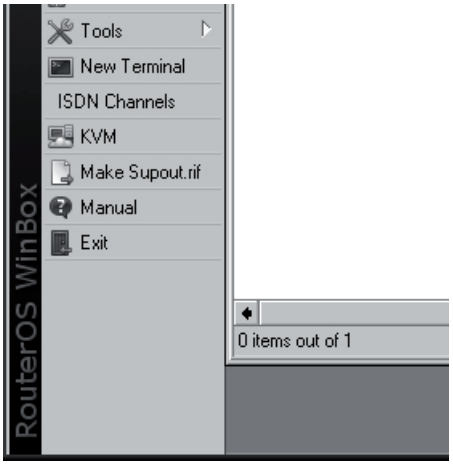


Figura 09.45: Botão Exit.

LICENCIAMENTO /O QUE É LICENÇA?

Você deve ter percebido que ao acessar o MikroTik RouterOS, após ser instalado, surge uma mensagem (em inglês) a respeito de uma chave de licença.

A licença é uma permissão para usar o MikroTik RouterOS com um conjunto de características pré-definidas. O licenciamento é dividido em níveis.

O nível 0 é a licença de demonstração. Te permite usar o MikroTik gratuitamente por 24 horas contadas. Ao desligar o computador a contagem é pausada, e ao religá-lo a contagem recomeça.

No nível 0 você consegue acessar a todos os recursos do MikroTik RouterOS. E ao adquirir uma chave de licença os recursos do MikroTik poderão ser usado de acordo com o nível adquirido.

Quando você compra uma licença você recebe um conjunto de caracteres que deverão ser inseridos no MikroTik RouterOS.

Ao comprar dispositivos RouterBoard ele já virá com o MikroTik RouterOS e uma licença de um determinado nível.

Mas, quando instalamos o MikroTik RouterOS em um computador PC obrigatoriamente deveremos comprar uma licença.

NÍVEIS

Como te disse, o licenciamento é dividido em níveis. Você pode acessar o endereço http://wiki.mikrotik.com/wiki/Manual:License e verificar uma tabela contendo todos os níveis e suas características.

Para ficar fácil, abaixo disponibilizo essa tabela. Apenas omitir os valores (em $) porque eles podem variar, não há garantias que eles serão sempre fixos.

Level number	**0 (Demo mode)**	**1 (Free)**	**3 (WISP CPE)**	**4 (WISP)**	**5 (WISP)**	**6 (Controller)**
Price	no key	registration required	volume only	***	***	***
Upgradable To	-	no upgrades	ROS v7.x	ROS v7.x	ROS v8.x	ROS v8.x
Initial Config Support	-	-	-	15 days	30 days	30days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes	yes	yes	yes

EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	300	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot	24h trial	1	1	200	500	unlimited
active users						
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Fonte: http://wiki.mikrotik.com/wiki/Manual:License

Um detalhe muito importante é que as licenças não possuem data de expiração, ou seja, você compra e pode usar ela no equipamento “eternamente”.

E vou ressaltar também que cada código de licença só pode ser usado em um único equipamento. Não adianta comprar uma licença e usá-la em um equipamento e depois tentar usá-la em um segundo equipamento. Isso porque uma licença fica vinculada ao HD ou outro tipo de memória ao qual o sistema está instalado. O que pode ser feito é usar um HD que possui o MikroTik RouterOS que já possui licença (você comprou a licença e depois inseriu nesse sistema) em outro computador.

Se o HD queimar ou for formatado por utilitários de terceiros você perde essa chave de licença e deverá comprar outra.

ONDE COMPRAR E QUANDO CUSTA?

Duas dúvidas muito comum em iniciantes é onde comprar e se as licenças são caras.

Você pode comprar as licenças em distribuidores MikroTik. Para conseguir uma lista de distribuidores, acesse:

http://www.mikrotik.com/buy

Além disso, você pode usar o Google (www.google.com.br) para pesquisar por “licenças Mikrotik”. Você encontrará diversas empresas que vendem licenças.

POR FIM, QUANTO CUSTA? É CARO?

Os preços são relativamente acessíveis. Os valores variam de acordo com o dólar. No exato momento em que escrevo este livro, a licença de nível 4 custava $45,00 (dólar). Portanto, o que posso dizer é que, até então, os valores são acessíveis e vale a pena adquirir a sua licença.

Mas, os valores podem variar. O ideal é pesquisar por algum distribuidor MikroTik e sempre entrar em contato com eles para manter-se atualizado sobre os valores.

COMO INSERIR A CHAVE DE LICENÇA

Você comprou uma chave de licença? Como inseri-la no MikroTik RouterOS? Para isso, faça o seguinte:

1 - Acesse o MikroTik RouterOS via WinBox;

2 - No menu à esquerda, clique em System - License;

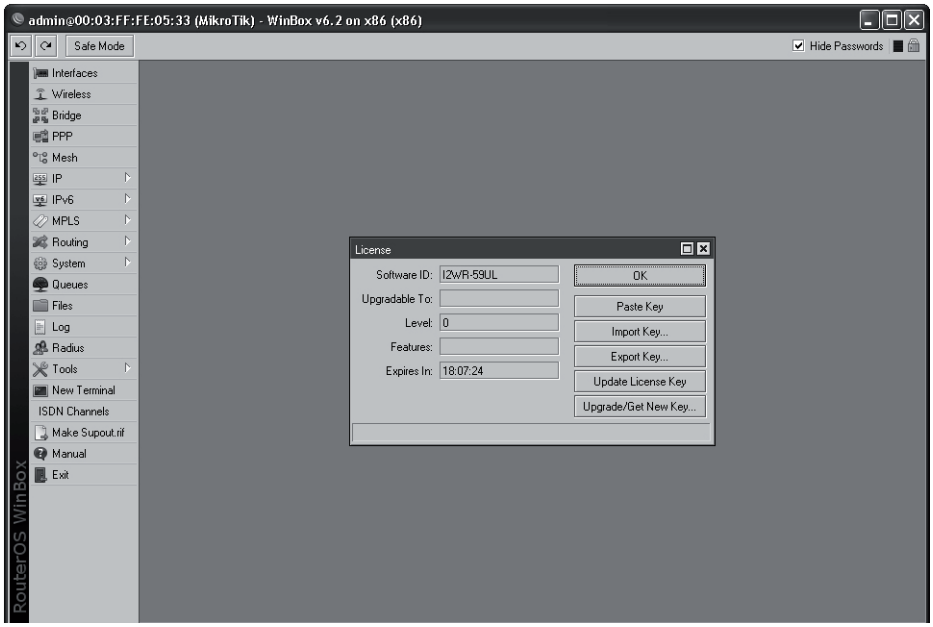


Figura 09.46: janela License.

3 - Copie a sua chave de licença (Ctrl + C);

4 - Na janela License, clique no botão Paste Key. Feito isso, clique no botão OK;

5 - Por fim, reinicie o MikroTik RouterOS.

PALAVRAS FINAIS

Chegamos ao final dessa nossa introdução. Vou relembrar o que eu disse no início deste capítulo: este capítulo é apenas um BÔNUS, ou seja, um capítulo EXTRA que estou te dando de presente. Além disso, este capítulo é apenas uma INTRODUÇÃO para você conhecer o assunto e, a partir daí, poder dar passos maiores.

Não pare de estudar aqui. MikroTik RouterOS e MikroTik RouterBoard são assuntos extensos, que exigem estudo e dedicação. O mercado é extremamente promissor. Quem domina MikroTik RouterOS e MikroTik RouterBoard torna-se um profissional diferenciado e com amplas possibilidades de trabalho.

Sucessos e continue estudando sempre.