UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

RAFAEL RAMON SANTOS

IMPLEMENTAÇÃO DE REDE MESH COM SERVIDOR CENTRALIZADO DE AUTENTICAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2012

RAFAEL RAMON SANTOS

IMPLEMENTAÇÃO DE REDE MESH COM SERVIDOR CENTRALIZADO DE AUTENTICAÇÃO

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Sistemas Para Internet do Departamento Acadêmico de Informática – DAINF – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. M.Sc. Fabiano Scriptore de Carvalho

CURITIBA
2012

A mim mesmo, que enfrentei a mais épica das jornadas para chegar até aqui.

À mulher da minha vida. Estamos quase lá, meu amor.

AGRADECIMENTOS

Agradeço imensamente o meu orientador, Prof. Fabiano. Sem a sua orientação, este trabalho jamais teria sido realizado.

Agradeço meus queridos colegas de turma por toda ajuda ao longo desta jornada, por fazerem da sala de aula um lugar tão divertido, e por tolerarem um cara como eu por tanto tempo.

Agradeço minha querida mãe, avó e tia, por cuidarem de mim em todos os aspectos, por todo o suporte e pelo amor incondicional.

Agradeço meus amigos, que com muito bom humor faziam eu me sentir menos miserável quando todos estavam em algum lugar curtindo e eu estava em casa estudando.

Agradeço à mulher da minha vida, que sempre foi compreensiva e amorosa nos inúmeros fins de semana que tive que passar longe dela.

E agradecimentos especiais para meu amigo Wilson, por ser o cara mais tolerante e atencioso do universo, e por me ajudar nos momentos em que eu não conseguia fazer mais nada. Piá, eu te devo sorvete para o resto da vida!

This is the end
Beautiful friend
This is the end
My only friend, the end
Of our elaborate plans, the end
Of everything that stands, the end
No safety or surprise, the end
I'll never look into your eyes...again
- The Doors

RESUMO

SANTOS, RAFAEL RAMON. **Implementação de uma rede sem fio Mesh com autenticação centralizada utilizando um servidor RADIUS.** 2012. Monografia de TCC (Curso de Tecnologia em Sistema para Internet). Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Este trabalho tem como tema central a implementação de uma rede padrão IEEE 802.11 utilizando a topologia em malha parcial (*Mesh*) em conjunto com um servidor RADIUS centralizado para a autenticação dos usuários. Será feito um levantamento das tecnologias de rede sem fio e as ferramentas e protocolos que permitem que estas redes sejam interligadas em malha. Visto que uma grande parte das implementações de redes sem fio corporativas é feita sem levar em consideração alguns pontos importantes na infra-estrutura de rede, este trabalho visa levantar as questões de implementações em uma rede sem fio com uma abrangência de campus, visando segurança e cobertura da rede.

Palavras chave: Redes *mesh*, IEEE 802.11, servidor RADIUS, autenticação**.**

ABSTRACT

SANTOS, RAFAEL RAMON. **Implementation of a wireless mesh network with centralized authentication using a RADIUS server.**2012. Monografia de TCC (Curso de Tecnologia em Sistema para Internet). Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

This paper has as its main subject the implementation of an IEEE 802.11 standard network, utilizing the partial mesh topology and a RADIUS central server for user authentication. A study will be conducted about the wireless technologies and protocols that allow those networks to be connected in a mesh topology. Since a great number of corporate networks are installed without taking into account some key aspects in the network infrastructure, this project intends to raise questions about implementations of wireless networks in a campus environment, having as goals the security and coverage of the network,

Key Words: Mesh networks, IEEE 802.11, RADIUS server, authentication.

LISTA DE FIGURAS

LISTA DE SIGLAS

AP	Access Point
ARPA	Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Sprectrum
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMP	Interface message processors
IP	Internet Protocol
ISM	Industrial Scientific and Medical.
ISO	International Standards Organization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MBPS	Megabit por segundo
MIMO	Multiple-Input Multiple-Output
MIT	Massachusetts Institute of Technology
NAS	Network Access Server
NCP	Network-Control Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing Protocol
OSI	Open System Interconnection
PDA	Personal digital assistant
RADIUS	Remote Authentication Dial-in User Service
RAS	Remote Access Server
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UCLA	University of California, Los Angeles

UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo será tratado o Tema, Delimitação da Pesquisa, Problemas e Premissas, o Objetivo Geral, os Objetivos Específicos, Justificativa, Procedimentos Metodológicos, Embasamento Teórico e a Estrutura deste trabalho.

Atualmente as redes sem fio estão sendo utilizadas tanto por usuários domésticos quanto em grandes corporações. Roteadores que utilizam a tecnologia Wi-Fi são tão comuns em residências quanto televisores ou fornos de micro-ondas. A implementação de redes sem fio em empresas públicas e privadas permite que os usuários tenham mobilidade, permitindo o acesso à rede tanto de dispositivos móveis (PDAs, celulares) quanto de *notebooks*. Em relação à implementação de uma rede sem fio, é possível tornar as coisas mais organizadas e eficientes. Nem sempre quem configura uma rede sem fio, seja no âmbito empresarial ou em um ambiente doméstico, implementa de forma correta. É comum empresas e outras instituições com muitos funcionários (escolas, universidades, etc.) possuírem muitos pontos de acesso à rede, e normalmente eles não estão organizados de forma eficiente. Cada ponto de acesso tem um SSID, uma chave compartilhada, e privilégios de acessos diferentes. Como funcionam de forma individual, cada ponto de acesso está limitado ao seu próprio alcance. Na maioria das vezes, todo esse "emaranhado de conexões sem fio" está afunilado por uma única rota de saída para a rede. Esta que, trabalhando com todo este descaso na infra-estrutura de rede, acaba por ser utilizada muito aquém do seu real potencial.

É possível organizar esses múltiplos pontos de acesso em uma rede em malha (*mesh*), onde todos os pontos de acesso são interconectados e funcionam como uma grande malha de roteadores. Os pacotes são encaminhados entre roteadores da rede, e ao invés de várias redes individuais de pequeno alcance, tem-se uma rede que abrange uma área geográfica de maior alcance.

Em relação à segurança do acesso à rede, pode-se utilizar uma forma de autenticação centralizada, através de um protocolo de autenticação tal qual RADIUS ou similar. Ao invés de cada ponto de acesso possuir uma chave de segurança diferente, o usuário faz um *login* utilizando uma base de dados de usuários. Esta por sua vez, proveria ou não o acesso ao cliente, mediante as diretivas associadas àquele *login*. Este conceito é similar ao modelo aplicado atualmente aos provedores de Internet.

O trabalho consiste em organizar a rede, configurar os equipamentos e implantar o servidor de autenticação, de forma integrada. Mais do que simplesmente implementar uma rede sem fio de longo alcance, este trabalho visa realizar uma exploração de conteúdo, com uma análise do problema. Partindo do princípio do estudo e aplicação de redes *mesh* para levar acesso sem fio de forma abrangente e eficiente, combinados com um servidor centralizado de autenticação, dá-se margem à aplicação deste conceito a inúmeras áreas de atuação.

Para um bom entendimento dessa pesquisa, será mostrado primeiramente o que é uma rede de computadores, como ela funciona e suas principais características. Em seguida serão abordados os conceitos de redes sem fio, seu surgimento, suas aplicações e os seus padrões de funcionamento.

Referente à interligação de redes sem fio em malha, o foco do estudo está no protocolo OLSR e no WDS. Referente à autenticação do usuário, o foco do estudo está no servidor RADIUS.

O planejamento na implantação de redes de computadores em estabelecimentos de médio e grande porte muitas vezes não considera a utilização de redes sem fio até que estas se tornem necessárias. A solução acaba resultando em mero acoplamento de pontos de acesso sem fio com configurações básicas, nem sempre de acordo com a demanda exigida. Muitas vezes é escolhida uma solução *wireless* provisória que, com o passar do tempo, torna-se permanente e causa incômodo aos administradores de rede. Falhas de segurança, perda de conectividade e desempenho tornam-se casos rotineiros.

Para remediar o problema causado pela falta de planejamento, muitas vezes é necessário deixar em segundo plano algumas características importantes, como segurança por exemplo, onde a senha é abdicada em função de problemas na autenticação. A partir disto, cada expansão da rede torna-se um problema para o administrador da rede.

É possível implementar uma infra-estrutura de rede mais adequada às necessidades reais do local. Uma rede *mesh* junto a um servidor centralizado de autenticação RADIUS provê um melhor aproveitamento do conceito de redes sem fio, proporcionando um nível considerável de comodidade aos usuários da rede e ao mesmo tempo elevando as possibilidades de controle da rede por parte dos administradores. Para uma rede de médio porte já se torna vantajosa a sua

aplicação, sendo possível expandí-la sem necessidade de alterações na configuração em uso.

O objetivo geral deste trabalho é implementar uma infra-estrutura de rede de acesso sem fio por meio de uma rede em malha (*mesh*), utilizando um servidor de autenticação centralizado via protocolo RADIUS, permitindo com isto uma melhor implementação da rede sem fio.

Os objetivos específicos deste trabalho são:

- ✓ Fazer um levantamento das tecnologias sem fio existentes no mercado;
- ✓ Verificar os firmwares existentes e escolher o que melhor se adapta à implementação;
- ✓ Configurar uma rede sem fio utilizando a tecnologia WDS para testes em redes em malha;
- ✓ Configurar uma rede sem fio utilizando o protocolo OLSR para testes em redes em malha;
- ✓ Configurar um servidor de autenticação RADIUS;
- ✓ Escolher o modelo de rede que será utilizado no projeto;
- ✓ Implementar uma topologia de rede sem fio utilizando uma rede malha parcial, com um servidor de autenticação RADIUS;
- ✓ Fazer os testes para analisar o funcionamento da implementação de redes *mesh* com a utilização de um servidor RADIUS.

Utilizar uma rede sem fio com a topologia *mesh* ao invés de dezenas ou até centenas de pequenas redes independentes pode ser uma solução eficaz. Empresas, escolas e universidades podem se beneficiar do uso de uma única rede. Na escala correta, é possível instalar redes em malha para prover a tecnologia Wi-Fi para cidades inteiras, como já tem sido feito em alguns países do mundo.

A vantagem de uma rede em malha juntamente com um servidor de autenticação não é só prover o acesso, mas provê-lo de forma eficiente e segura. Como as diferenças são apenas a nível de configuração, é possível obter todos os benefícios de uma rede *mesh* sem custo adicional algum de equipamento.

A metodologia utilizada para desenvolvimento do trabalho será fundamentalmente prática. O primeiro passo será instalar o *firmware* DD-WRT nos roteadores sem fio. Feito isso, será feita a configuração dos mesmos, para que passem a formar uma rede *mesh*. Após a configuração, serão realizados testes para

verificar o funcionamento da rede. Com a rede *mesh* funcionando, o próximo passo é configurar o servidor RADIUS. Aqui será utilizada uma máquina rodando o sistema operacional Linux, onde será instalado o FreeRADIUS, uma implementação do protoloco RADIUS livre e de código aberto. Após a instalação, configura-se o RADIUS para interagir com os roteadores e realizar a autenticação. Neste momento a rede estaria completa, e o passo seguinte seria a realização de mais testes para verificar o funcionamento.

O teste final seria um teste de campo visando testar a conectividade, disponibilidade do sinal e autenticação em todos os roteadores da rede. Todo o processo será documentado em cada uma de suas etapas.

Estruturalmente, o trabalho está organizado em quatro capítulos:

O capítulo um apresenta a Introdução, falando do tema, delimitação da pesquisa, problemas e premissas, objetivos, justificativa, procedimentos metodológicos, embasamento teórico e a estrutura descrita aqui.

O capítulo dois concentra a fundamentação teórica da pesquisa.

O capítulo três é a parte da implementação da rede sem fio utilizando a topologia em malha, com autenticação centralizada utilizando o servidor RADIUS.

O capitulo quatro contém a conclusão do trabalho e sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo tem como objetivo explanar alguns tópicos que servem como referência para a realização deste trabalho.

2.1 REDES DE COMPUTADORES

Uma rede de computadores é uma coleção de dispositivos e computadores interconectados por canais de comunicação que permitem compartilhamento de recursos e informações (CANTU, Evandro, 2003, p.3). Se pelo menos um processo em um dos dispositivos é capaz de enviar/receber dados de/para outro processo em um dispositivo remoto, pode-se dizer que os dispositivos estão em rede. As redes podem ser classificadas de acordo com uma variedade de características, como o meio físico utilizado para transportar os dados, protocolo de comunicação utilizado, escala, topologia e escopo organizacional.

2.1.1 História

Na década de 1960, a rede de comunicação dominante no mundo era a rede telefônica. A comunicação telefônica utiliza comutação por circuitos para transmitir os dados, o que permite que a voz seja transmitida a uma taxa constante entre a origem e o destino. À medida que os computadores foram ganhando importância e adquiriram capacidades de multiprogramação (*time-sharing*), buscaram-se maneiras de interligar computadores que estivessem e localidades geográficas diferentes. O tráfego gerado era provavelmente por rajadas curtas, envios de comandos e recebimentos de respostas intercalados por períodos de inatividade (KUROSE, 2006, p.40).

A comutação por pacotes passou a ser pesquisada de forma independente por Leonard Kleinrock no MIT, Paul Baran no Rand Institute, e Donald Davies e Roger Scantlebury no National Physical Laboratory, na Inglaterra. Estes trabalhos tornaram-se a fundação do que hoje é a Internet (KUROSE, 2006, p.40).

No início da década, J.C.R. Licklider e Lawrence Roberts, então colegas de Kleinrock, lideravam o programa de ciência da computação na ARPA (*Advanced*

Research Projects Agency – Agência de Projetos de Pesquisa Avançada) nos EUA. Em 1967, Roberts publicou um plano geral para a chamada ARPANet, a primeira rede de computadores por comutação de pacotes. Os primeiros comutadores eram conhecidos como processadores de mensagens de interface (*interface message processors* - IMPs) (KUROSE, 2006, p.40).

O primeiro IMP foi instalado na UCLA (Universidade da Califórnia em Los Angeles) em 1969, e ao final do ano a rede possuía quatro nós. Em 1972 a ARPANet tinha cerca de 15 nós e foi apresentada publicamente pela primeira vez. O primeiro protocolo fim-a-fim entre sistemas finais, conhecido como protocolo de controle de rede (*network-control protocol* - NCP) estava concluído, o que permitiu o desenvolvimento de aplicativos (KUROSE, 2006, p.41).

A ARPANet é uma ancestral direta da Internet como conhecemos hoje (KUROSE, 2006, p.40).

Mais redes foram surgindo em ambientes acadêmicos, e logo surgiu a necessidade de interconectar as diversas redes isoladas. O primeiro projeto nesse sentido criou uma rede de redes: o termo *internetting* surgiu para descrever esse trabalho (KUROSE, 2006, p.42).

No Havaí foi criada a ALOHANet, uma rede de pacotes por rádio que permitia que vários lugares remotos das ilhas havaianas se comunicassem uns com os outros. Este foi o primeiro protocolo que permitiu que usuários localizados em diferentes lugares utilizassem o mesmo meio de transmissão (ondas de rádio). Esse protocolo foi aprimorado e deu origem ao que futuramente seria conhecido como Ethernet (KUROSE, 2006, p.43), o padrão de redes com fio mais utilizado.

2.1.2 Modelo de referência OSI

Com o crescimento do número de redes e a consequente necessidade de interconectá-las, foi desenvolvido um modelo de referência visando à padronização dos protocolos.

O modelo OSI foi baseia-se em uma proposta desenvolvida pelo ISO (*International Standards Organization*) como um primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas. OSI significa *Open Sytems Interconnection*, interconexão de sistemas abertos, e o modelo presta-se a

tornar possível a interconexão de sistemas abertos à comunicação com outros sistemas (TANENBAUM, 2003, p. 40).

O modelo OSI tem sete camadas, conforme a figura:

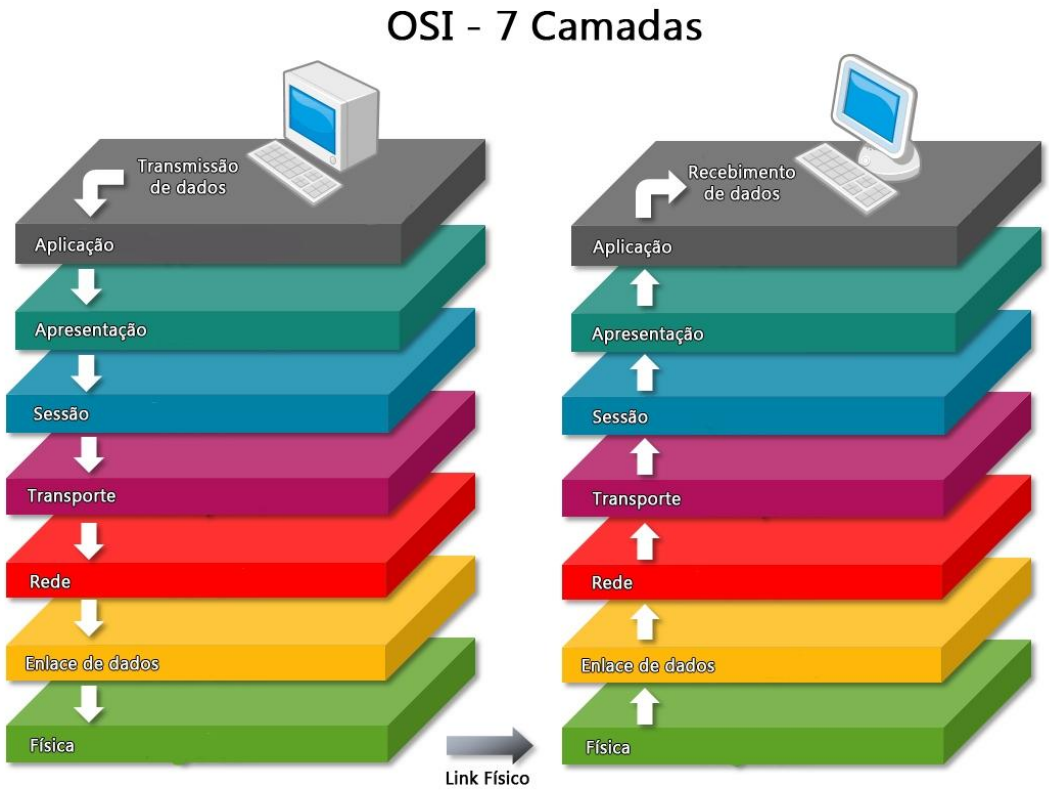

Figura 1: Camadas do Modelo OSI

Fonte: REDE/NETWORK: Explicação Resumida Camada OSI.

Os seguintes princípios foram aplicados para se chegar a cada uma das camadas (TANENBAUM, 2003, p. 41):

- Uma camada deve ser criada onde houver necessidade de um grau de abstração adicional
- Cada camada deve executar uma função bem definida
- A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente
- Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces
- O número de camadas deve ser grande o suficiente para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada, e pequeno o suficiente para que a arquitetura não se torne difícil de controlar

Resumidamente, as sete camadas são:

Camada física: trata da transmissão do fluxo bruto de bits pelo meio físico. Lida com características mecânicas, elétricas, funcionais e de procedimento para acessar o meio físico (STALLINGS, 2005, p. 97).

Camada de enlace: divide os dados de entrada em quadros de dados e transmite os quadros sequencialmente. Se o serviço for confiável, o receptor confirmará a recepção de cada quadro, enviando um quadro de confirmação. A função desta camada é transformar um canal de transmissão bruto em uma linha livre de erros. Ela também evita que uma quantidade de dados muito grande seja enviada de um transmissor muito rápido para um receptor muito lento (TANENBAUM, 2003).

Camada de rede: controla como os pacotes são roteados da origem até o destino (TANENBAUM, 2003). É responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em físicos, de forma que os pacotes consigam chegar corretamente ao destino. Também determina a rota que os pacotes seguirão, levando em consideração o tráfego da rede e outros fatores (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 12/01/2012).

Camada de transporte: responsável por receber os dados da camada superior e dividi-los em pacotes que serão transmitidos pela rede. No computador receptor, esta camada é responsável por remontar os pacotes recebidos da camada inferior (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 12/01/2012).

Camada de Sessão: permite que usuários de diferentes máquinas estabeleçam sessões entre eles. Uma sessão oferece serviços como o controle de diálogo (controla quem deve transmitir a cada momento), gerenciamento de *token* (impede que duas partes realizem a mesma operação crítica simultaneamente) e sincronização (monitora transmissões longas para que continuem de onde pararam em caso de falha) (TANENBAUM, 2003).

Camada de Apresentação: gerencia estruturas de dados abstratas e permite a definição e o intercâmbio de estruturas de dados de nível mais alto (como registros bancários), de modo a tornar possível a comunicação entre computadores com diferentes representações de dados (TANENBAUM, 2003).

Camada de Aplicação: contém uma série de protocolos comumente necessários para os usuários. Um protocolo amplamente utilizado é o HTTP (*Hyper Text Transfer*

Protocol), que constitui a base para a *World Wide Web*. Outros protocolos de aplicação são usados para transferências de arquivos, correio eletrônico e transmissão de notícias pela rede (TANENBAUM, 2003).

2.1.3 O modelo de referência TCP/IP

O modelo TCP/IP foi utilizado na pioneira ARPANET, e é usado até hoje na sua sucessora, a Internet. A ARPANET era uma rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos. À medida que a rede foi crescendo e novas universidades e repartições públicas foram conectadas por meio de linhas telefônicas dedicadas, problemas começaram a surgir. Quando surgiram redes via rádio e via satélite, os problemas com os protocolos existentes tornaram-se evidentes. Surgiu então a necessidade de uma nova arquitetura de referência, a qual tinha como uma de suas metas principais a interconexão de várias redes de maneira mais uniforme (TANENBAUM, 2003).

Devido às necessidades do Departamento de Defesa, era imperativo que as novas redes sobrevivessem a falhas repentinas de hardware (em caso de ataque, por exemplo). Enquanto as máquinas de origem e destino estivessem ativas, a transmissão de dados deveria ser mantida. Também era importante ter uma arquitetura versátil, capaz de se adaptar a aplicações com fins diversos, como transmissão de arquivos ou voz (TANENBAUM, 2003).

O modelo TCP/IP é composto de quatro camadas, em vez de sete como é o modelo OSI. A figura a seguir faz uma comparação de ambos os modelos:

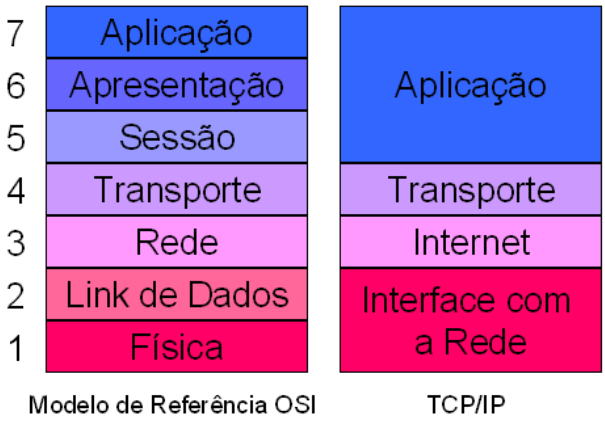

Figura 2: Modelo OSI x Modelo TCP/IP

Fonte: Como o protocolo TCP/IP funciona.

As camadas do modelo TCP/IP são:

Camada inter-redes (*internet*): Permite que os hosts injetem pacotes em qualquer rede e garante que eles cheguem de forma independente ao destino, que pode ser uma rede diferente, mesmo que cheguem em ordem diferente (cabe às camadas superiores a reorganização dos pacotes). Essa camada define um formato de pacote oficial e um protocolo chamado IP (*Internet Protocol*). Cabe a ela entregar os pacotes IP onde eles são necessários, e evitar congestionamentos (TANENBAUM, 2003).

Camada de transporte: Assim como no modelo OSI, permite que os hosts de origem e destino mantenham uma conversação. Dois protocolos foram definidos aqui. O TCP (*Transmission Control Protocol* – protocolo de controle de transmissão) e o UDP (*User Datagram Protocol* – protocolo de datagrama do usuário). O TCP é orientado a conexões, confiável, e permite a entrega ordenada e sem erros de um fluxo de bytes de uma determinada máquina para qualquer outro destinatário na inter-rede. O TCP fragmenta o fluxo de bytes em várias mensagens distintas no ato da saída e passa para a camada inter-rede. Essas mensagens são montadas na ordem correta quando chegam ao destino. O TCP também cuida do controle de fluxo entre os dois hosts, impedindo que um transmissor muito rápido sobrecarregue um receptor muito lento (TANENBAUM, 2003).

O UDP é um protocolo sem conexão e não confiável, destinado a aplicações que não precisem de controle de fluxo e manutenção da ordem do envio das mensagens. É amplamente utilizado em aplicações cliente/servidor do tipo solicitação/resposta, nas quais a entrega imediata é mais importante que a entrega precisa, como aplicações de vídeo e voz (TANENBAUM, 2003).

Camada de aplicação: contém os protocolos de nível mais alto como protocolos de terminal virtual (TELNET), transferência de arquivos (FTP), protocolo de correio eletrônico (SMTP), e o protocolo usado para buscar páginas na *World Wide Web*, o HTTP, dentre muitos outros.

Camada host/rede: o modelo TCP/IP não especifica exatamente o que ocorre abaixo da camada inter-redes. Apenas dita que o host deve conectar-se à rede utilizando algum protocolo de modo que consiga enviar pacotes IP. Esse protocolo varia de host para host e de rede para rede.

2.2 TOPOLOGIAS DE REDE

A topologia de uma rede é a disposição física em que os equipamentos encontram-se conectados, sendo, portanto o *layout* físico da rede. As topologias encontradas atualmente são: barramento, anel, estrela, ponto a ponto e malha.

2.2.1 Barramento

Todos os dispositivos são conectados ao mesmo barramento (conjunto de linhas de comunicação) físico de dados. Apenas um nó de cada vez pode escrever no barramento em um dado momento. Quando um nó está transmitindo, toda a rede fica ocupada, e caso haja outra transmissão concorrente, ocorre uma colisão, e a transmissão precisa começar novamente. Normalmente utilizada com cabos coaxiais, o cabo único é cortado em cada ponto onde será instalada uma máquina. A máquina receberá um conector em “T” onde se encaixam cada uma das pontas do cabo cortado. É uma tecnologia obsoleta. A figura a seguir mostra o esquema de uma rede em barramento:

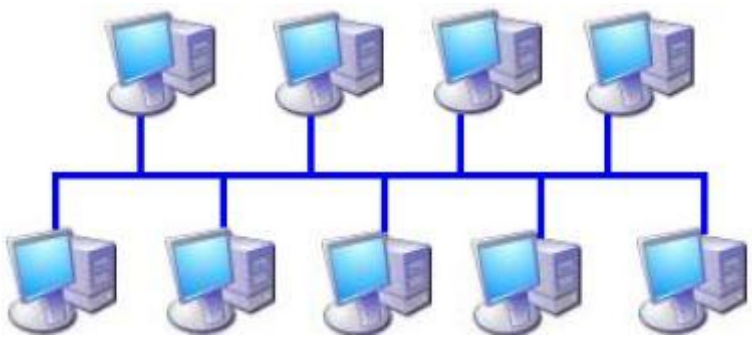

Figura 3: Topologia em Barramento
Fonte: Topologia Física em Barramento

2.2.2 Anel

Na topologia em anel, os dispositivos são ligados em série de modo a formar um circuito fechado (anel). Diferente da topologia em barramento, o anel não interliga as estações diretamente. Ele consiste de uma série de repetidores ligados ciclicamente por um meio físico, e cada uma das estações é ligada a um dos repetidores. Portanto, a qualidade do sinal mantém-se durante a transmissão, pois é

repetida seguidas vezes. A transmissão dos dados se dá unidirecionalmente, o que simplifica os protocolos de comunicação e elimina problemas de roteamento.

Uma desvantagem desta topologia é que se uma das máquinas falhar, toda a rede estará comprometida, pois o caminho unidirecional seguido pelos dados será interrompido. Assim como o barramento, esta também é uma configuração obsoleta. A figura a seguir ilustra a topologia em anel.

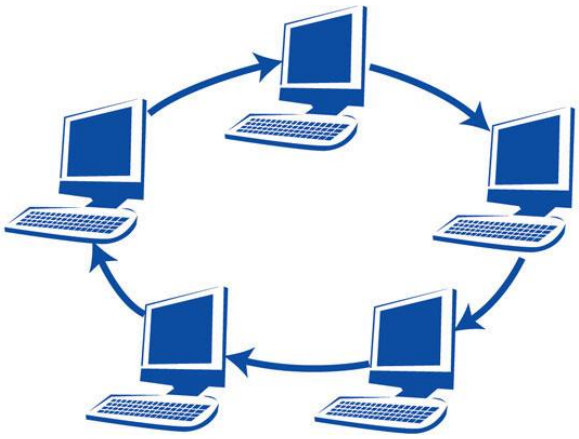

Figura 4: Topologia em Anel

Fonte: Modelos de redes de computadores de grande porte

2.2.3 Estrela

A topologia mais usada atualmente. Utiliza cabos de par trançado e um concentrador como ponto central da rede. Este concentrador transmite todos os dados para todas as estações, e tem a tarefa de saber para qual estação enviar cada pacote. Essa arquitetura facilita muito a localização de problemas na rede, pois de um dos cabos ou um dos conectores da rede falhar, apenas o nós ligado ao componente defeituoso ficará fora da rede. Em contrapartida, qualquer defeito no concentrador central irá comprometer toda a rede.

Essa topologia normalmente não se aplica a redes muito grandes, pois normalmente os concentradores (hubs e switches) não possuem um grande número de portas. A figura a seguir ilustra a topologia em estrela.

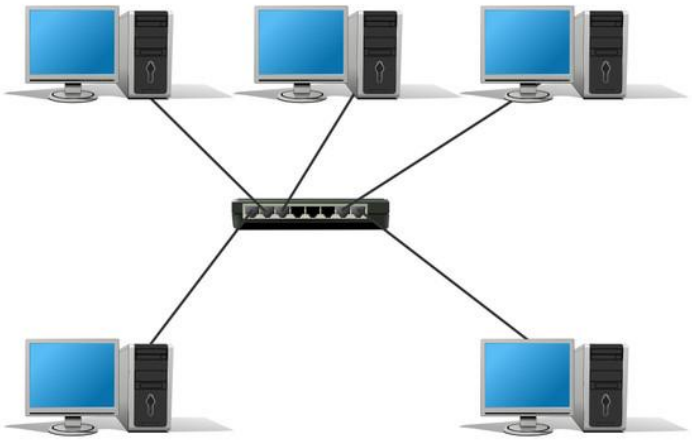

Figura 5 - Topologia em estrela
Fonte: Topologia de rede, 2011

2.2.4 Ponto a ponto

A topologia mais simples. Nada mais que uma ligação direta e permanente entre dois dispositivos, onde não se utiliza nenhum equipamento intermediário. Tem a vantagem de permitir comunicação sem impedimentos entre ambos os dispositivos. Uma maneira fácil de imaginar uma conexão ponto a ponto com meio físico dedicado é pensar no famoso telefone de lata usado pelas crianças. A figura a seguir ilustra essa topologia.

FIGURA 6 – Topologia ponto a ponto
Fonte: Redes ponto a ponto e cliente servidor.

2.2.5 Malha

Em uma rede em malha (*mesh network*), cada nó, além de receber e transmitir os seus próprios dados, também serve como um repetidor para os outros nós na rede. Em outras palavras, cada nó colabora para a propagação de dados na

rede. Uma rede em malha pode ser classificada em dois tipos: totalmente conectada (*fully connected*) ou parcialmente conectada (*partially connected*). Em uma rede totalmente conectada, cada nó tem uma ligação dedicada a cada um dos outros nós da rede. Ou seja, em uma rede de cinco nós, cada nó possuiria quatro ligações, uma para cada um dos outros nós. Em redes parcialmente conectadas, nem todos os nós possuem ligações com todos os outros. Normalmente os nós com mais ligações são os nós considerados mais importantes nas ligações com o *gateway* de internet ou com a máquina de destino.

Uma das principais vantagens das redes em malha é a sua confiabilidade. Devido ao alto grau de redundância nas conexões entre os nós, existem vários caminhos possíveis entre dois nós quaisquer. Caso um nó da rede caia, quase sempre será possível encontrar um caminho alternativo para transportar a informação. As redes em malha possuem algoritmos que automaticamente recalculam as rotas e caminhos na rede quando um ou mais nós está ausente (*self-healing algorythms,* ou algoritmos de reparo automático). Contudo, isso gera tráfego adicional na rede, pois os nós precisam trocar informações entre si para recalcularem as rotas e caminhos.

Redes em malha cabeadas demandam um alto custo de infra-estrutura por conta da quantidade de cabeamento requerida para implantação da rede, e por isso essa topologia normalmente está associada com redes de tecnologias sem fio.

Em redes malha sem fio (*wireless mesh networks*), temos normalmente os clientes (computadores, celulares, etc.) e os roteadores e/ou pontos de acesso (*access points,* ou APs). Estes devem comunicar-se entre si para encontrar o melhor caminho para o destino ou o *gateway* de internet. Com a associação de vários roteadores em uma rede *mesh* é possível cobrir uma área física considerável, que pode ser toda uma empresa, uma universidade ou um condomínio residencial, facilitando o amplo acesso à rede e à internet de forma barata e eficiente.

A figura a seguir ilustra uma rede *mesh* parcialmente conectada, onde existem vários caminhos possíveis para chegar ao *gateway* de acesso à internet.

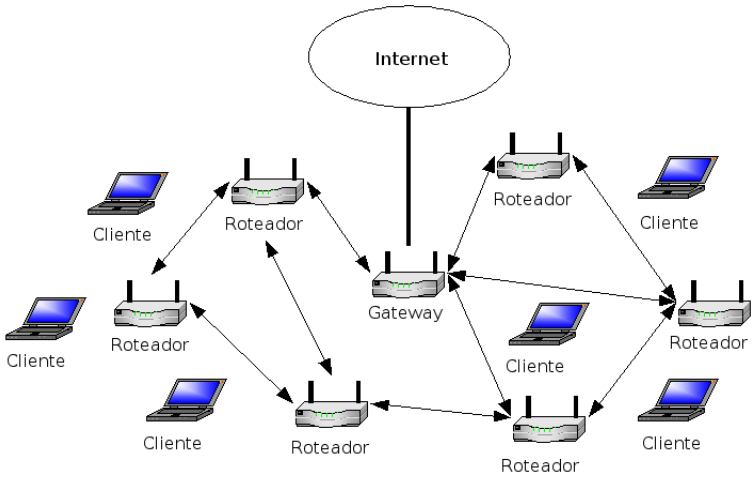

Figura 7 - Topologia em Malha

Fonte: PASSOS, Diego. Métricas de Roteamento para Redes em Malha Sem Fio, 2007, p.11.

2.3 REDES SEM FIO

"Pessoas se movem. Redes não." (GAST, 2005, p.xi). Essas duas frases ajudam a entender o recente crescimento na popularidade de redes e equipamentos sem fio. Nos últimos anos, redes sem fio deixaram de ser objetos de pesquisa científica e acadêmica, e tornaram-se tecnologia comum e disponível para as pessoas comuns. (GAST, 2005, p.xi).

As redes sem fio têm várias vantagens em relação a redes cabeadas:

Mobilidade: os usuários se movem, mas os dados são armazenados de forma centralizada, o que permite que sejam acessados "em trânsito", o que permite enormes ganhos de produtividade (GAST, 2005, p.xi).

Facilidade e rapidez de implantação: o cabeamento pode tornar-se difícil, ou impossível, em alguns lugares como prédios antigos e locais históricos, e mesmo em construções modernas a instalação de cabos pode acabar sendo muito cara e laboriosa (GAST, 2005, p.xi).

Flexibilidade: eliminação da necessidade de refazer cabeamentos antigos ou defeituosos. Mudanças de posições de trabalho em escritórios são fáceis e rápidas, pois não há necessidade de reestruturar o cabeamento de rede. A expansão da rede é quase automática, pois o meio de transmissão já está presente, não há necessidade de novos cabos. Os pontos de acesso podem ser facilmente instalados em qualquer lugar, permitindo o acesso à rede e à internet em praticamente qualquer situação (GAST, 2005, p.xi).

Custo: em vários casos os custos podem ser reduzidos utilizando-se tecnologia sem fio, como em ligações diretas entre prédios, ou pequenas redes domésticas ou em pequenas empresas.

Até o padrão 802.11 estar concluído em 1997, quem quisesse usufruir dos benefícios de redes sem fio era obrigado a adotar soluções proprietárias e fechadas, e assumir todos os riscos relacionados. Assim que o padrão foi adotado, as velocidades de transmissão aumentaram, e equipamentos padronizados facilitaram muito o projeto e implantação de redes sem fio (GAST, 2005, p.xi).

Atualmente o padrão 802.11 é um método de conexão universal. Em uma infinidade de locais públicos como hotéis, bibliotecas, cafés, universidades e muitos outros, os pontos de acesso sempre podem ser encontrados provendo acesso rápido e fácil à internet para o público geral. Combinando equipamentos 802.11 com links via satélite, é possível inclusive prover acesso à internet enquanto as pessoas se deslocam em trens e aviões.

2.3.1 O padrão IEEE 802.11

Logos após o surgimento dos *laptops*, as pessoas começaram a pensar na possibilidade de entrar em seus escritórios e serem automaticamente conectadas à internet. Várias pesquisas então foram iniciadas com esse intuito. Computadores e escritórios foram equipados com transmissores e receptores de rádio de ondas curtas para realizar essa comunicação. A partir daí, várias empresas passaram a comercializar soluções para redes locais sem fio.

Como os formatos eram proprietários e haviam sido desenvolvidos separadamente, não havia compatibilidade entre as várias soluções. Um computador equipado com transmissor da marca “X” não seria compatível com uma sala equipada com uma estação-base da marca “Y”. A partir daí ficou evidente a necessidade de um padrão para LANs sem fio. (TANENBAUM, Andrew S., p.73)

O IEEE, *Institute of Electrical and Electronics Engineers,* que foi o comitê que padronizou as LANs com fio, recebeu a tarefa de padronizar as LANs com fio. Este padrão recebeu o nome de 802.11, e também é conhecido como Wi-Fi (TANENBAUM, Andrew S., p.73).

O IEEE 802.11 compreende as duas primeiras camadas do modelo OSI, camada física e a camada de enlace de dados, conforme figura a seguir.

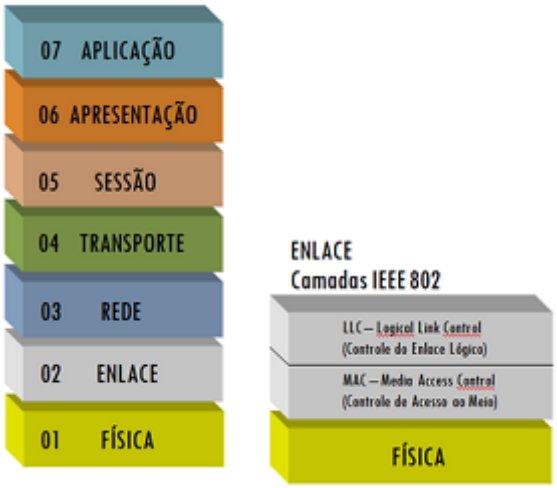

Figura 8 - Relação das camadas OSI e camadas do padrão IEEE 802.11

Fonte: Barbosa, 2010

O padrão 802.11 estabelece as camadas baixas do modelo OSI para uma ligação sem fios que utiliza ondas eletromagnéticas, ou seja:

- a **camada física**, propondo três tipos de codificações da informação
- a **camada de enlace de dados**, constituída por duas subcamadas: o controle do enlace lógico (*Logical Link Control*, ou LLC) e o controle de acesso ao meio (*Medium Access Control*, ou MAC)

A camada física define a modulação das ondas e as características da sinalização para a transmissão de dados, enquanto a camada de enlace de dados define a interface entre a máquina e a camada física, principalmente um método de acesso próximo do utilizado no padrão *Ethernet* e as regras de comunicação entre as diferentes estações. A norma 802.11 propõe na realidade três camadas físicas, definindo modos de transmissão alternativos, que serão estudadas mais adiante.

A frequência de rádio definida para uso do 802.11 foi a de 2.4 GHz, também conhecida com faixa ISM (*industrial, scientific and medic*), que é a faixa de rádio de uso industrial, científico e médico, definida pela FCC (*Federal Communications Commission*, órgão regulador das comunicações nos EUA) como a faixa do espectro de rádio que pode ser utilizada sem a necessidade de licenças especiais.

2.3.2 Modos de funcionamento do 802.11

O padrão proposto deveria funcionar em dois modos: com uma estação-base, também chamado de modo infra-estrutura, e sem uma estação base. No primeiro caso, toda a comunicação deve passar pela estação base, que na terminologia do 802.11 chama-se ponto de acesso (*access point*, ou AP). No outro caso, a

transmissão é feita entre os próprios computadores, no que é comumente chamado de rede *ad hoc*. Um exemplo disso seria duas ou mais pessoas em uma sala onde não há um AP, fazendo seus computadores se comunicarem diretamente. As figuras a seguir ilustram ambos os modos de funcionamento.

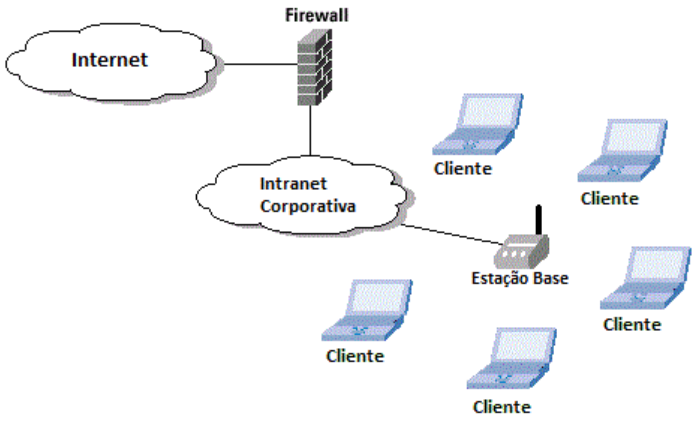

Figura 9 - modo infra-estrutura

Fonte: DANIELYAN

Figura 10 - modo ad hoc

Fonte: Viva sem fio

2.3.3 802.11 – Técnicas de transmissão

O padrão 802.11 de 1997 define três técnicas de transmissão para as redes sem fio: uma utilizando infravermelho e outras duas utilizando métodos de radiofrequência: o FHSS (*Frequency Hopping Spread Spectrum*) e o DSSS (*Direct Sequence Spread Spectrum*). Em 1999, foram apresentadas duas novas técnicas para alcançar maior largura de banda: o OFDM (*Orthogonal Frequency Division Multiplexing*) e o HR–DSSS (*High Rate Direct Sequence Spread Spectrum*) (Tanenbaum, 2003). As técnicas mais populares estão definidas pelos protocolos

802.11b e 802.11g, que são anexos ao padrão original. Esses padrões utilizam a faixa de frequência de 2.4GHz, e, portanto podem ocasionalmente sofrer interferência de outros aparelhos, tais como fornos micro-ondas, telefones sem fio e dispositivos Bluetooth, e tais técnicas de transmissão visam minimizar esses efeitos. Essas técnicas serão explicadas a seguir.

2.3.3.1 Infravermelho

São utilizados como meio de transmissão raios próximos à luz visível. Pelo fato dos sinais infravermelhos não ultrapassarem paredes, e por estarem sujeitos a interferências, esta técnica de transmissão é restringida a ambientes fechados, operando a 1Mbps ou 2 Mbps. Existem duas formas de realização das comunicações infravermelhas: reflexão (difusão) ou linha direta (direta). Na primeira, a comunicação entre o emissor e um ou mais receptores é realizada através de um ponto de reflexão. Para que isso seja possível, não deve existir nenhum obstáculo entre as estações móveis e o ponto de reflexão, permitindo que todas as estações "enxerguem" o ponto de reflexão. Quando a comunicação é direta, os sinais transmitidos pelos raios infravermelhos são focados e dirigidos diretamente a um receptor, sem a necessidade de um "ponto intermediário" para permitir a comunicação. Como exemplo, temos o controle remoto de um aparelho de televisão ou uma transferência de arquivos entre dois computadores portáteis. (Forouzan, 2004)

2.3.3.2 FHSS

Frequency hopping spread spectrum (FHSS): A banda de frequência é dividida em 79 canais de frequência com 1 MHz de largura, sedo que é gerada uma sequência pseudo–randômica destes canais, por onde o sinal é difundido. É necessário garantir o sincronismo de todas as estações, para que elas mudem para as mesmas frequências de forma simultânea, utilizando igualmente os canais da sequência. Isso pode ser assegurado com a utilização de um mesmo gerador de números pseudo–aleatórios. Em um determinado momento, um canal desta sequência é utilizado por curto período de tempo para transmissão dos dados. Com o sincronismo entre receptor e o transmissor, considerando que a série de canais

deste é conhecida pelo receptor, a informação será totalmente recuperada, fornecendo, além disso, maior segurança, já que um intruso não poderá espionar as transmissões se não conhecer a sequência de saltos ou o tempo de parada, além de menos suscetibilidade a interferências. A principal desvantagem desse método é a sua baixa largura de banda (Rufino, 2005). Essa técnica de modulação é usada no padrão 802.11 original, mas não em suas alterações.

2.3.3.3 DSSS

DSSS (*Direct Sequence Spread Spectrum*): o tempo de cada bit é dividido em n subintervalos chamados de "chips". Cada estação possui uma sequência pseudo–aleatória de "n" bits, chamada sequência de chips. Para enviar o bit 1, uma estação envia uma sequência de chips. Para enviar o bit 0, é enviado o complemento de sua sequência de chips. A DSSS usa uma sequência de 11 bits para espalhar os dados antes de transmiti-los. Cada bit transmitido é modulado por esta sequência. Este processo espalha a energia de radiofrequência em torno de uma banda de faixa larga que pode ser necessária para transmitir o dado. O receptor concentra o sinal de radiofrequência recebido para recuperar o dado original (Rufino, 2005).

2.3.3.4 OFDM

OFDM (*Orthogonal Frequency Division Multiplexing*): para se transmitir um grande volume de informações, o canal de transmissão é dividido em vários subcanais, cada um com uma portadora independente. Na sua forma de implementação, o OFDM é chamado de *coded OFDM* (COFDM). O COFDM quebra uma portadora de dados de alta velocidade em várias portadoras de velocidades menores, e todas transmitem em paralelo. Cada portadora de alta velocidade é de 20 MHz e possui 52 subcanais, cada um com aproximadamente 300 kHz. Quatro subcanais são utilizados para a correção de erros e para manter a coerência do sinal de frequência. Os 48 subcanais restantes são para dados. O COFDM provê um robusto transporte em diferentes ambientes, onde a transmissão dos sinais de rádio é refletida por vários pontos (Rufino, 2005).

2.3.4 Variantes do 802.11

A versão original do 802.11 foi lançada em 1997 e revista em 1999, mas hoje está obsoleta. Ela especificava duas taxas de transmissão: 1Mbit/s ou 2 Mbit/s, definia três técnicas de transmissão (infravermelho, FHSS e DSSS) e definiu a frequência de rádio a ser utilizada como a de 2.4 GHz.

2.3.4.1 802.11b

Em 1999 foi lançada uma atualização denominada 802.11b. Esta versão poderia estabelecer conexões nas seguintes velocidades: 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps. O intervalo de frequências é o mesmo do padrão original, mas a técnica de transmissão limita-se ao DSSS, devido à inadequação do FHSS às normas do FCC. Em teoria, a área de cobertura do 802.11 pode chegar a 400m em campo aberto e 50m em ambientes fechados.

O padrão 802.11b foi o primeiro a ser adotado e produzido em larga escala, assim sendo um dos responsáveis pela popularização das redes Wi-Fi (ALECRIM, 2008).

2.3.4.2 802.11a

Foi disponibilizado no final de 1999, quase na mesma época da versão b. Pode trabalhar com as seguintes taxas de transmissão: 6, 9, 12, 18, 14, 36, 48 e 54 Mbps. Seu alcance geográfico é de cerca de 50 metros. A principal diferença para o padrão original é sua frequência de operação, que é de 5Ghz. O uso desta frequência é conveniente pois é pouco usada e estaria pouco suscetível a interferências. Porém, muitos países não possuem regulamento para essa frequência, e a diferença de frequências poderia gerar dificuldades de comunicação com dispositivos operando no padrão original e no padrão 802.11b.

2.3.4.3 802.11g

Foi disponibilizado em 2003 e é totalmente compatível com a versão b, sendo considerado seu sucessor natural. Um dispositivo 802.11g pode comunicar-se com

um 802.11b sem problemas, a única limitação sendo a taxa de transmissão deste último.

A principal vantagem do padrão g é poder trabalhar com taxas de transmissão até 54 Mbps, tal e qual o padrão 802.11a, ao mesmo tempo em que mantém a frequência de 2.4 GHz. Sua área de cobertura é praticamente a mesma do padrão 802.11b, e a técnica de transmissão utilizada é OFDM, mas quando um dispositivo 802.11g comunica-se com um dispositivo 802.11b, a técnica de transmissão utilizada passa a ser o DSSS.

2.3.4.4 802.11n

O desenvolvimento desta especificação começou em 2004 e foi finalizado em setembro de 2009. Durante este período foram lançados vários dispositivos compatíveis com a versão incompleta do padrão, que é um sucessor totalmente compatível do 802.11g, tal como este foi do 802.11b.

Este novo padrão é capaz de combinar várias vias de transmissão (antenas) de modo a aumentar consideravelmente a velocidade de transmissão, através de um esquema chamado de *Multiple-Input-Multiple-Output* (MIMO). Com isso é possível usar múltiplos emissores e receptores para o funcionamento da rede.

Uma das configurações mais comuns neste caso é o uso de APs que utilizam três antenas e estações que usam três receptores. Somando isso ao aprimoramento das especificações, o padrão 802.11n seria capaz de fazer transmissões na casa dos 300 Mbps e teoricamente seria capaz de alcançar 600 Mbps.

Este padrão pode trabalhar tanto com 2.4 GHz quanto com 5 GHz de frequência, o que, em teoria, faz com que ele seja retroativamente compatível com os padrões anteriores, inclusive com o 802.11a. Sua técnica de transmissão é o OFDM com alterações, agora chamado MIMO-OFDM. Especula-se que sua área de cobertura pode passar de 400 metros.

2.3.5 Canais de transmissão

O 802.11 divide a sua banda de frequência em canais. Por exemplo, a banda de 2.4000 – 2.4835 GHz é dividida em 13 canais em intervalos de 6 Mhz, com o canal 1 centralizado em 2.412 GHz e o canal 13 centralizado em 2.472 GHz. O

802.11b foi baseado em formas de onda DSSS que usam 22 MHz e não tem bordas acentuadas. Consequentemente, apenas três canais não se sobrepõem. O padrão 802.11g possui quatro canais que não se sobrepõe, pois usam sinais de 20 MHz com formatos de onda OFDM. A figura abaixo ilustra a divisão dos canais:

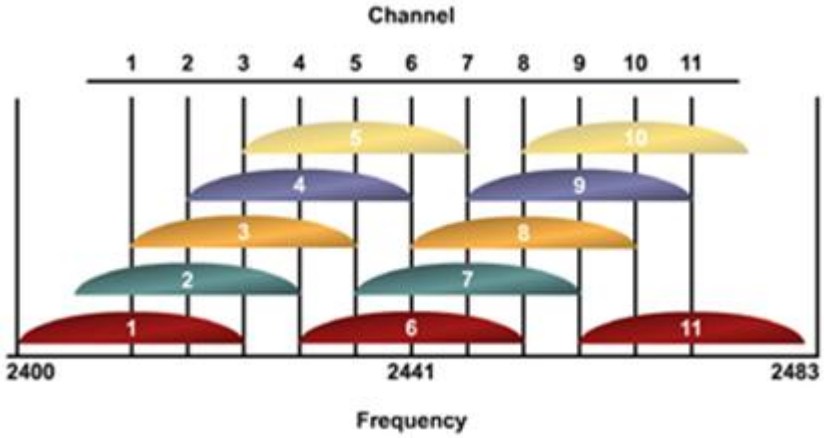

Figura 11 - Divisão de banda em canais

Fonte: Peixoto, 2011

2.4 O PROTOCOLO RADIUS

Remote Authentication Dial In User Service (RADIUS) é um protocolo de rede que provê gerenciamento centralizado de autenticação, autorização e contas (*Authentication, Authorization and Accounting,* AAA), para que outros computadores se conectem e utilizem serviços de rede. Foi desenvolvido em 1991 pela Livingston Enterprises, Inc., em 1991 como um protocolo de acesso, autenticação e contas a servidores, e mais tarde virou um dos padrões da *Internet Engineering Task Force* (IETF) (VOLLBRECHT, 2006).

Devido ao amplo suporte e à ubiquidade do protocolo RADIUS, é frequentemente usado por provedores de Internet e empresas para gerenciar acesso à Internet ou redes internas, redes sem fio e serviços integrados de e-mail.

O RADIUS é um protocolo cliente/servidor que funciona na camada de aplicação, usando UDP como transporte. O servidor de acesso remoto, o servidor de VPN (*Virtual Private Network*, ou rede virtual privada), o switch de rede com autenticação baseada em portas, o servidor de acesso à rede (Network Access Server, NAS), todos eles são *gateways* que controlam o acesso à rede, e todos possuem um componente cliente do RADIUS que se comunica com o servidor RADIUS, que normalmente é um processo rodando em *background* em um servidor Windows ou UNIX (POSEY, 2006).

O protocolo RADIUS desempenha três funções:

- Autenticar usuários e/ou dispositivos antes de conceder acesso à rede
- Autorizar usuários e/ou dispositivos a determinados serviços de rede
- Manter um registro de uso destes serviços (*accounting*)

2.4.1 Autenticação e autorização

O usuário ou estação manda uma requisição para um Servidor de Acesso Remoto (*Remote Access Server*, RAS) buscando obter acesso a um determinado recurso da rede, utilizando credenciais de acesso. As credenciais são passadas ao RAS via protocolo da camada de enlace (por exemplo, protocolo ponto-a-ponto, no caso de alguns provedores de Internet), ou postado em um formulário seguro HTTPS.

Em seguida, o RAS manda uma RADIUS *Access Request* (requisição de acesso) para o servidor RADIUS, solicitando autorização para garantir o acesso via protocolo RADIUS (RIGNEY, 2000).

Essa requisição inclui credenciais de acesso, tipicamente em forma de nome de usuário e senha, ou certificado de segurança provido pelo usuário. Além disso, a requisição pode conter outras informações conhecidas pelo RAS sobre o usuário, como o seu endereço na rede ou número de telefone, e informações a respeito da conexão física com o RAS.

O servidor RADIUS verifica se a informação está correta usando algum esquema de autenticação conhecido como o PAP (*Password Authentication Protocol*, protocolo de autenticação por senha). A identificação do usuário é verificada, juntamente com outras informações relacionadas à requisição (opcional). Historicamente, os servidores RADIUS verificam a informação de usuário usando um banco de dados local de arquivo único. Servidores RADIUS mais modernos podem usar o arquivo simples, ou referir-se a fontes externas, como bancos de dados relacionais ou servidores LDAP para verificar as credenciais dos usuários (POSEY, 2006).

O servidor RADIUS então retorna uma de três respostas para o RAS:

Access reject – o usuário tem seu acesso negado a todos os recursos de rede. As razões incluem falha na autenticação (identificação inválida) ou uma conta desconhecida ou inativa (RIGNEY, 2000)

Access challenge – demanda informação adicional do usuário como uma segunda senha, número PIN, *token* ou cartão de segurança. *Access challenge* também é usada em autenticações mais complicadas onde um túnel seguro é estabelecido entre a máquina do usuário e o servidor RADIUS de uma maneira que as credenciais de aceso ficam escondidas do RAS (RIGNEY, 2000).

Access accept – o usuário recebe acesso. Uma vez que esteja autenticado, o servidor RADIUS checará periodicamente se o usuário tem autorização para usar o serviço de rede requisitado. Um usuário pode usar a rede wireless de uma empresa, mas não a sua VPN, por exemplo. Essa informação também pode ser armazenada localmente em um arquivo simples, ou em uma fonte externa como um servidor LDAP ou banco de dados (RIGNEY, 2000).

Cada uma dessas três respostas pode incluir uma mensagem de resposta que pode conter a razão para rejeição do acesso, demandar outras informações, ou mensagem de boas vindas. O texto pode ser mostrado ao usuário em uma página web.

Atributos de autorização são adequados aos termos de acesso estipulados pelo RAS. Por exemplo, os seguintes atributos de autorização podem estar incluídos em um *Access-Accept:*

- Endereço de IP que será atribuído ao usuário
- Conjunto de endereços IP de onde será escolhido o endereço do usuário
- Tempo limite que o usuário deverá permanecer conectado
- Lista de acesso, fila de prioridades ou outras restrições ao acesso do usuário

A figura abaixo ilustra o fluxo de autorização e autenticação do RADIUS:

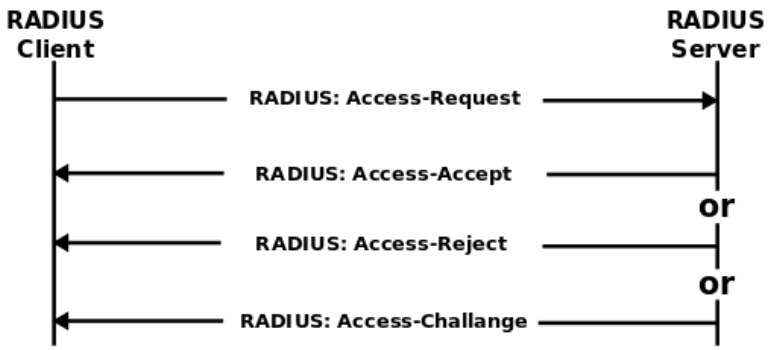

Figura 12 - Fluxo de autenticação e autorização do RADIUS

Fonte: Wikipédia

2.4.2 *Accounting*

Quando o acesso à rede é garantido pelo NAS, um *Accounting Start*, pacote RADIUS de requisição de *accounting*, contendo um atributo de status com o valor *start*, é enviado pelo NAS para o servidor RADIUS para sinalizar o início do acesso do usuário à rede. O “start” normalmente contém a identificação do usuário, endereço de rede, ponto de conexão e um identificador único de sessão (POSEY, 2006).

Periodicamente, registros de *Interim Update,* um pacote de requisição de *accounting* contendo um atributo de status com valor *interim-update*, são enviados pelo NAS para o servidor RADIUS, para atualizá-lo sobre o status de uma sessão ativa. Os registros de “interim” normalmente levam informações sobre a duração da sessão e informações sobre a utilização dos dados.

Por fim, quando o acesso do usuário à rede é fechado, o NAS envia um registro *Accounting Stop*, um pacote de requisição de *accounting* com atributo de status *stop*, para o servidor RADIUS, fornecendo informações finais sobre o uso em termos de tempo, pacotes transferidos, dados transferidos, razão para desconexão e outras informações relacionadas ao acesso do usuário à rede (POSEY, 2006).

Essas informações podem ser muito úteis para vários propósitos como cobrança, nas redes onde o acesso é pago, ou utilizadas para fins estatísticos e monitoramento da rede.

A figura abaixo ilustra o fluxo de *accounting* do RADIUS:

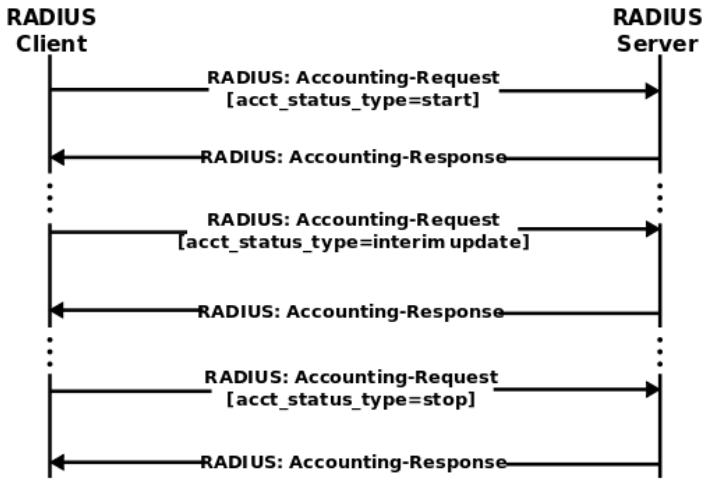

Figura 13 - Fluxo de autenticação e autorização do RADIUS

Fonte: Wikipédia

2.5 DD-WRT

O DD-WRT é um firmware alternativo baseado em Linux, compatível com um grande número de roteadores e sistemas embarcados operantes nos padrões 802.11 a/b/g/n. Foi desenvolvido com o objetivo de fornecer facilidade no uso e configuração, ao mesmo tempo em que adiciona várias funcionalidades adicionais aos equipamentos nos quais é instalado, além de ganho de desempenho (About DD-WRT, 2011) .

Possui uma grande comunidade de usuários que dá suporte aos desenvolvedores do firmware, o que permite que defeitos e bugs no seu funcionamento sejam encontrados e corrigidos de maneira bastante ágil. Suporte ao seu uso e configuração é amplamente disponível nos fóruns e na *wiki* dos desenvolvedores, bem como guias *how-to* (About DD-WRT, 2011).

Para dispositivos usados para propósitos privados, o DD-WRT é totalmente gratuito. Plataformas usadas para propósito comercial requerem uma licença paga, onde é possível também configurar os parâmetros da WLAN, tornando possível a criação de infra-estruturas de rede robustas e confiáveis. Suas principais características são (About DD-WRT, 2011):

- Suporta mais de 200 dispositivos diferentes
- Fácil de operar e configurar
- Suporta todos os padrões atuais de WLAN (802.11 a/b/g/n)
- Suporta implantação em ambientes externos
- Suporta frequências aprimoradas
- Integração com VPN
- Suporta sistemas com vários *hotspots*
- Gerenciamento de largura de banda
- Interface em vários idiomas

Além dessas características, o DD-WRT também possui suporte aos protocolos RADIUS e OLSR, o que em conjunto permitem a implantação de uma rede sem fio usando a topologia em malha.

2.5.1 OLSR

O *Optimized Link State Routing Protocol* (protocolo otimizado de roteamento de estados de enlace) é um protocolo de roteamento IP otimizado para redes móveis *ad hoc*, que também pode ser utilizado em outras redes *ad hoc* sem fio. É um protocolo baseado nos estados dos enlaces (*link-state*), que usa mensagens para descobrir e disseminar informações sobre o estado dos enlaces pela rede. Cada nó usa essa informação para computar os próximos saltos para todos os nós na rede, utilizando os menores caminhos (SCHILLER, 2011).

O OSLR é um protocolo pró-ativo, ou seja, ele troca informações com os outros nós da rede em intervalos regulares, mantendo assim atualizadas as informações sobre os caminhos da rede, mesmo que não haja tráfego. Ele utiliza os chamados *multipoint relays* (MPRs). Em protocolos de estado de enlace, quando um nó recebe um pacote com informações sobre o estado da rede, ele o encaminha para seus vizinhos, que encaminham para seus vizinhos, e assim sucessivamente. Esse mecanismo é chamado de inundação (*flooding*). Cada nó recebe o mesmo pacote dos seus vizinhos várias vezes, o que gera um grande tráfego adicional, e o problema é agravado pelo fato do OSLR sem um protocolo pró-ativo, que está sempre trocando informações entre os nós. O objetivo dos MPRs é minimizar o problema de *flooding*, escolhendo alguns nós estratégicos na rede para realizar a transmissão de informações (SCHILLER, 2011).

Cada nó possui um ou mais MPRs, que são os responsáveis por transmitir os pacotes que se originam dele. A escolha desses é feita seguindo o princípio de que ele consiga alcançar todos os nós a dois saltos de distância passando pelo menor número de MPRs possível. Ou seja, através dos MPRs o nó de origem deve alcançar qualquer nó a dois enlaces de distância.

As figuras abaixo ilustram a diferença entre a inundação normal e a inundação usando os MPRs, que estão em negrito (SCHILLER, 2011).

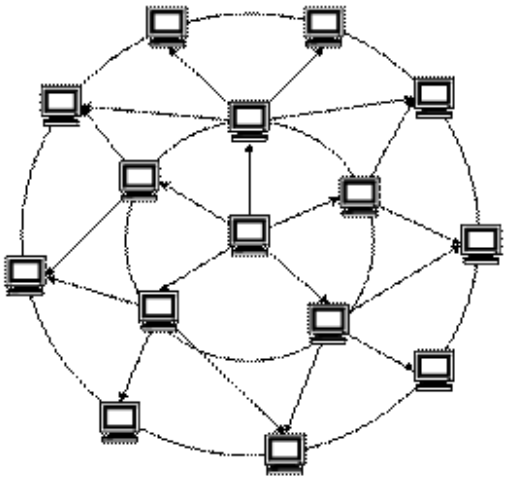

Figura14 - *flooding* normal
Fonte: SCHILLER, 2011

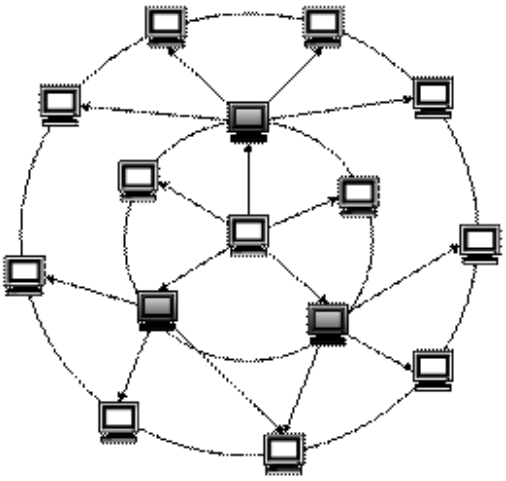

Figura 15 - *flooding* com MPRs
Fonte: SCHILLER, 2011

2.5.2 WDS

O *Wireless Distribution System*, ou sistema de distribuição sem fios, é um sistema que permite a interconexão de APs sem o uso de fios em redes 802.11. Ele permite que uma rede sem fio expanda-se utilizando vários pontos de acesso sem haver a necessidade de um *backbone* cabeado para conectá-los.

Um AP pode ser uma estação base principal, repetidora ou remota. Uma estação base principal normalmente está conectada (via cabo) à rede Ethernet. Uma estação repetidora retransmite dados entre estações base remotas, clientes sem fio e outras estações repetidoras. Uma estação base remota aceita conexões de clientes sem fio e redireciona-as para estações repetidoras ou estações principais. Conexões entre clientes são feitas usando o endereço MAC ao invés de especificar endereços IP (Everything You Need To Know About Wireless Bridging and Repeating, 2011).

Todas as estações base em um sistema WDS devem ser configuradas para usar o mesmo canal de rádio, método de criptografia (nenhum, WEP ou WPA) e as mesmas chaves. Eles podem ter SSIDs diferentes. O WDS também requer que cada estação base seja configurada de modo a encaminhar tráfego para outras no sistema.

O WDS pode ser incompatível entre produtos diferentes, mesmo do mesmo fabricante, pois não é certificado pela Wi-Fi Alliance.

Existem dois modos de conexão entre APs:

- Bridging, onde os APs comunicam-se somente entre si e não permitem o acesso de clientes sem fio e estações
- Repeating, onde os APs comunicam-se entre si e com estações sem fio

Duas desvantagens de usar o WDS são:

- A saída de dados máxima sem fio é diminuída pela metade depois da primeira retransmissão. Por exemplo, dados dois roteadores conectados usando WDS, e a comunicação está sendo realizada entre um computador ligado, via cabo, ao roteador A, e um laptop conectado sem fio ao roteador B, a saída cai pela metade, porque o roteador B precisa retransmitir a informação durante a comunicação de ambas as máquinas. No entanto, caso a comunicação seja feita entre um computador ligado com fio ao roteador A, e um computador ligado com fio ao computador B, a saída de dados não cai pela metade, pois não há necessidade de retransmissão.
- Chaves de criptografia dinamicamente associadas e revezadas normalmente não são suportadas pela conexão WDS. Isso significa que tecnologias populares de segurança como o WPA, onde as chaves são associadas dinamicamente, na maioria dos casos não podem ser usadas, embora usar WPA com chaves pré-compartilhadas seja possível. Isso se deve à falta de padronização nesta área, que talvez seja resolvida com a chegada do padrão 802.11s. Somente chaves estáticas WEP e WPA podem ser usadas em conexões WDS, incluindo estações que estejam associadas à AP funcionando como repetidor WDS (Everything You Need To Know About Wireless Bridging and Repeating, 2011).

3 PROCEDIMENTOS EXPERIMENTAIS

Neste capítulo serão descritos os procedimentos experimentais realizados para implementação de uma rede sem fio em malha com autenticação centralizada usando o protocolo RADIUS.

3.1 PREPARAÇÃO

O primeiro passo é gravar substituir o firmware original do roteador pelo DD-WRT. O processo é simples e consiste de quatro passos:

- *Hard reset* do roteador usando o botão apropriado para isso
- Fazer *logon* no roteador usando o a interface web do mesmo
- Fazer *upload* do *firmware*
- Novo *Hard reset* do roteador

Uma vez realizado esse processo, o roteador está com o DD-WRT instalado e pronto para ser configurado.

3.2 CONFIGURAÇÃO DO ROTEADOR

Para configurar o roteador, basta conectá-lo a um computador usando um cabo de rede comum (UTP). No computador, basta abrir o navegador de internet e digitar o endereço padrão do roteador, normalmente 192.168.1.1. Essa é a página que aparecerá:

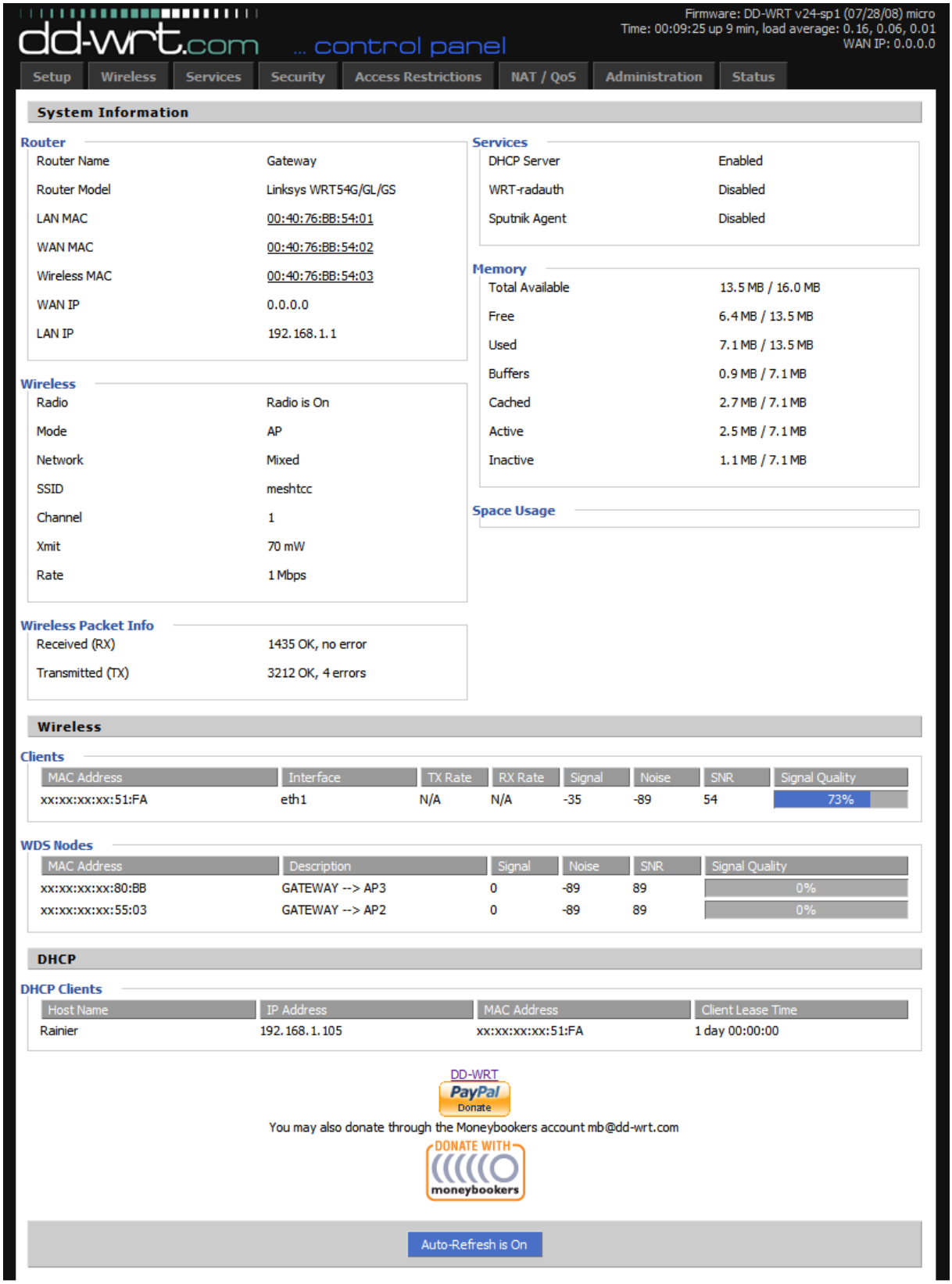

Figura 16 - Página inicial do DD-WRT

Fonte: autoria própria

Ao clicar na aba Setup, aparece o *prompt* para digitar o nome de usuário e senha. Após a autenticação, é possível alterar os parâmetros de configuração do roteador, tantos os básicos tais como endereço IP e máscara de sub-rede, bem como parâmetros mais avançados de funcionamento. A figura abaixo mostra a tela de configurações básicas:

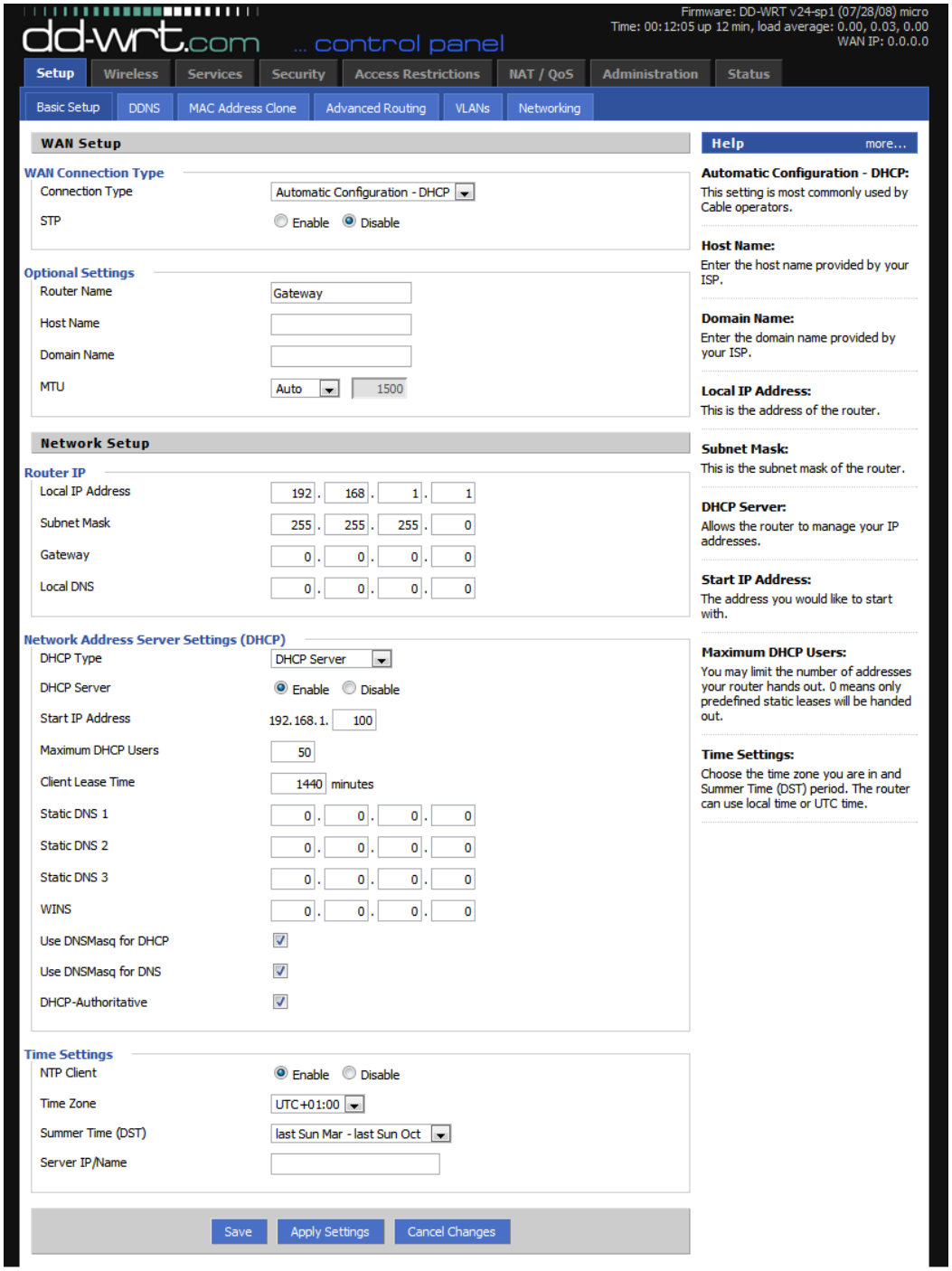

Figura 17 - Configurações básicas do DD-WRT

Fonte: autoria própria

A configuração do roteador é feita alterando-se os campos para os valores e modos de configuração adequados à nossa rede. Se o planejamento da rede foi bem realizado e sabe-se previamente como ela deve funcionar, a configuração em si é fácil de ser feita, o que facilita na implantação de um projeto de rede.

3.3 IMPLANTAÇÃO DA REDE

Primeiro cenário: rede *mesh* utilizando OLSR e roteadores Linksys.
Equipamentos: roteadores Linksys modelo WRT54GS.
Versão do DD-WRT: v24-sp1.
Configurações necessárias:

Para utilizar o protocolo OLSR, é necessário configurar os roteadores em modo ad hoc. O modo de operação do roteador deve mudar para “Router OLSR”. Esse modo de operação automaticamente desliga as funções de NAT do roteador, que precisam ser habilitadas novamente, usando iptables.

Essa configuração apresentou os seguintes problemas:

- A rede está funcionando em modo ad hoc, e não no modo infra-estrutura. Por conta disso, não seria possível ter autenticação centralizada com um servidor RADIUS.
- Não seria possível utilizar um servidor DHCP para atribuir os endereços IP automaticamente. A configuração de endereço IP e *gateway* padrão teria que ser feita manualmente ao se conectar na rede.

O resultado final seria uma rede onde um usuário comum poderia ter dificuldades para realizar a configuração, e o serviço de autenticação seria precário, pois não se poderia utilizar um serviço completo e com funcionalidades administrativas como o RADIUS.

Segundo cenário: rede *mesh* utilizando WDS e roteadores TP-Link.
Equipamentos: roteadores TP-Link modelo TL-WR741ND
Versão do DD-WRT: v24-sp2.

Aqui, o protocolo de roteamento escolhido foi o WDS. A sua característica fundamental é que os vizinhos de cada roteador devem ser especificados

manualmente, enquanto que no OLSR as rotas na rede são calculadas automaticamente.

Portanto, é preciso especificar em cada um dos roteadores quais são seus dois vizinhos mais próximos. Isso tem uma consequência: como cada roteador está ligado com apenas outros dois, e não com todos os roteadores da rede, ela será uma rede *mesh* parcial, não total.

As vantagens de utilizar o WDS são:

- É possível utilizar um servidor DHCP para atribuir automaticamente os endereços IP na rede
- Os APs funcionarão no modo infra-estrutura e não ad hoc

Ambos os fatores fazem com que esta configuração de rede seja mais tradicional e mais amigável ao usuário.

3.3.1 Mapa da Rede

Inicialmente a rede foi planejada para três APs. Nesse caso particular, os três APs formam uma rede *mesh* total, mas qualquer número acima de três faz com que a rede seja *mesh* parcial, pois cada nó estaria ligado com apenas dois vizinhos, e não com todos os outros nós da rede. O diagrama de abaixo ilustra como a rede deverá ser implantada:

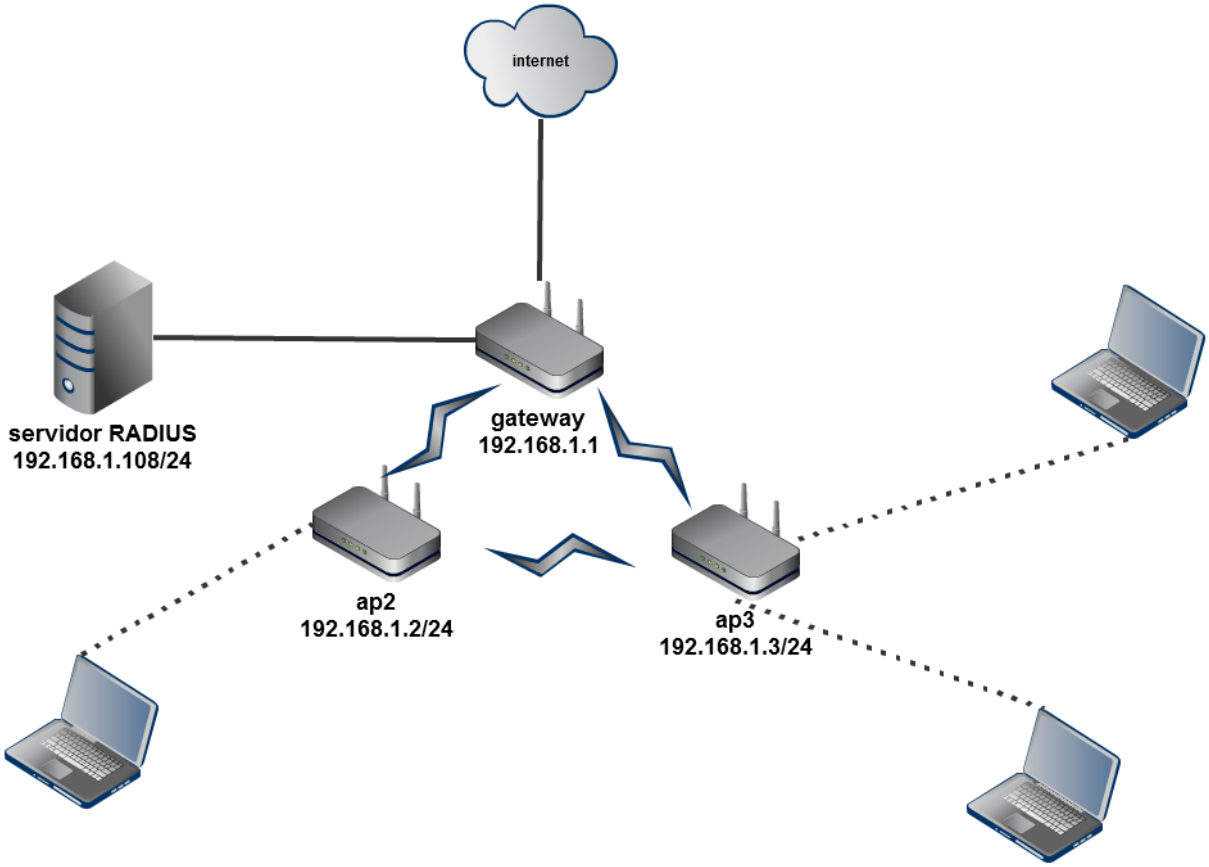

Figura 18 - Diagrama final da rede

Fonte: Autoria própria

O AP1, ou gateway, é o único que tem conexão com a Internet, via cabo. Ele também está conectado por cabo ao servidor RADIUS, onde será realizada a autenticação dos usuários da rede. Os outros servidores fazem a sua comunicação com o gateway, servidor RADIUS e com a Internet exclusivamente por rádio.

3.3.2 Configuração dos roteadores

Depois de fisicamente ligados e conectados todos os integrantes da rede, é hora de configurar os roteadores. O gateway ficará responsável também por distribuir os endereços IP para os clientes conectados na rede, portanto é preciso configurar o seu servidor DHCP. Nos demais roteadores, o DHCP ficará desativado.

Configuração do gateway

O restante da configuração do gateway é diferente da configuração dos outros roteadores. A configuração do gateway deve ficar como apresentado a seguir:

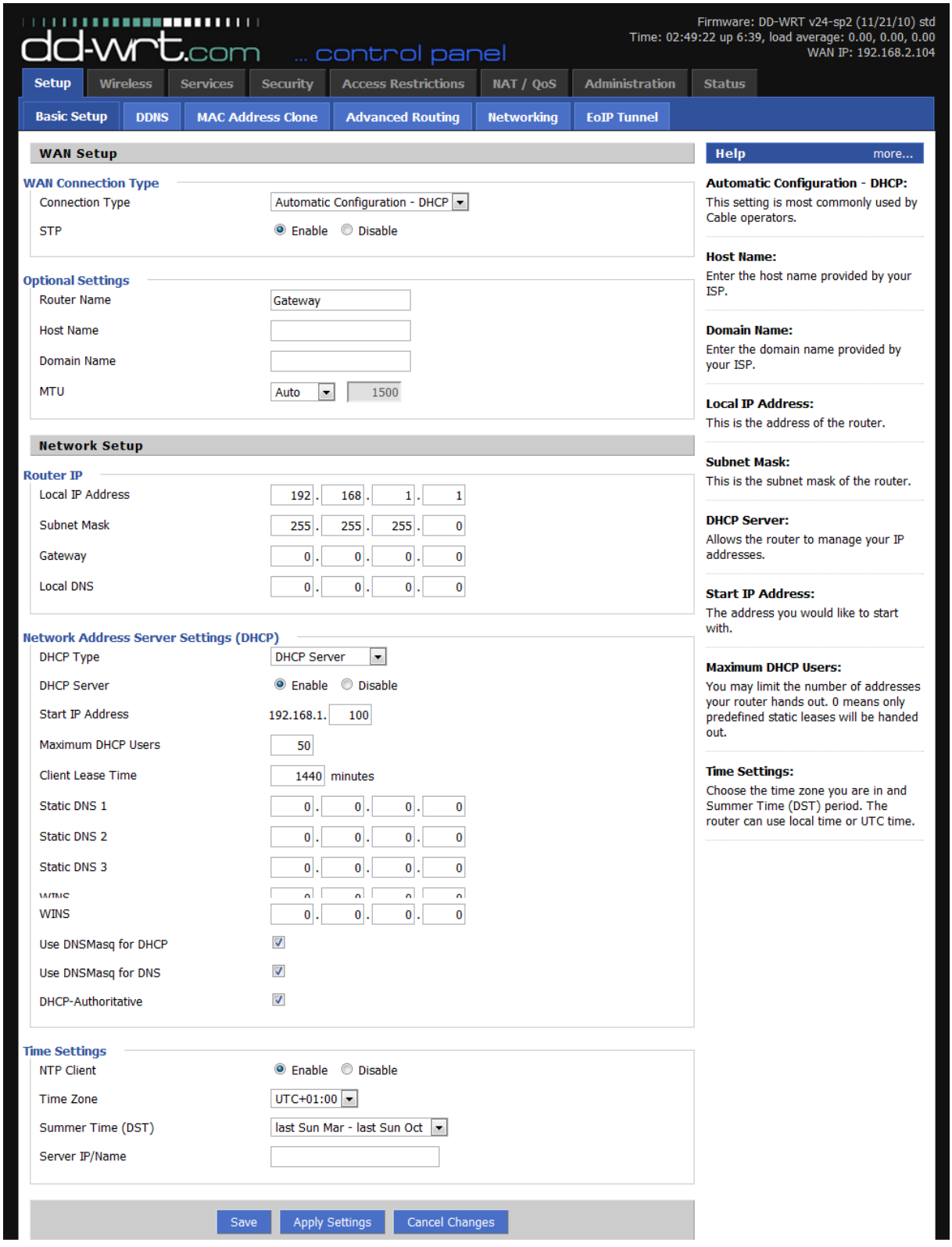

Figura 19 - Configurações básicas do DD WRT para o gateway

Fonte: Autoria própria

SETUP - BASIC SETUP

WAN Connection Type

Connection Type: Automatic Configuration – DHCP

É como o *gateway* irá se conectar à Internet. No caso, configuração automática e obtenção de endereço IP por meio de DHCP.

STP: Enable

Esse é o *Spanning Tree Protocol*, que precisa ser habilitado para que os roteadores consigam calcular as rotas em redes *mesh* com mais de dois roteadores.

Router Name: Gateway

Opcionalmente, podemos configurar o nome do roteador, o que ajuda na organização da rede, principalmente na medida em que ela for crescendo.

Router IP

Local IP Address: 192.168.1.1

O endereço IP do gateway na rede local, conforme o diagrama da rede.

Subnet Mask: 255.255.0.0

Máscara da sub-rede de acordo com o diagrama da rede.

Network Address Server Settings (DHCP)

DHCP Type: DHCP Server

DHCP Server: Enable

Start IP Address: 192.168.100

As opções acima habilitam o servidor DHCP, e configuram-no para começar a distribuir os endereços IP começando pelo 192.168.1.100.

As demais opções nesta página podem ser deixadas com o valor padrão.

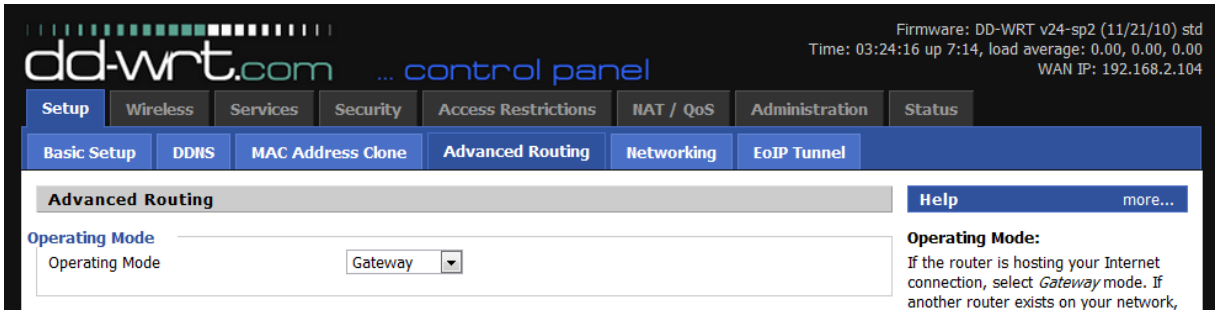

Figura 20 - Opções de roteamento avançado

Fonte: autoria própria

Operating Mode

Operating Mode: Gateway

Configura o roteador para agir como um gateway para uma rede externa (Internet).

As opções mais importantes para o funcionamento da rede estão na sessão a seguir, configuração dos recursos *wireless* do roteador.

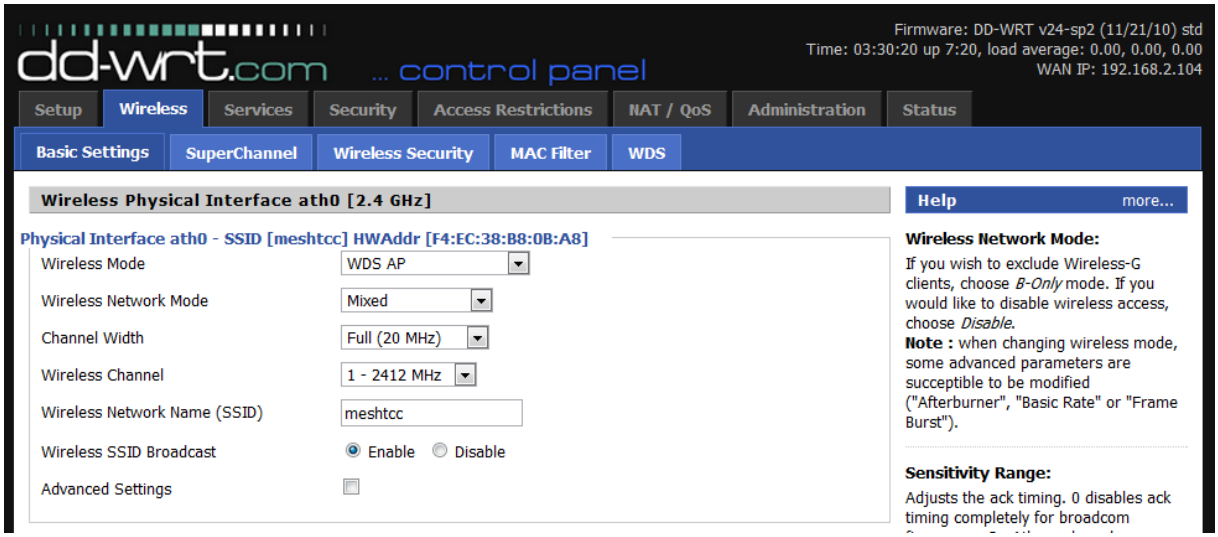

Figura 21 - Configurações básicas do wireless

Fonte: Autoria própria

WIRELESS – BASIC SETTINGS

Wireless Mode: WDS AP

Aqui o roteador está sendo configurado para ser um AP utilizando o protocolo WDS.

Wireless Network Mode: Mixed

Configura o roteador para usar qualquer padrão dentre 802.11b, 802.11g ou 802.11n.

Wireless Channel: 1 – 2412 MHz

Todos os roteadores da rede devem escolher o mesmo canal para funcionar, no caso o canal 1.

Wireless Network Name: meshtcc

O nome da rede sendo implantada. Deve ser o mesmo em todos os roteadores.

WIRELESS SECURITY

Aqui é realizada a configuração da autenticação via servidor RADIUS.

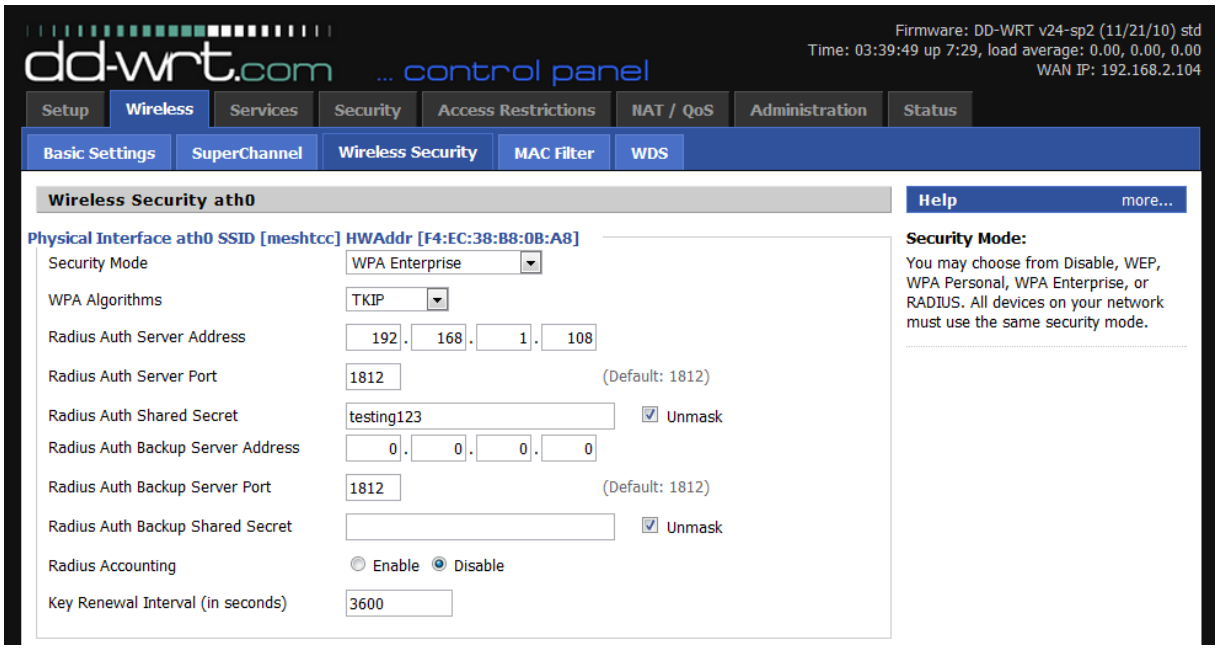

Figura 22 - Configurações de segurança

Fonte: autoria própria

Security Mode: WPA Enterprise

WPA é um padrão de encriptação seguro e recomendado. O enterprise significa que é possível utilizar um servidor RADIUS para realizar a autenticação.

WPA Algorithm: TKIP

Algoritmo de autenticação.

Radius Auth Server Address: 192.168.1.108

Endereço do servidor RADIUS, conforme diagrama da rede.

Radius Auth Server Port: 1812

Porta onde o RADIUS estará funcionando. Este é o valor padrão.

Radius Auth Shared Secret: testing123

Senha compartilhada entre o servidor RADIUS e o seus clientes. Somente clientes com essa senha podem tentar autenticar-se no servidor RADIUS.

WIRELESS – WDS

Aqui, cada roteador recebe a configuração de quem são os seus nós mais próximos na rede. É essa configuração que faz a rede tornar-se uma *mesh* parcial. Cada nó conhece dois outros nós na rede.

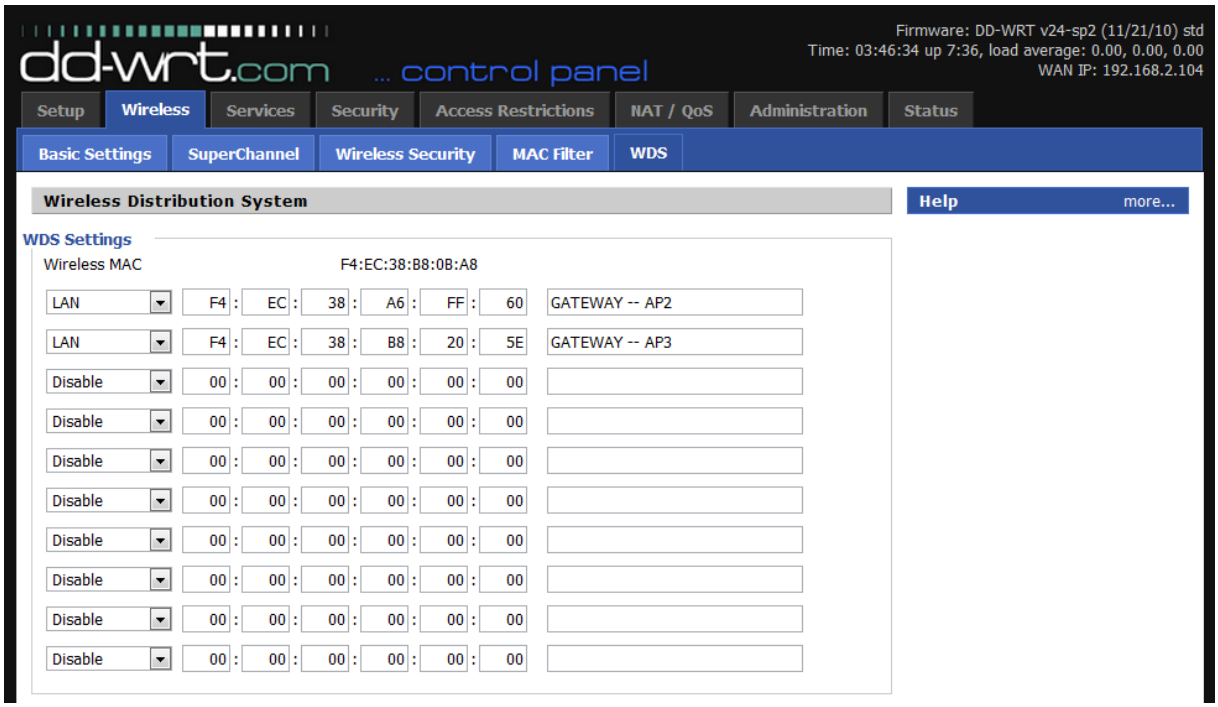

Figura 23 - Configurações do WDS

Fonte: autoria própria

Em cada linha devemos configurar o modo LAN, preencher com o endereço MAC das interfaces wireless dos outros APs, e inserir um rótulo para cada conexão.

Configuração do cliente

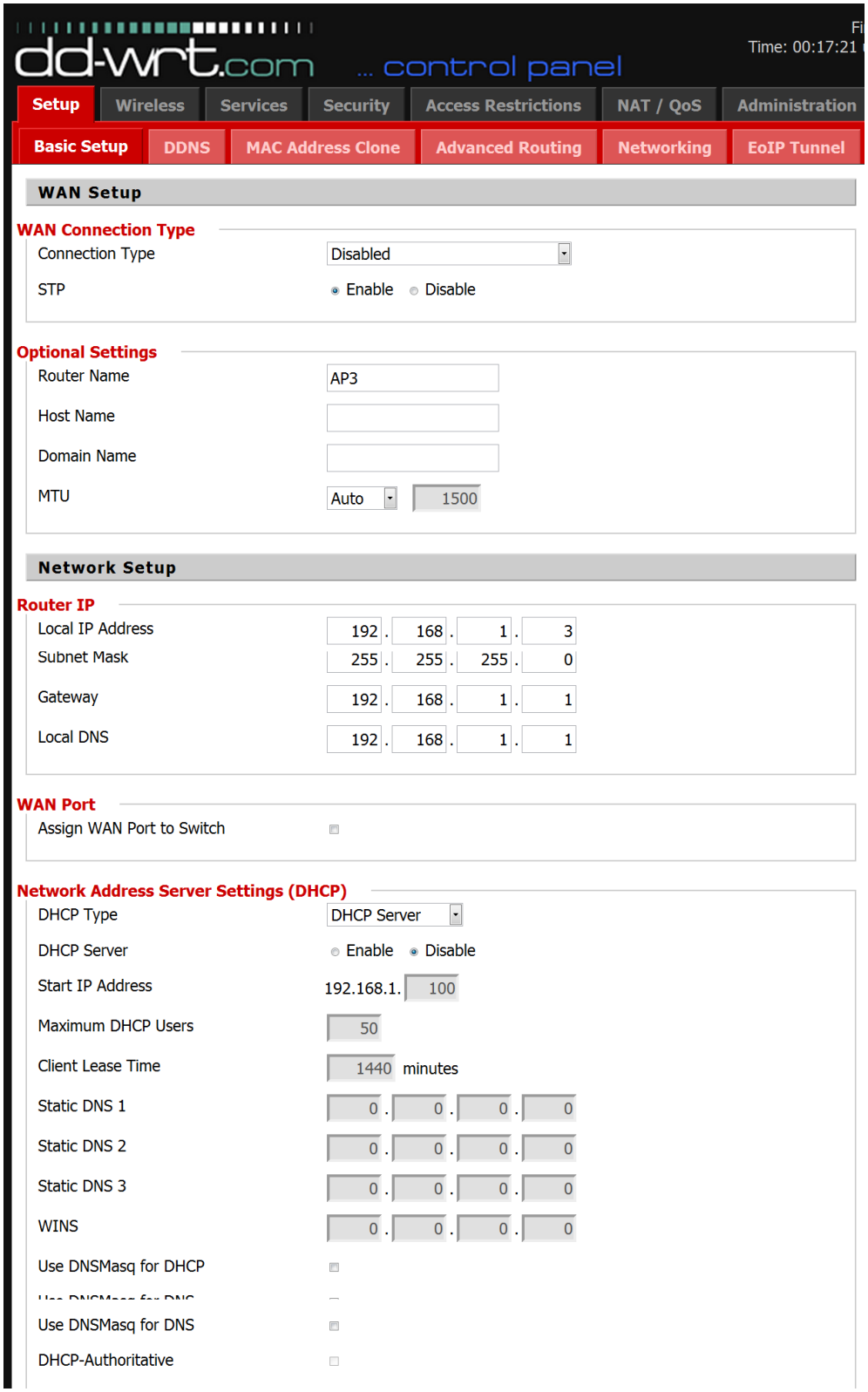

Figura 24 - Configuração básica do cliente

Fonte: autoria própria

SETUP - BASIC SETUP

WAN Connection Type

Connection Type: Disabled.

Os clientes não se conectam diretamente à rede externa, apenas o gateway.

STP: Enable

Esse é o *Spanning Tree Protocol*, que precisa ser habilitado para que os roteadores consigam calcular as rotas em redes *mesh* com mais de dois roteadores.

Router Name: AP3

Opcionalmente, podemos configurar o nome do roteador, o que ajuda na organização da rede, principalmente na medida em que ela for crescendo.

Router IP

Local IP Address: 192.168.1.3

O endereço IP do cliente na rede local, conforme o diagrama da rede. Pode ser qualquer endereço na mesma sub-rede do gateway.

Subnet Mask: 255.255.255.0

Máscara da sub-rede de acordo com o diagrama da rede.

Gateway: 192.168.1.1

Local DNS: 192.168.1.1

Indicam o gateway e o servidor DNS da rede local, no caso o AP1.

Network Address Server Settings (DHCP)

DHCP Type: DHCP Server

DHCP Server: Disable

Desabilita o servidor DHCP, que já está ativo no gateway.

As demais opções nesta página podem ser deixadas com o valor padrão.

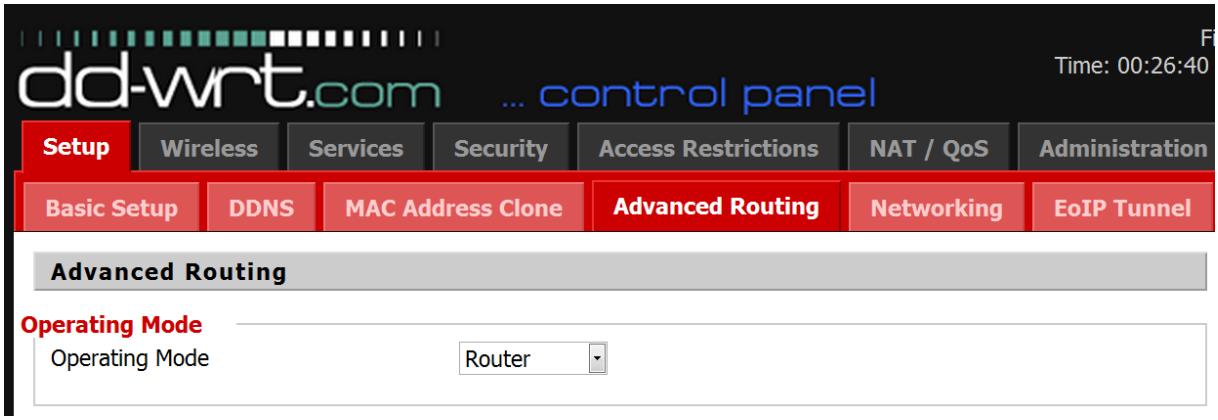

Figura 25 - Opções de roteamento avançado

Fonte: autoria própria

Operating Mode

Operating Mode: Router

Habilita as funções de roteamento.

As opções mais importantes para o funcionamento da rede estão na sessão a seguir, configuração dos recursos *wireless* do roteador.

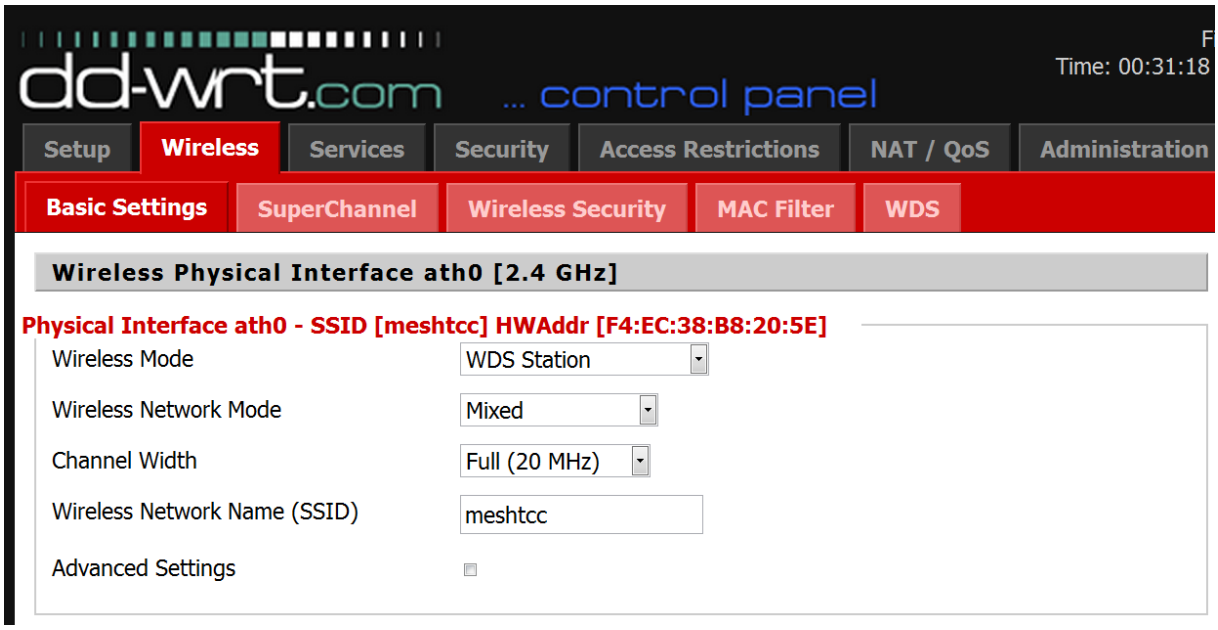

Figura 26 - Configurações básicas do wireless

Fonte: Autoria própria

WIRELESS – BASIC SETTINGS

Wireless Mode: WDS Station

Aqui o roteador está sendo configurado para usar o protocolo WDS como uma estação.

Wireless Network Mode: Mixed

Configura o roteador para usar qualquer padrão dentre 802.11b, 802.11g ou 802.11n.

Wireless Network Name: meshtcc

O nome da rede sendo implantada. Deve ser o mesmo em todos os roteadores.

WIRELESS SECURITY

Aqui é realizada a configuração da autenticação via servidor RADIUS.

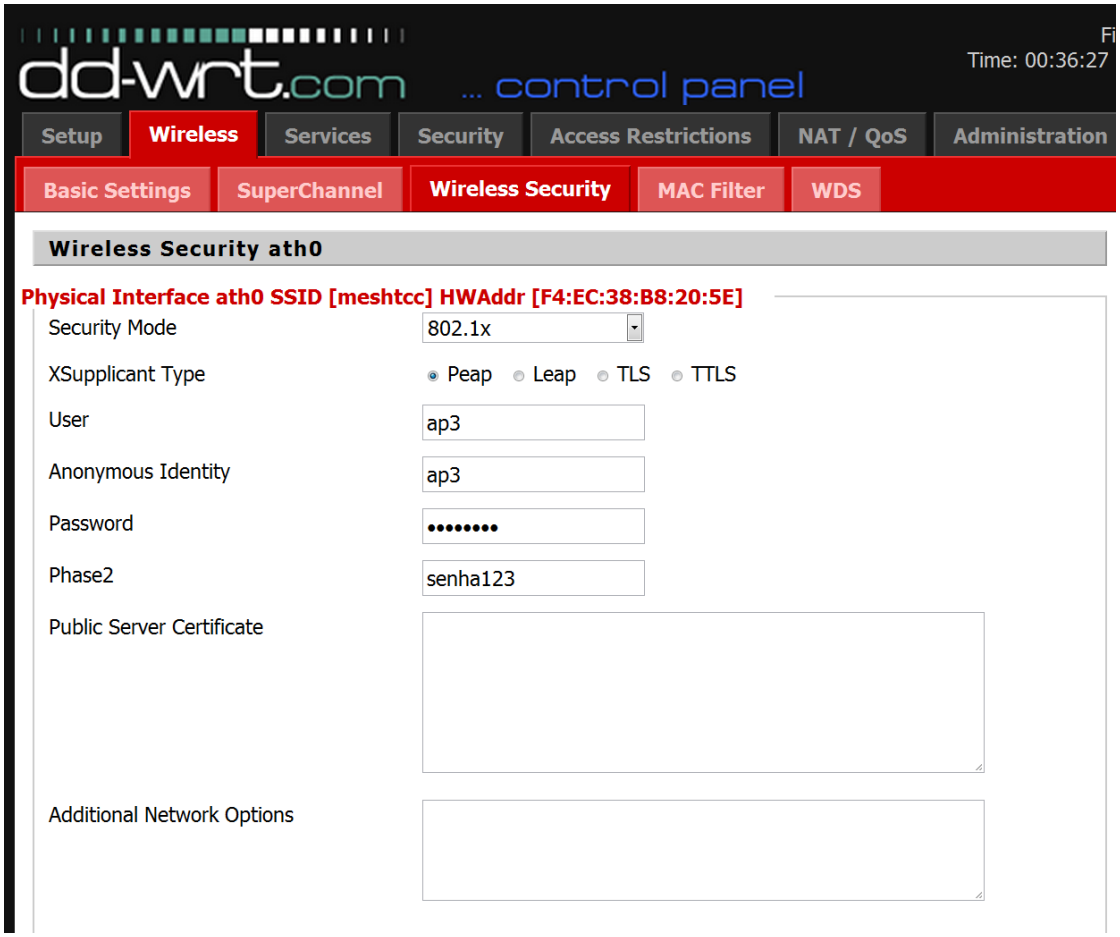

Figura 27 - Configurações de segurança

Fonte: autoria própria

Security Mode: 802.1x

XSupplicant Type: Peap

User: ap3

Anonimous Identity: ap3

Password: senha123

Phase2: senha123

Essas configurações farão o roteador autenticar-se no servidor RADIUS. O nome de usuário é ap3, um usuário previamente cadastrado na lista de usuários do RADIUS. Essa autenticação será realizada utilizando-se o protocolo PEAP (*Protected Extensible Authentication Protocol*). As demais opções podem ser deixadas em branco.

WIRELESS – WDS

Aqui, cada roteador recebe a configuração de quem são os seus nós mais próximos na rede. É essa configuração que faz a rede tornar-se uma *mesh* parcial. Cada nó conhece dois outros nós na rede.

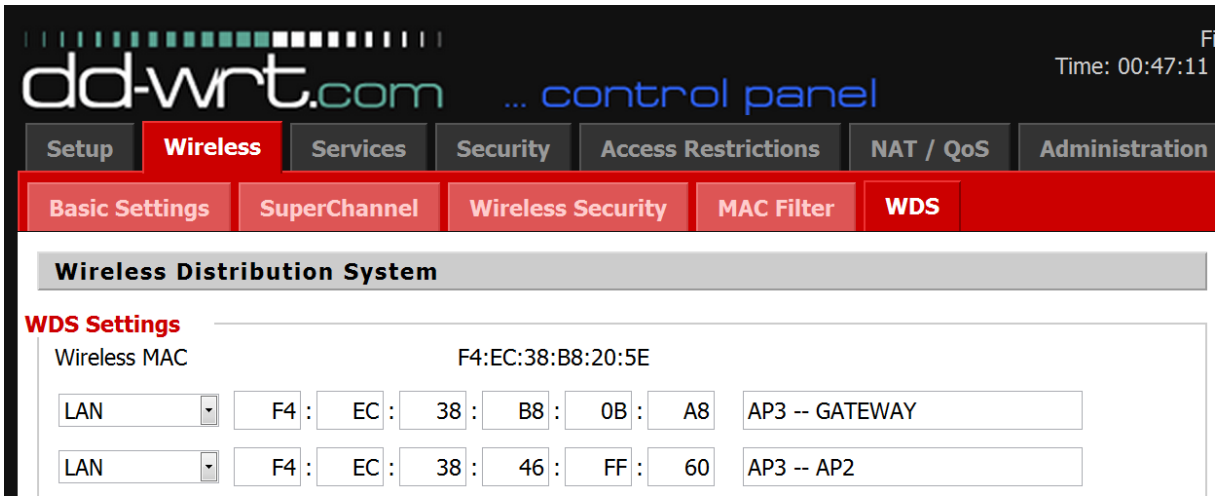

Figura 28 - Configurações do WDS

Fonte: autoria própria

Em cada linha devemos configurar o modo LAN, preencher com o endereço MAC das interfaces wireless dos outros APs, e inserir um rótulo para cada conexão.

Configuração do servidor RADIUS

O FreeRADIUS é uma implementação do protocolo RADIUS para o Linux, gratuito e de código aberto. A instalação é simples e pode ser feita via sistema gerenciador de pacotes do próprio Linux. Para que a autenticação passe a funcionar na rede, alguns arquivos de configuração devem ser editados conforme a seguir:

clients.conf

Nesse arquivo são configurados todos os clientes que terão acesso ao servidor RADIUS. Para a rede aqui descrita, as seguintes linhas devem ser adicionadas ao arquivo:

```
clienttesteRADIUS {
ipaddr = 192.168.1.1
secret = testing123
}
```

O AP1 está sendo autorizado como cliente deste servidor RADIUS. A senha “testing123” está configurada neste arquivo e também no roteador AP1. Requisições feitas pelo gateway serão recebidas e processadas normalmente pelo servidor RADIUS.

users

Neste arquivo são configurados os usuários da rede:

```
testeCleartext-Password := "senha123"
rafaelCleartext-Password := "rafael123"
fabianoCleartext-Password := "fabiano123"
ap2Cleartext-Password := "senha123"
ap3Cleartext-Password := "senha123"
```

Além dos usuários comuns da rede, é preciso cadastrar uma senha para cada AP cliente da rede. É dessa maneira que eles irão se juntar à rede e se conectar ao gateway, formando a rede *mesh*.

Para este teste os usuários e as senhas foram armazenados em um arquivo de texto, mas o FreeRADIUS pode trabalhar com várias outras formas de banco de dados, inclusive LDAP e bancos de dados, o que torna fácil associar a autenticação a um banco de dados de alunos ou funcionários.

Configuração dos *notebooks*

A princípio, a rede estaria pronta para ser utilizada. Como estação cliente, foram utilizados *notebooks* rodando Ubuntu e Windows. Para que a autenticação seja realizada corretamente, algumas configurações são necessárias nos clientes. No Ubuntu, é necessário escolher a opção de segurança WPA & WPA2 Enterprise e o tipo de autenticação deve ser *Protected EAP* (PEAP). Isso fará com que o servidor RADIUS reconheça as requisições do cliente. As demais opções podem ficar com o valor padrão, e usuário e senha devem ser preenchidos como normal:

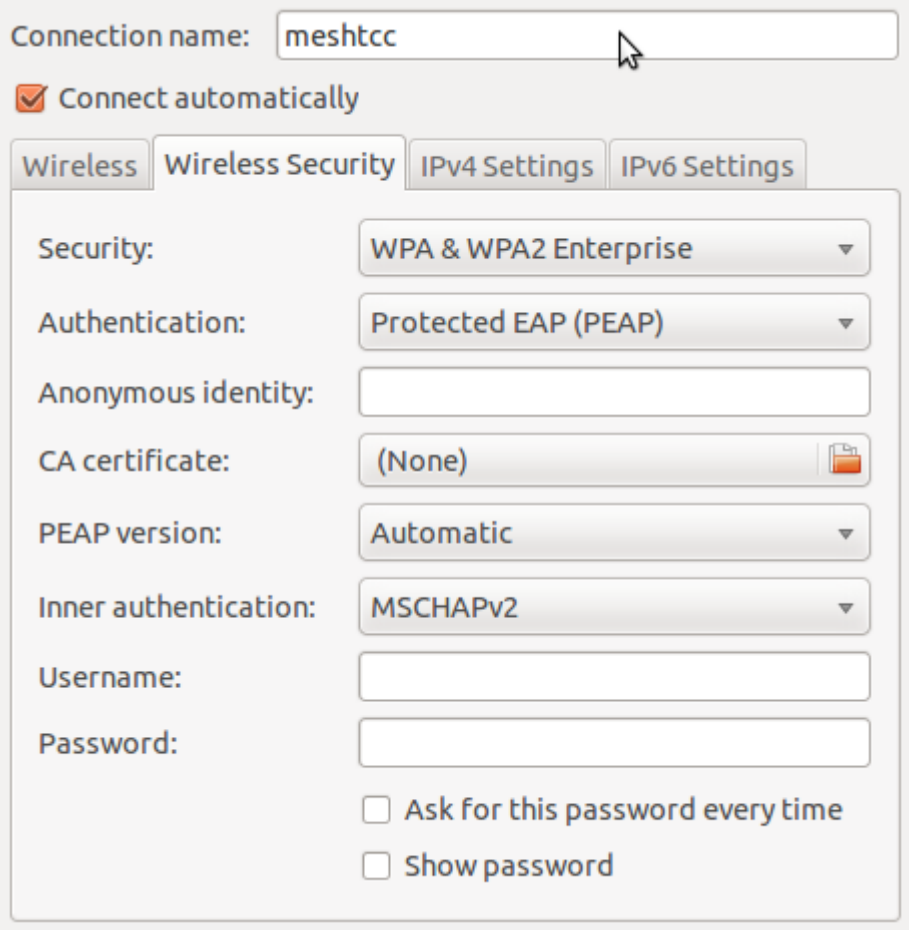

Figura 29 - Configurações WiFi no Ubuntu

Fonte: Autoria própria

No Windows a configuração é semelhante. Nas propriedades da conexão deve-se escolher WPA-Enterprise e autenticação PEAP:

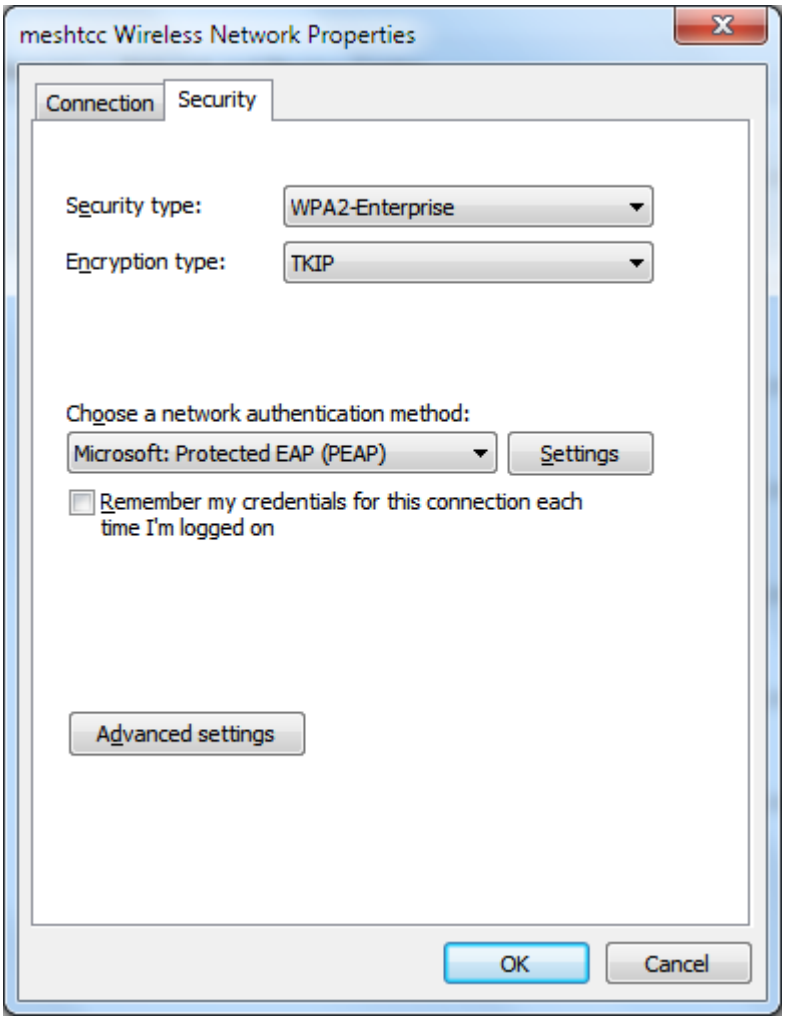

Figura 30 - Configuração WiFi no Windows

Fonte: autoria própria

PRIMEIRO TESTE

O objetivo do primeiro teste foi verificar se a Internet estava disponível nos dois roteadores clientes. Este teste poderia ser realizado com cabos, apenas para verificar a conectividade. O teste do RADIUS seria realizado posteriormente.

Conectou-se um cabo de rede ao *notebook* de teste e ao AP2, e foi possível navegar na Internet sem problemas. O link entre esses dois roteadores estava funcionando. Repetindo-se o teste com o AP3, o resultado também foi positivo. Os roteadores estavam, portanto, ligados. Porém, ao tentar usar o comando ping para alcançar outros roteadores na rede, não foi possível encontrá-los. Eles estavam ligados, mas não estavam ligados em malha.

O passo seguinte foi retirar as configurações de segurança dos APs e deixar a rede aberta. Realizando o teste de conectividade com uso de cabos, novamente obteve-se resultado positivo. Ao usar o comando ping para alcançar os outros roteadores na rede, houve retorno imediato dos pacotes. A rede estava, portanto, funcionando como uma malha.

Concluiu-se desse teste que não seria possível proteger a rede usando criptografia nos roteadores, pois isso comprometeria o funcionamento do WDS, e a rede não funcionaria como o proposto.

Assim sendo, buscou-se uma alternativa de autenticação que pudesse ser realizada depois de estar conectado na rede. Esse é o funcionamento básico de grande parte dos pontos de acesso existentes em lugares públicos, tais como cafés, bibliotecas e hotéis, e principalmente de pontos de acesso que exigem pagamento ou um plano de acesso. A rede não possui criptografia, qualquer um pode conectar-se a ela, mas para ter acesso à Internet, é preciso autenticar-se via nome de usuário e senha, um código numérico fornecido pelo estabelecimento que oferece o serviço, ou as credenciais do plano de acesso.

A solução para esse caso seria, portanto, um formulário de *login* onde seria possível fazer a autenticação usando nome de usuário e senha, e obter autorização para o acesso. Obviamente, se algum usuário mal-intencionado se conectasse à rede e não tivesse um nome de usuário e senha válidos, ele seria apenas redirecionado novamente para a página de *login*, a despeito do endereço que ele digitasse em seu navegador.

O DD-WRT tem um módulo de suporte a esse tipo de autenticação, chamado Chillispot. Duas configurações adicionais são necessárias para que tudo funcione:

- Um servidor web funcionando e com a página de *login* disponível, para ser utilizada pelo Chillispot mandar requisições para o servidor RADIUS.
- Configuração do Chillispot no DD-WRT

Configuração do Apache:

A configuração do Apache pode ser realizada com alguns comandos simples:

```
sudoapt-getinstall apache2
```

Instala o Apache versão 2 no Ubuntu.

```
sudo a2enmod ssl
```

Habilita o SSL (*Secure Sockets Layer*) no Apache, o que permitirá conexões criptografadas.

```
sudo a2ensite default-ssl
```

Configura o Apache com chave e certificado de segurança padrões.

Após a configuração inicial, deve-se copiar o arquivo `hotspotlogin.cgi` para a pasta de scripts CGI do Apache. Esse script é o responsável pelo *login* e autenticação no RADIUS. É escrito em Perl e pode ser customizado de acordo com a necessidade.

Por fim, deve-se editar uma linha deste script:

```
$uamsecret = "testing123";
```

Essa é a outra chave, que é compartilhada entre o script de autenticação e o Chillispot.

Configuração do Chillispot:

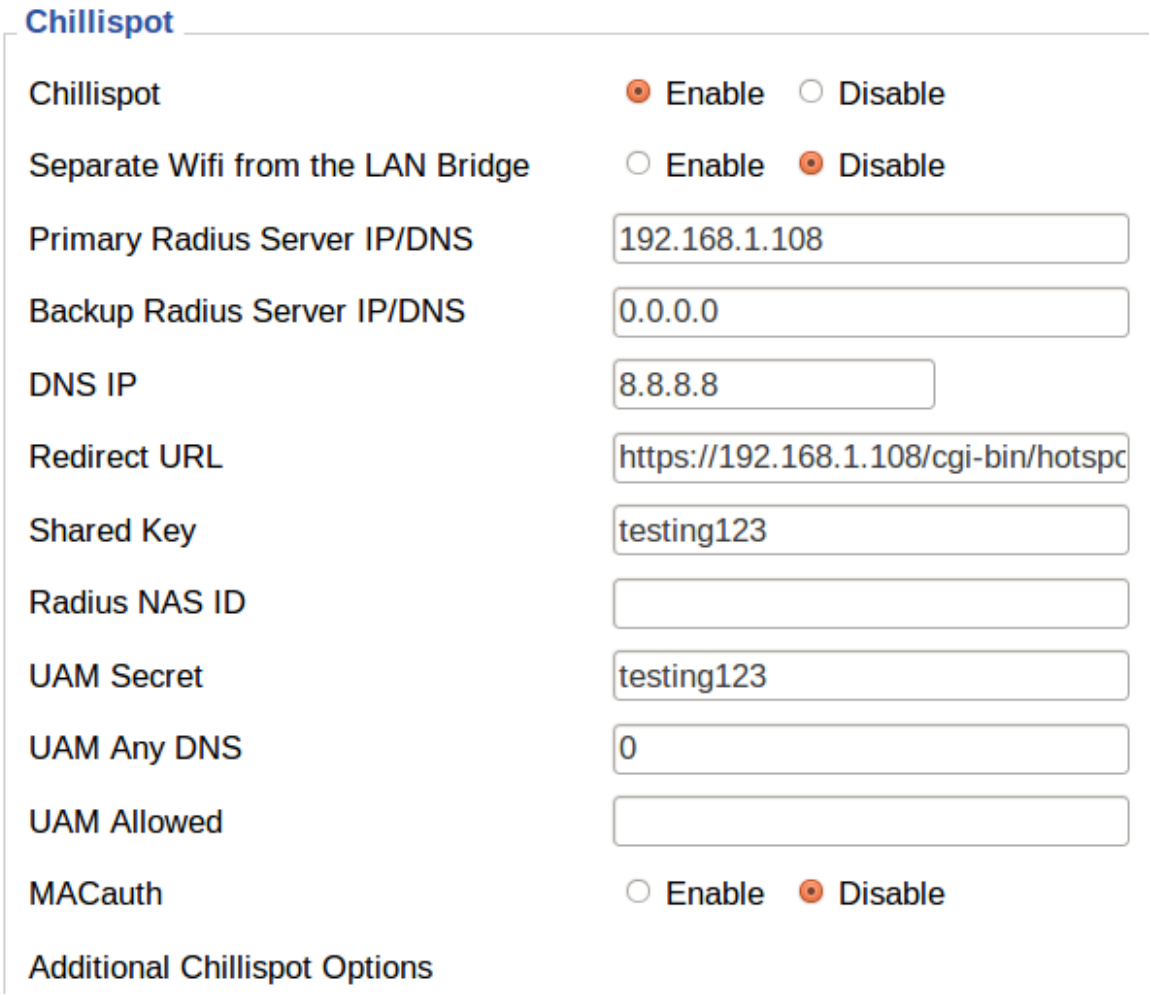

Figura 31 - Configurações do Chillispot

Fonte: autoria própria

Chilispot: enable

Habilita o Chillispot.

Primary Radius Server IP/DNS: 192.168.1.108

Informa o Chillispot de onde está o servidor RADIUS.

DNS-IP: 8.8.8.8

Neste caso, utilizado o DNS público do Google.

Redirect URL: https://192.168.1.108/cgi-bin/hotspotlogin.cgi

Esta é a URL do script de autenticação do *hotspot*, que foi configurado no passo anterior. O HTTPS garante que a autenticação será criptografada.

Shared Key: testing123

Essa é a chave compartilhada do servidor RADIUS.

UAM Secret:testing123

Chave compartilhada entre o script de autenticação e o Chillispot. Deve ser a mesma configurada no script.

SEGUNDO TESTE

Após realizar todas as configurações, realizou-se o segundo teste. A rede meshtcc estava aparecendo aberta, sem segurança. Foi possível conectar sem problemas. Ao digitar o endereço de uma página qualquer no browser, a tela de *login* apareceu:

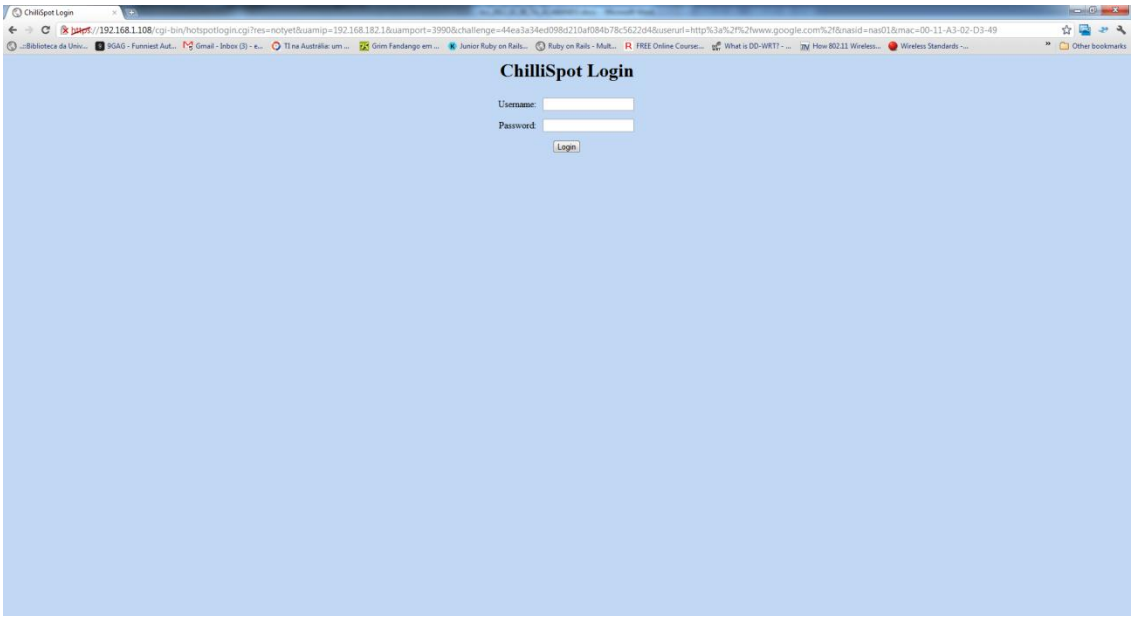

Figura 32 - Formulário de *login* do Chillispot

Fonte: autoria própria

Após digitar o nome de usuário e senha pré-configurados no servidor RADIUS, surgem duas janelas no navegador: uma janela indicando o *login* bem sucedido, e a própria página do browser carregada:

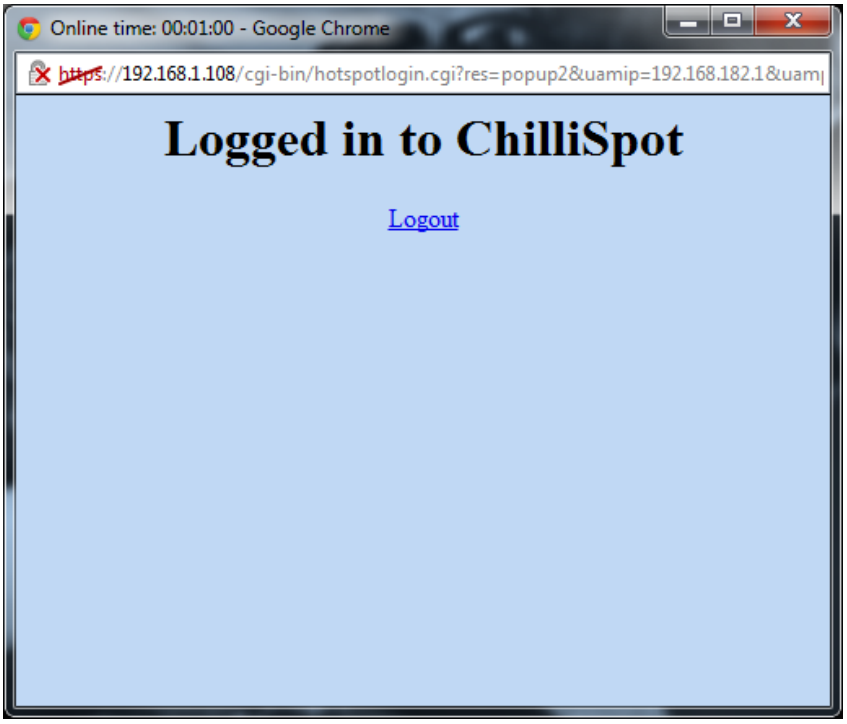

Figura 33 - Confirmação do *login*

Fonte: autoria própria

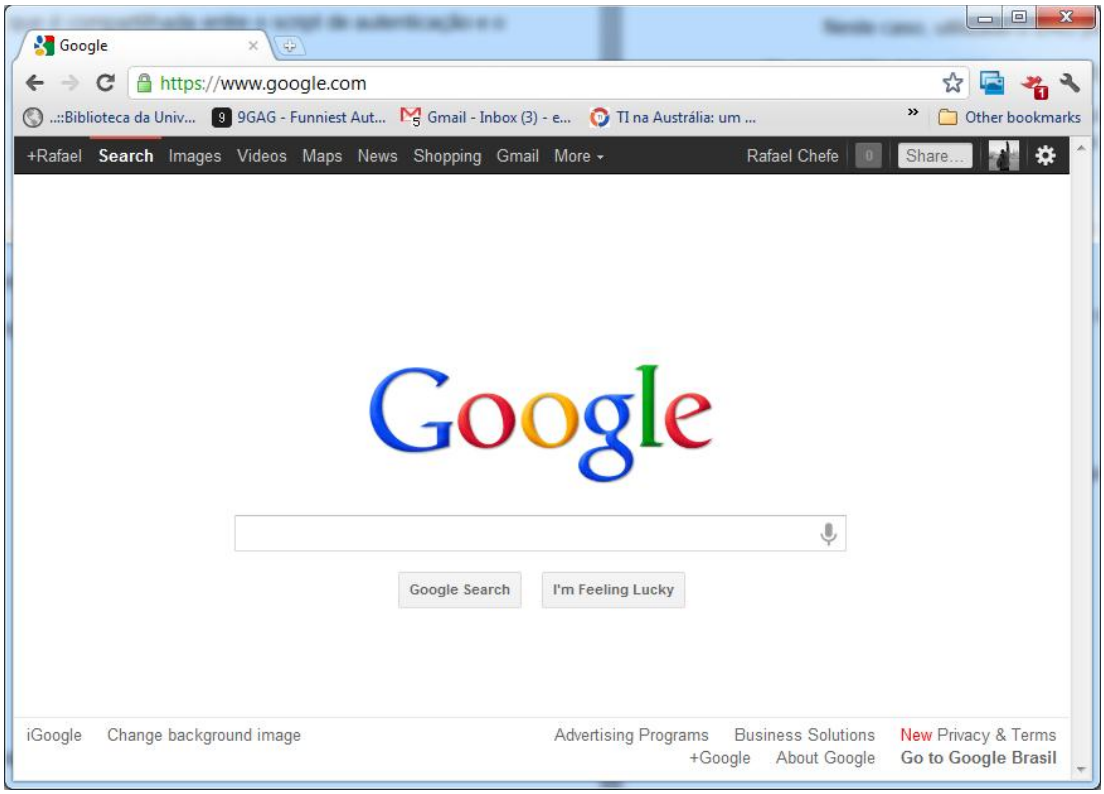

Figura 34 - Página carregada através do chilispot

Fonte: Autoria própria

No log do servidor RADIUS é possível ver a requisição chegando, sendo processada e o aceite sendo enviado novamente para o cliente:

```
rad_recv: Access-Request packet from host 192.168.1.1 port 48005, id=0,
length=196
      User-Name = "chefe"
      User-Password = "senha123"
[files] users: Matched entry chefe at line 1
++[files] returns ok
[pap] login attempt with password "senha123"
[pap] Using clear text password "senha123"
[pap] User authenticated successfully
++[pap] returns ok
Sending Access-Accept of id 0 to 192.168.1.1 port 48005
```

E mais a requisição referente ao *accounting*, que futuramente pode ser um serviço a mais na rede:

```
rad_recv: Accounting-Request packet from host 192.168.1.1 port 44348, id=1,
length=130
Sending Accounting-Response of id 1 to 192.168.1.1 port 44348
```

TESTES DE SINAL

Com os três roteadores ligados em rede e a autenticação funcionando, realizou-se um teste para testar o sinal da rede *mesh* como um todo.

O procedimento foi simples: deixar o AP1 ligado e afastar o *notebook* até o sinal sumir. Repetir o mesmo procedimento para o AP3.

Os resultados foram positivos: ao ligar um AP secundário, o sinal voltava a aparecer, e era possível conectar à Internet. Ao usar o comando ping para tentar alcançar os outros roteadores, sempre houve resposta, concluindo-se, portanto, que a rede estava em perfeito funcionamento.

4 CONSIDERAÇÕES FINAIS

Através desta pesquisa foi possível verificar que com um pouco de planejamento é possível idealizar e implantar uma rede sem fio em malha altamente confiável e segura a um custo baixíssimo, ou mesmo nulo, caso o objetivo da rede seja apenas organizar vários roteadores e várias redes já existentes em uma rede mais eficiente e robusta.

São evidentes os benefícios que o projeto de uma rede implementada desta forma pode trazer: organizações podem cortar custos utilizando melhor os seus equipamentos. Instituições de ensino podem prover acesso à Internet mais controlado e de melhor qualidade aos seus alunos. Comunidades carentes onde não haja Internet cabeada, ou cujos moradores não possuam poder aquisitivo suficiente para ter a sua própria conexão, podem se valer de redes municipais projetadas desta maneira.

Este projeto visa não apenas eficiência e conectividade, mas principalmente ser de grande utilidade e grande valia para a sociedade em que vivemos.

4.1 Trabalhos Futuros

Este projeto de rede apresenta muitas possibilidades de expansão e adição de funcionalidades. Adicionar mais roteadores na rede seria trivial, somente sendo necessário repetir a configuração já existente. Novos usuários seriam cadastrados na rede apenas uma vez, de forma prática, e teriam seus acessos garantidos enquanto fosse necessário. O projeto poderia ser expandido para aceitar usuários cadastrados em um banco de dados relacional, como o cadastro de funcionários de uma empresa, alunos de uma universidade ou condôminos em um complexo de apartamentos. Usando-se mais funcionalidades de *accounting* do RADIUS seria possível controlar o que os usuários estão acessando, o volume de dados transferido, entre outras coisas. Fica muito mais fácil controlar os acessos à rede usando tais funcionalidades, e como consequência, mais fácil de otimizara rede de acordo com o seu uso.

REFERÊNCIAS

ALECRIM, Emerson. **O que é Wi-Fi (IEEE 802.11)?**. Disponível em <http://www.infowester.com/wifi.php>. Acesso em: 22 jan. 2011.

BARBOSA, Anderson. **Padrão IEEE 802.** 2010. Disponível em: http://desmontacia.wordpress.com/2010/09/29/padro-ieee-802 > Acessado 22/06/2011.

CANTÚ, Evandro. **Redes de Computadores e Internet**. São José, SC:[s.n.], 2003.

DANIELYAN, Edgar. **IEEE 802.11**. Disponível em <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_5-1/ieee.html>. Acesso em: 21 jan. 2011.

FOROUZAN A. Behrouz. **Comunicação de Dados e Redes de Computadores**. 3ª ed. Porto Alegre, Bookman, 2004.

GAST, Matthew. 802.11 wireless networks: the definitive guide. 2nd ed. Beijing; Farnham: O'Reilly, c2005. xxi, 630 p ISBN 0596100523.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 3. ed. São Paulo, SP: Pearson Addison-Wesley, 2006. xx, 634 p. ISBN 85-88639-18-1.

PASSOS, Diego. Métricas de Roteamento para Redes em Malha Sem Fio. Universidade Federal Fluminense. Departamento da Ciência da Computação, Niterói, 2003.

PEIXOTO Martins Aureliano. **Detalhes e Webinar sobre a vulnerabilidade Hole 196 do WPA2**, 2010.
Disponível em http://aurelianomartins.wordpress.com/2010/08/03/detalhes-e-webinar-sobre-a-vulnerabilidade-hole196-do-wpa2/>
Acessado em 22 out 2010

POSEY, Brien. SolutionBase: **RADIUS deployment scenarios**, 2006 Disponível em <http://i.techrepublic.com.com/downloads/PDF/SolutionBase_RADIUS_deployment_scenarios.pdf>. Acesso em: 22 jan. 2011.

RIGNEY, C. et al. RFC 2865 - **Remote Authentication Dial In User Service (RADIUS)**, 2000.

RUFINO, Nelson M. de Oliveira. **Segurança em Redes sem fio**. São Paulo, Novatec, 2005.

SCHILLER, Felipe O. S. **Redes em Malha**. Disponível em <http://www.gta.ufrj.br/grad/06_2/felipe/>. Acesso em: 23 jan. 2011.

STALLINGS, William. **Redes e sistemas de comunicação de dados**: teoria e aplicações corporativas. Rio de Janeiro, RJ: Elsevier, 2005. xvi, 449 p. ISBN 8535217312.

TANENBAUM, Andrew S.. **Redes de computadores.** Rio de Janeiro: Elsevier, 2003 945 p. ISBN 9788535211856

VOLLBRECHT, John. **The Beginnings and History of RADIUS**, 2006.Disponível em <http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf> Acessado em 22 jan. 2012

About DD-WRT. Disponível em <http://www.dd-wrt.com/site/content/about/>. Acesso em: 24 jan. 2011.

Como o protocolo TCP/IP funciona. Disponível em <http://www.clubedohardware.com.br/artigos/1351/>. Acesso em: 17 jan. 2011

Everything You Need To Know About Wireless Bridging and Repeating - Part 1: WDS. Disponível em <http://www.smallnetbuilder.com/wireless/wireless-

howto/31191-everything-you-need-to-know-about-wireless-bridging-and-repeating-part-1-wds>. Acesso em: 28 jan. 2011.

Modelos de redes de computadores de grande porte. Disponível em <http://www.netdownloads.com.br/tutoriais/redes/aq174-modelos-de-redes-de-computadores-de-grande-porte.html?pagina=2/>. Acesso em: 19 jan. 2011

O Modelo de Referência OSI para Protocolos de Rede. Disponível em <http://www.clubedohardware.com.br/artigos/O-Modelo-de-Referencia-OSI-para-Protocolos-de-Rede/1349/>. Acesso em: 12 jan. 2011

REDE/NETWORK: Explicação Resumida Camada OSI. Disponível em <http://tucones.blogspot.com/2010/11/redenetwork-explicacao-resumida-camada.html>. Acesso em: 11 jan. 2011

Redes ponto a ponto e cliente servidor. Disponível em <http://redesiosi15.blogspot.com/2009/06/sistema-operacional-do-servidor-redes.html>. Acesso em: 21 jan. 2011

Topologia de rede. Disponível em <http://analiseds.blogspot.com/2010/06/topologia-de-rede.html>. Acesso em: 19 jan. 2011

Topologia física em barramento. Disponível em <http://pefonline.pefproductions.com/comunicacao_de_dados/modulo2/topologia_fisica_em_barramento.html/>. Acesso em: 17 jan. 2011

Viva sem fio. Disponível em <http://www.vivasemfio.com/blog/modo-ad-hoc/>. Acesso em: 20 fev. 2011