Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e
Pesquisas Computacionais

Josias de Souza Borges

AUTENTICAÇÃO SEGURA DE USUÁRIOS DE DOMÍNIOS DIFERENTES ATRAVÉS DE REDES WIRELESS

Rio de Janeiro

2014

Josias de Souza Borges

AUTENTICAÇÃO SEGURA DE USUÁRIOS DE DOMÍNIOS DIFERENTES ATRAVÉS DE REDES WIRELESS

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Claudio Miceli de Farias, M.Sc., UFRJ, Brasil

Rio de Janeiro

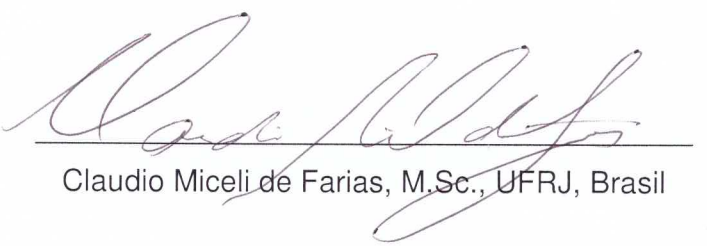
2014

Josias de Souza Borges

AUTENTICAÇÃO SEGURA DE USUÁRIOS DE DOMÍNIOS DIFERENTES ATRAVÉS DE REDES WIRELESS

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2014.



Claudio Miceli de Farias, M.Sc., UFRJ, Brasil

AGRADECIMENTOS

Agradeço a Deus que me deu a vida, a minha esposa Ana Paula e aos meus filhos pela compreensão quanto a minha ausência, aos professores do curso pelo conhecimento transmitido com eficiência, aos meus amigos de classe pelo companheirismo em todos esses dias e ao meu orientador pela paciência e dedicação.

RESUMO

BORGES, Josias de Souza. **AUTENTICAÇÃO SEGURA DE USUÁRIOS DE DOMÍNIOS DIFERENTES ATRAVÉS DE REDES WIRELESS**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

Uma das dificuldades em ambientes de redes wireless é garantir sua segurança, principalmente em ambientes com redes compartilhadas onde é permitido que usuários compartilhem infraestruturas heterogêneas e de diferentes administrações.

Este estudo tem como foco a melhoria da segurança nesse tipo de ambiente através da análise de ferramentas que permitam a integração, a segurança e o monitoramento neste tipo de ambiente.

ABSTRACT

BORGES, Josias de Souza. **AUTENTICAÇÃO SEGURA DE USUÁRIOS DE DOMÍNIOS DIFERENTES ATRAVÉS DE REDES WIRELESS**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

One of the challenges in wireless network environments is to ensure their safety, especially in environments with shared networks where users are allowed to share heterogeneous infrastructures and different administrations.

This study focuses on the improvement of safety in this type of environment through the analysis tools that enable the integration, security and monitoring in this type of environment.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Algumas das grandes universidades brasileiras, construídas em um período onde a realidade tecnológica era bem diferente da atual, não foram projetadas pensando em conectividade, são carentes em suas infraestruturas no que se refere a essa tecnologia. A expansão das redes de computadores nos campus nem sempre seguem planejamentos que considerem o rápido crescimento na demanda por internet em nossas universidades.

Devido ao baixo preço e a diversidade de equipamentos com internet móvel, cada vez mais os usuários das redes de computadores nas universidades, principalmente os alunos, utilizam simultaneamente vários dispositivos com acesso a rede, é possível que apenas um usuário use três ou mais conexões ao mesmo tempo, basta ele utilizar um notebook, um smartphone e um tablete, algo muito comum hoje em dia, por isso precisa-se melhorar essas infraestruturas a fim de atender esta nova e crescente demanda para conexões de redes sem fio.

1.1. MOTIVAÇÃO E JUSTIFICATIVA

Através de um cenário real, uma Universidade Pública (neste caso a UFRJ), observa-se a necessidade de ampliar a cobertura do sinal da rede *wireless* para garantir aos alunos e funcionários o acesso à internet e também aos serviços de intranet da instituição nas áreas externas das unidades.

Uma solução ideal seria a implantação de redes padrão *Mesh* (redes em malha) [Schiller, 2006], porém, em muitas universidades, a falta de centralização de

gerência de redes dificulta a sua implementação, provocando o desinteresse por uma solução eficaz e definitiva.

A solução que apresenta o melhor custo/benefício é aumentar a área de cobertura do sinal dos rádios existentes nos locais envolvidos, utilizando recursos que permitam o compartilhamento destes.

Como essa solução envolve redes com tecnologias e equipamentos heterogêneos, com administrações independentes e sem qualquer integração, faz-se necessário um cuidado extra com relação ao acesso a rede sem fio e assim também com a segurança das informações.

Métodos de instalação, configuração e administração de redes não padronizadas são utilizados, o que pode permitir acesso não autorizado à rede, oscilações do nível do sinal wifi e baixo desempenho por mau uso da banda, comprometendo a qualidade e a disponibilidade do serviço, gerando muitas vezes insatisfação de usuários e desestímulo de administradores de redes envolvidas.

1.2. OBJETIVOS

Ao final da leitura deste trabalho o leitor conhecerá possíveis soluções e seus decorrentes problemas para fornecer autenticação segura aos seus usuários através de outras redes conhecidas e compartilhadas e também para permitir que usuários de outras redes se autentiquem pela sua rede wireless com segurança.

1.3. METODOLOGIA

Será utilizado o método de pesquisa investigativo [Lakatos], onde será indicada uma proposta de infraestrutura de redes sem fio para uma universidade,

contemplando o uso adequado de padrões, topologia, cenário e mecanismo de segurança e autenticação que melhor se adapte na solução de um problema similar ao citado neste trabalho.

1.4. ORGANIZAÇÃO DO TRABALHO

O Capítulo 1 apresenta a motivação para o seu desenvolvimento, seus objetivos, a metodologia utilizada e sua organização.

O Capítulo 2 apresenta, para fins de nivelamento do conhecimento, o conceito de redes sem fio, seus diferentes padrões, topologias e equipamentos.

O Capítulo 3 apresenta os problemas com ataques conhecidos contra redes sem fio e os protocolos que propõem técnicas de segurança.

O Capítulo 4 apresenta uma proposta de infraestrutura de redes sem fio para universidades capaz de suprir as expectativas deste trabalho.

O Capítulo 5 apresenta as conclusões do trabalho.

2. CONCEITOS DE REDES SEM FIO

Cada instalação de redes de computador nos departamentos participantes tem sua própria infraestrutura de redes sem fio, o que exige decisões importantes, como a escolha do padrão de comunicação, a topologia de rede, tipos de antenas, pontos de acesso (AP's), serviços envolvidos e mecanismos de segurança.

Serão analisados agora os padrões de comunicação utilizados na implementação de uma rede wireless, buscando identificar o que melhor se adequa em um ambiente universitário.

Esta analise também envolverá componentes envolvidos no acesso a redes sem fio, como AP's e antenas e suas características, como o sinal e seu alcance.

2.1. PADRÕES

Desenvolvidos pelo Institute of Electrical and Electronics Engineers (IEEE), uma organização composta por cientistas e engenheiros com o objetivo de homologar padrões de comunicação para diferentes tipos de redes [IEEE, 2007] os padrões podem ser divididos em Redes de Área Pessoal (WPAN's), Redes de Área Local (WLAN's) e Redes de Área Metropolitana (WMAN's), atendendo assim diferentes características e situações de aplicabilidade [Santos, 2003]. A seguir uma curta analise dos padrões IEEE 802.11, 802.15 e 802.16, considerados os padrões mais importantes para comunicação em redes SF.

2.1.1. Padrão IEEE 802.11

Aplicado principalmente em WLAN's, oferece mobilidade interna em ambientes corporativos, pontes entre redes sem fio, redes de acesso público, redes sem fio residências, etc.

A família IEEE 802.11 pode ser classificada ou dividida, em vários modelos, com características específicas, de acordo com a necessidade existente em cada ambiente [IEEE, 2007], conforme as tabelas abaixo.

Tabela 1 - As variações do padrão 802.11 [Adaptação de Stallings, 2002].

Padrão	Frequência	Velocidade	Funcionalidade
IEEE 802.11a	5Ghz	6 a 54Mbs	Transferência de dados
IEEE 802.11b	2.4GHz	Até 11Mbs	Transferência de dados
IEEE 802.11c/IEEE 802.11d	2.4 e 5Ghz	------	Uso de desenvolvedoras
IEEE 802.11e	------	------	Qualidade de serviço
IEEE 802.11f	------	------	Protocol (IAPP)
IEEE 802.11g	2.4GHz	Até 54Mbs	Transferência de dados(OFDM)
IEEE 802.11h	------	------	Adaptação do IEEE 802.11a
IEEE 802.11i	------	------	Melhora requisitos de segurança
IEEE 802.11s			Comunicação entre AP's(Mesh)
IEEE 802.11n	2.4GHz	100 a 600Mbps	MIMO

Os padrões 802.11c/d/e/f/h/i/s, apesar de sua importância na família IEEE, são complementares ou atualizações para os demais padrões de comunicação 802.11a/b/g/n.

Tabela 2 - Quadro Comparativo: padrões 802.11a/b/g/n.

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Homologado	Setembro de 1999	Setembro de 1999	Junho de 2003	Esperado fim de 2008
Aplicação	Wlan	Wlan e Wpan	Wlan	Wlan
Taxa Máx. Transmissão	54 Mbps	11 Mbps	54 Mbps/108Mbs (SG)	108 Mbps Esperada
Alcance Máx.	100 m	150 m	150 m	250 m
Usuários Conectados	64	36	-	-
Canais não Sobrepostos	12	11 – 13	13	11 – 13
Frequência	5 Ghz	2,4 Ghz	2,4 Ghz	2,4 e 5 Ghz
Modulação	OFDM	DSSS	OFDM ou DSSS	MIMO-OFDM
Compatibilidade	Somente 802.11ª	Somente 802.11g	Somente 802.11b	802.11a/b/g

Na tabela acima vale destacar a taxa de transferência de 54Mbs, dos padrões 802.11a e 802.11g.

No padrão 802.11g se destaca o fato de ser homologado em 2003 e ser o mais conhecido, além de herdar características do padrão 802.11a, como a modulação OFDM e velocidade de 54 Mbps ou 108 Mbps em dispositivos proprietários. Outro atrativo do padrão 802.11g é a utilização da frequência livre 2,4GHz.

O padrão 802.11n [Conceição, 2006] é uma alternativa mais eficiente comparado aos demais modelos, destacando a modulação MIMO-OFDM com múltiplos canais de envio e recebimento de dados.

2.1.2. Padrão IEEE 802.15

O padrão IEEE 802.15 começou a ser desenvolvido em 1994, pela empresa Ericsson, mas somente a partir de 1998 iniciou-se o seu desenvolvimento efetivo, pelo Bluetooth Special Interest Group (SIG), com o objetivo de atender principalmente as características de ambientes WPan, redes pessoais, não sendo compatível com os modelos da família 802.11 [Bonatto, 2007].

Tem como principal característica o fato de não necessitar de AP's para encaminhar os dados do transmissor até o receptor, ou seja, os nós da rede são independentes, apresentando uma nova forma de conexão entre nós, centradas no usuário [Carvalho, 2004]. Assim como o padrão IEEE 802.11, a família IEEE 802.15 é dividida em grupos: 802.15.1(Bluetooth), 802.15.2, 802.15.3(UWB-Ultra Wideband) e 802.15.4(Zigbee), classificados de acordo com a aplicabilidade, potência e alcance do sinal dos seus equipamentos.

Por suas características e aplicações, a família 802.15 tem sua utilização em áreas de pequeno perímetro como salas de aula, auditórios, ambulatórios, residências etc, lugares com baixo fluxo de informações e pequenas distâncias entre os dispositivos de rede, tornando o padrão 802,15 pouco atrativo para a implementação de redes de comunicação sem fio em ambientes que fogem a estas características.

2.1.3. Padrão IEEE 802.16

O padrão IEEE 802.16, desenvolvido em 1999, e regulamentado pelo grupo Broadband Wireless Access (BWA), especifica formalmente redes sem-fio de banda larga, que cobrem áreas metropolitanas (WMAN's), com altas taxas de transferência capaz de atender centenas de usuários com diferentes demandas de tráfego (dados de áudio, vídeo etc.) ou ainda, interligar redes geograficamente separadas. O projeto foi concluído em 2001, com o lançamento da versão final do documento IEEE 802.16 [Lima, 2006]. No entanto teve diversas emendas, 16a(Wi-MAx), 16b(Qos), 16c, 16REVd(Wi-Max fixo) e 16e(Wi-Max móvel).

O fato de fornecer conectividade a usuários a grandes distâncias torna o padrão de pouca utilidade em ambientes universitários, onde se necessita de redes onde os usuários se encontram próximos aos AP’s, outro fator relevante é o alto custo dos dispositivos necessários neste padrão, aumentando significativamente o valor da implementação destas redes e tornando-o pouco atrativo ao cenário proposto pelo trabalho.

2.2. TOPOLIGIAS DE REDES SEM FIO

A topologia é a relação lógica e física dos nós em uma rede, é um mapa de rede que indica os segmentos, pontos de interconexão e as comunidades de usuários [Silva, 2005]. No caso de uma rede sem fio, a maneira com que são organizados, AP's e nós, vão influenciar diretamente na qualidade, escalabilidade, disponibilidade e desempenho da rede. Existem atualmente três possíveis topologias de rede que atendam os padrões IEEE, sendo estas analisadas a seguir.

2.2.1. Topologia Ad-Hoc

As redes Ad-Hoc são criadas por dispositivos que se comunicam entre si através de um canal de comunicação estabelecido somente no período em que ocorre a troca de dados entre os dispositivos [Bonatto, 2007].

O termo *Ad-Hoc* pode ser substituído por *Independent Basic Service Set* (IBSS), pois cada dispositivo é de certa forma independente, podendo migrar de uma rede para outra sem problemas de conexão [Malafaya, 2007].

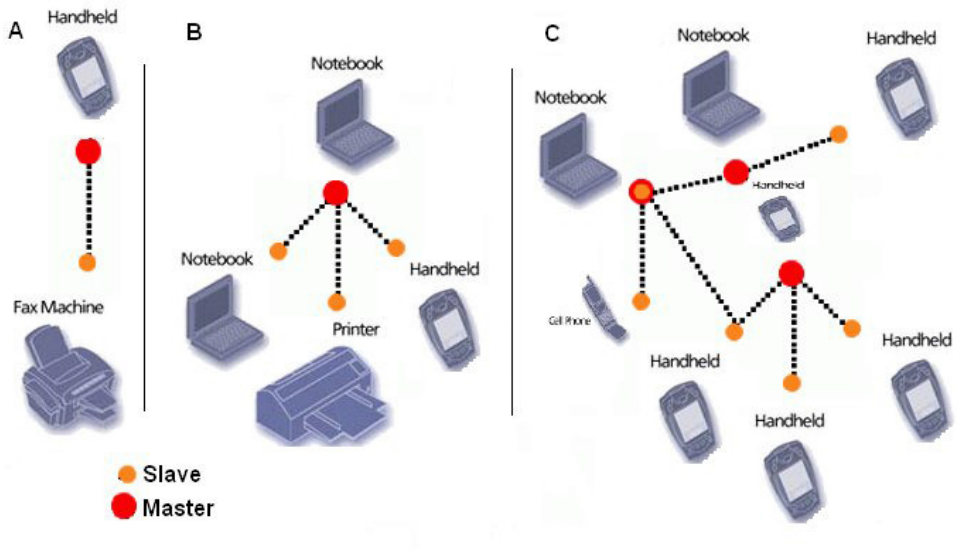


Figura 1 - Topologia Ad-Hoc:A – Piconet, B – Piconet Multi-Slave C – Scatternet, usadas com padrões IEEE 802.15.

Como ilustra a figura 1, é composta por dispositivos denominados mestre, que requisita e coordena a transmissão e recepção dos dados, e escravo que apenas provem o serviço às redes Ad-Hoc, são divididas em três grupos classificadas de acordo com a quantidade de mestres presentes na rede. O primeiro grupo é denominado *Piconet* Simples (A), o segundo *multi-slave* (B), e o terceiro *Scatternet* (C).

2.2.2. Topologia de Infraestrutura

Consiste em computadores e um ou mais AP's, configurados com o padrão 802.11 ou 802.16. Dependendo da quantidade de pontos de acesso a rede pode ser caracterizada como: *Basic Service Set* – BSS (um AP) e *Extended Service Set* – ESS (dois ou mais AP's), conectados entre si através de uma rede cabeada, onde todas as comunicações entre os computadores móveis, ou entre uma estação SF e um cliente fixo, é realizada através do AP [Endler, 2004], como na figura 2.

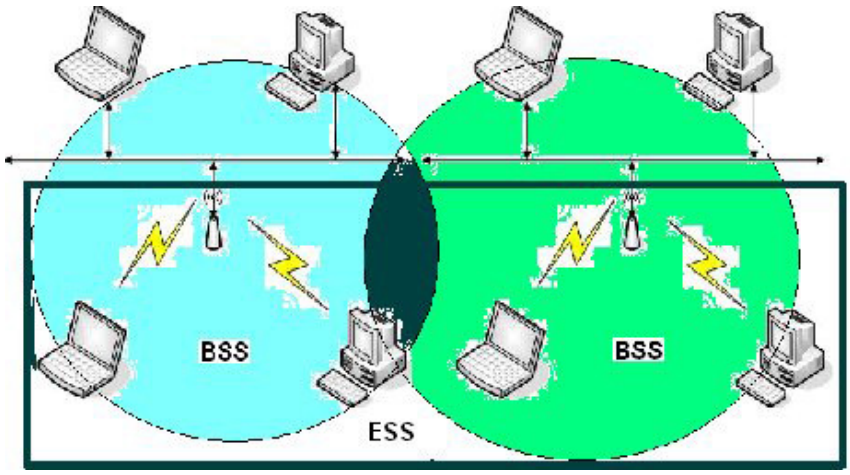


Figura 2 - Topologia de Infraestrutura e suas classificações BSS (1 AP) e ESS (2 ou mais AP's).

A utilização da topologia Infraestrutura em ambientes universitários ocorre principalmente em locais que oferecem acesso a redes sem fio conectadas a uma rede guiada já existente na instituição, geralmente através dos padrões IEEE 802.11a/b/g/n.

2.2.3. Topologia em Malha (Mesh)

As redes *Wireless Mesh Networking* – WMN foram desenvolvidas com o objetivo de ampliar o alcance das redes sem fio convencionais. Para isso, a rede deve ser formada por dois tipos de nós denominados roteadores e clientes e baseia-se nos padrões desenvolvidos pela família IEEE 802.11s [Schiller, 2006] e [Bruel, 2004].

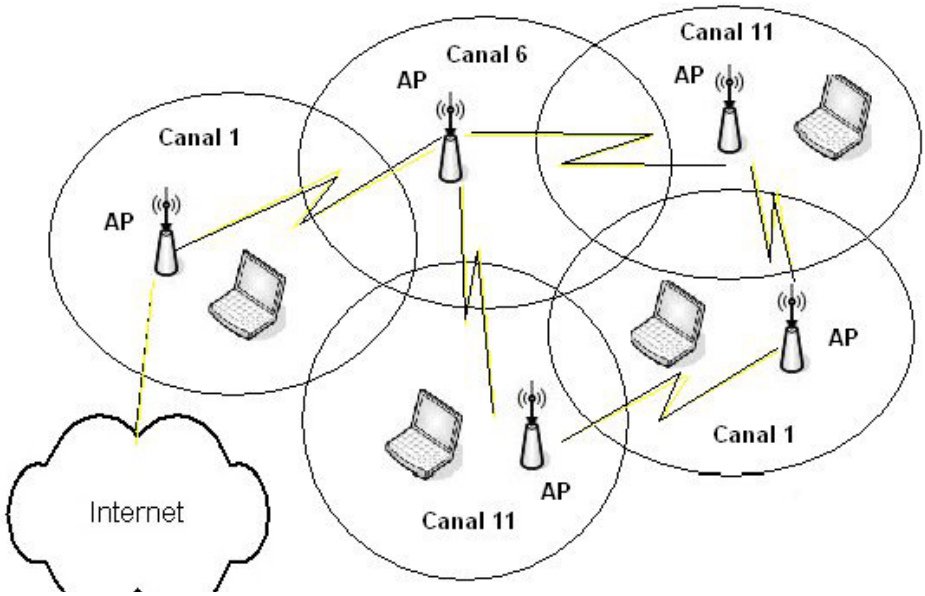


Figura 3 - Topologia de Rede em Malha (Mesh).

Na figura 3, é possível perceber a característica da não necessidade de cabos para a comunicação entre os pontos de acesso, possibilitando a criação de uma rede autoconfigurável com múltiplos AP's. As redes em malha se tornam relevantes a ambientes universitários, pois oferecem comunicação entre nós, otimizando o tráfego das mesmas e aumentando o perímetro de cobertura.

Após os estudos realizados sobre as possíveis topologias de redes sem fio, percebe-se que as redes Piconet e Scatternet, são utilizadas principalmente, onde a necessidade de conexão entre dispositivos ocorre em tempo real, rápida e fácil. As redes de infraestrutura, destacam-se principalmente na conexão entre redes sem fio, tendo uma rede guiada como porta de saída para outras redes distintas (Internet). Já as redes em malha seriam mais funcionais provendo serviços de acesso a grandes áreas locais, onde a exigência de roteamento entre os nós da rede é determinante.

2.3. EQUIPAMENTOS E MODOS DE OPERAÇÃO

Seguem opções de equipamentos e modos de operação para definir uma melhor combinação que atenda a necessidade deste trabalho na definição da infraestrutura de redes sem fio e assim minimizar erros futuros com relação a estas escolhas.

2.3.1. Ponto de Acesso em redes sem fio (AP - Access Point)

Existem basicamente três configurações ou modos de operação para os dispositivos de AP's:

2.3.1.1. Ponto de Acesso modo Repetidor (Hub) – Camada Física

Os dispositivos que operam no modo repetidor, são geralmente aplicados como extensor do alcance da rede sem fio ou guiada, ou seja, são utilizados para aumentar o alcance e perímetro de cobertura das redes.

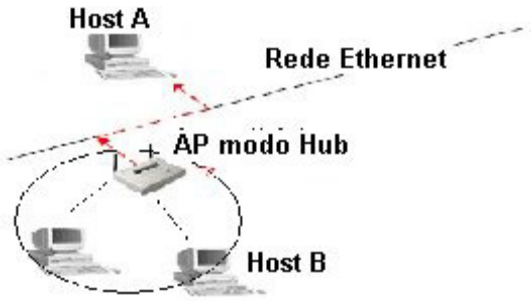


Figura 4 - Exemplo de AP aplicado com o objetivo de aumentar o perímetro da rede guiada.

2.3.1.2. Ponto de Acesso modo Bridge (Ponte) – Camada Enlace

Em síntese, um equipamento Bridge Wireless é um mecanismo de ponto de acesso equipado com rádio transmissor/receptor usado para conectar dois segmentos de uma mesma rede que estejam geograficamente separadas.

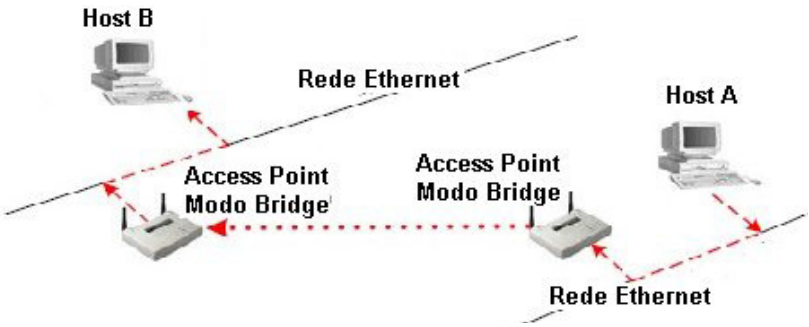


Figura 5 - Exemplo de comunicação entre hosts através de dois AP's no modo Bridge.

2.3.1.3. Ponto de Acesso modo Router (Roteador) – Camada de Rede

São dispositivos que apresentam características próprias, como firewall e portas 10/100 (Ethernet). Em síntese o AP funciona conectando segmentos de rede seja cabeada ou não.

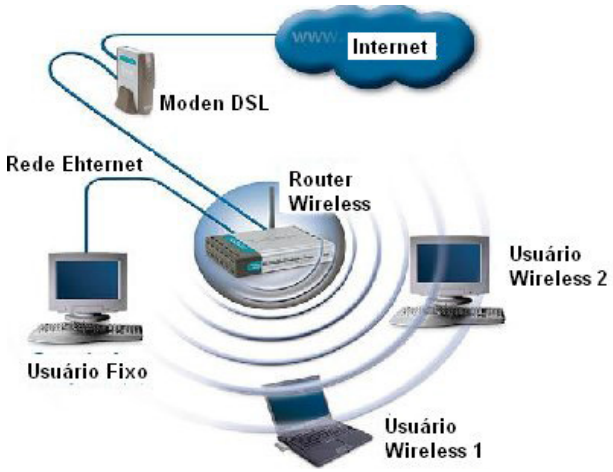


Figura 6 - Mostra a conexão à internet de duas redes conectadas ao router wireless.

Como se vê na figura 6, existem dois segmentos de rede, sem fio e guiado, sendo conectados a internet através de um AP operando no modo router. Assim, percebe-se que a escolha do modo de operação dos AP's da rede pode variar de acordo com a necessidade e cenários aplicados a rede.

2.3.2. Dispositivos para Irradiação de RF (Rádio Frequência)

Para abranger toda a área do campus geralmente será necessária a utilização de antenas para aumentar o alcance dos AP's. Sabendo que toda a transmissão e recepção de sinais wireless, baseiam-se em comunicação por Rádio frequência(RF) e que o comportamento destes equipamentos (antenas) pode afetar drasticamente o desempenho de rede sem fio [Farias, 2006], é importante observar alguns aspectos relevantes para a escolha adequada dos dispositivos de irradiação.

2.3.2.1. Distância

Devido à degradação sofrida pelo sinal ao longo da sua propagação, [Angelo, 2003] conhecida como perda de amplitude os usuários localizados na borda do perímetro de cobertura podem receber um sinal ruim, por isso recomenda-se que as antenas cobram uma distância maior que a especificada pelo projeto de rede.

2.3.2.2. Largura da onda

A largura de onda denota o alcance de um sinal. Geralmente, quanto mais larga for a onda, mais curta será a área de cobertura, porém, as ondas mais largas compensam melhor as barreiras como vento, chuva e paredes que prejudicam o sinal.

2.3.2.3. Ganho

Expresso em dbi(decibel), é a potência do sinal após processado por um dispositivo eletrônico (amplificador). Ganhos maiores gastam mais energia, alcançam distâncias maiores e irradiam o sinal a locais não desejados. Ganhos menores aumentam a margem de erro durante a transmissão de dados.

2.3.2.4. Tipo da Antena

Existem tipos de antenas para aplicações wireless: Omnidirecionais, Semi-Direcionais e Direcionais, sendo cada uma com características e formas de irradiação próprias [Bravo, 2007].

- **Omnidirecional**: Cobrem 360º no plano horizontal e entre 3 e 20° na vertical, por isso são mais funcionais quando aplicadas em áreas amplas para comunicação do tipo ponto-multiponto, onde a estação base (ponto de acesso) se encontra no centro das estações remotas (clientes) [Bravo, 2007].

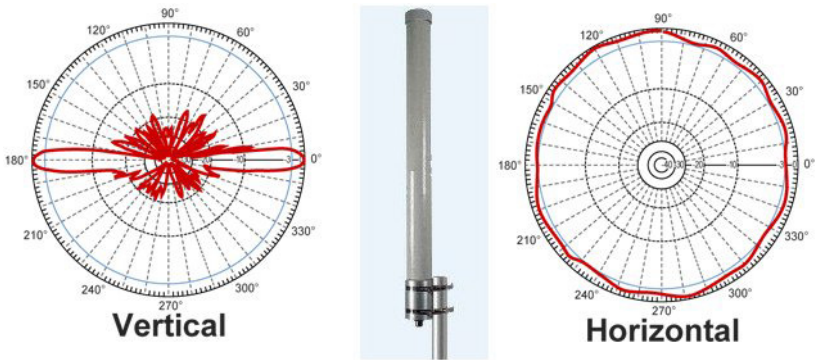


Figura 7 - Antena Omnidirecional e seu diagrama de irradiação 360° - Horizontal e 3-20° - Vertical.

- **Direcional**: Desenvolvidas de maneira a prover o sinal em uma única direção, concentrando a propagação vertical e horizontal entre 3 e 60° de abertura.

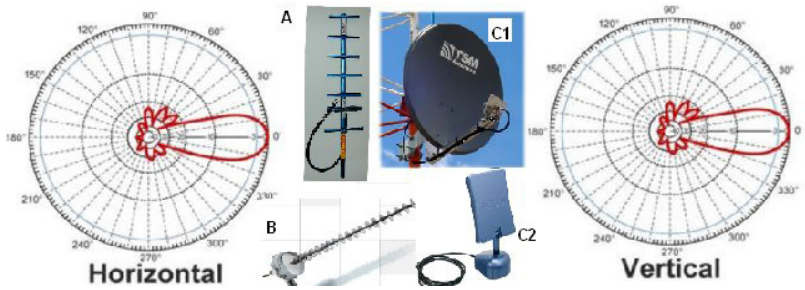


Figura 8 - Antenas A - Yagi, B – Helicoidal e C1 e C2 – Parabólica, e o diagrama de irradiação.

- **Semi-Direcional**: Assim como as antenas Direcionais, as Semi-Direcionais, transmitem os sinal em uma única direção, porém, com um ângulo de irradiação bastante aberto, entre 30 - 180° graus na horizontal, e entre 6 - 90°, na vertical [Bravo, 2007] como mostra a figura 9.

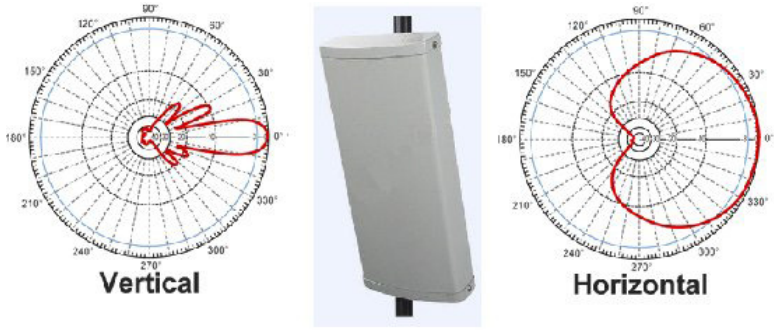


Figura 9 - Exemplo de antena Semi-Direcional (Setorial) e seu diagrama de elevação.

2.4. CONSIDERAÇÕES

Nota-se que a definição de uma infraestrutura de redes sem fio a ser adotada envolve a análise de vários dispositivos e suas configurações, como: padrões de comunicação IEEE, topologias, AP e antenas. A decisão sobre estas opções está

diretamente ligada às necessidades e características do ambiente onde a rede será implementada.

A composição e configuração das redes sem fio dependem dos serviços a serem oferecidos aos usuários, da forma como essas redes interagem e também quais as áreas que a rede deve cobrir.

Assim, no capítulo 4 serão definidas as características dos padrões, equipamentos e serviços do ambiente proposto para este trabalho que garanta a conexão do usuário em redes sem fio heterogêneas, compartilhadas através de uma autenticação segura.

3. SEGURANÇA EM REDES SEM FIO

As redes wireless têm sido largamente utilizadas em corporações e instituições de ensino para auxiliar as tarefas cotidianas de seus usuários, tendo em vista o aumento da produtividade e outros benefícios. No entanto, o principal obstáculo para uma maior expansão dessas redes encontra-se na questão da segurança de suas informações e usuários, onde os principais desafios podem ser representados por [Andrade, 2003]:

Autenticação: garantir acesso somente as estações/usuários autorizados;

Confidencialidade: garantir que os dados capturados não sejam compreendidos;

Integridade: certificar-se que os pacotes recebidos são iguais aos enviados pelo transmissor.

Para avaliar adequadamente os mecanismos oferecidos para proteger a rede de forma adequada, é necessária uma análise das principais formas de explorar as falhas e vulnerabilidades.

3.1. PRINCIPAIS ATAQUES A REDES SEM FIO.

Os ataques às redes sem fio apresentam algumas características próprias, que as diferem das redes cabeadas, como por exemplo, a necessidade de que o atacante esteja dentro do perímetro de cobertura da rede durante o ataque e a

possibilidade de obter informações mesmo sem estar autenticado à mesma [Duarte, 2003].

Os ataques podem ser divididos em dois grupos, passivos (usuário malicioso não altera as informações capturadas) e ativos (ocorre a alteração das informações capturadas ou configurações dos dispositivos acessados), como mostra a figura 10 [Amaral, 2004].

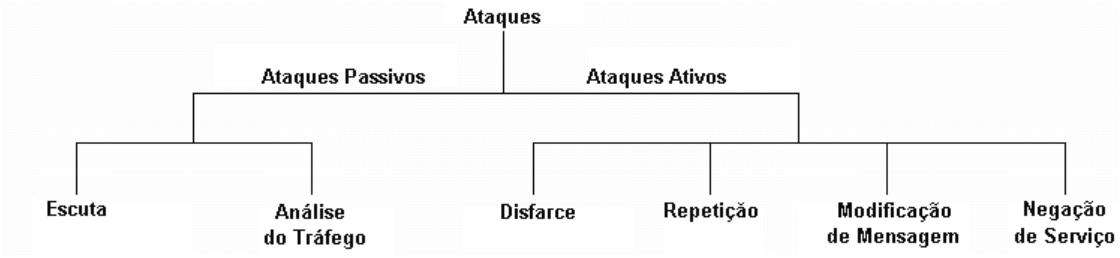


Figura 10 - Tipos de ataques a redes sem fio

Diversos padrões foram desenvolvidos para dificultar e até mesmo eliminar as vulnerabilidades em redes SF, dentre eles destacam-se os padrões WEP, WPA, WPA-2/802.11i e 802.1X como veremos a seguir.

3.2. PADRÕES DE SEGURANÇA EM REDES SEM FIO

3.2.1. Padrão WEP

Devido este ser um dos primeiros protocolos de segurança incorporado às redes 802.11, em 1995, apresenta algumas vulnerabilidades e falhas identificadas,

por exemplo, a chave de criptografia RC4, fazendo com que o protocolo WEP perdesse quase toda sua credibilidade sendo, preferencialmente, indicado em redes pequenas onde o valor das informações não compromete as aplicações ou usuários, ou ainda, em redes com dispositivos antigos com padrão 802.11b que não permitam a atualização para versões mais atuais e seguras como WPA e WPA-2 [Barcelos, 2003] e [Roshan,2002].

3.2.2. WPA e WPA-2/802.11i

Por causa de interesses conflitantes no mercado de WLANs, ocorreu um atraso na homologação do padrão IEEE 802.11i. Como resultado, um conjunto de empresas (Wi-Fi Alliance), desenvolveu uma solução chamada WPA - (Wi-Fi Protected Access) [Linhares, 2005].

Dentre as características deste padrão têm-se o fato dos dispositivos que trabalham com o WPA suportarem o padrão WEP além das melhorias: TKIP e autenticação baseada no protocolo 802.1X. Posteriormente com o desenvolvimento do padrão WPA-2 em 2004, que corresponde ao padrão 802.11i, passou a operar, também, com o algoritmo de criptografia AES.

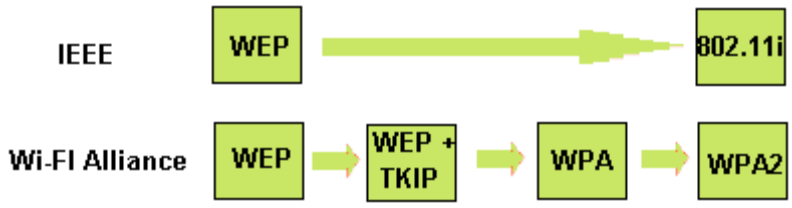


Figura 11 - Linha evolutiva dos padrões de segurança IEEE e WiFi Alliance.

Na figura 11 percebe-se a cronologia de desenvolvimento dos padrões de segurança. Pode-se concluir que o primeiro padrão, efetivo, desenvolvido foi o WEP adotado pelos grupos IEEE e Wi-Fi Alliance. Após a identificação das vulnerabilidades WEP o padrão IEEE se esforçou para desenvolver o padrão 802.11i enquanto o grupo Wi-fi buscou o desenvolvimento do mesmo através de melhorias por etapas lançando os novos padrões, WPA e WPA-2.

3.2.3. Autenticação 802.1X

O método consiste basicamente na autenticação de estações e usuários baseado nas informações obtidas por um cliente NAS (Network Authentification Service). Os dados obtidos devem ser repassados ao servidor responsável pela autenticação dos usuários, geralmente, opta-se pelos mesmos mecanismos utilizados para autenticação de usuários remotos, denominado RADIUS (Remote Authentication Dial-In User Service) [RFC-2865, 2000], embora outras soluções também possam ser usadas[Amaral, 2004].

A autenticação baseia-se no EAP (Extensible Authentication Protocol), desenvolvido pelo IETF (Internet Engineering Task Force), com protocolos de autenticação que incluem EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAP, LDAP etc. O que distingui cada método é a forma com que realizam a verificação do desafio enviado ao servidor e nas informações contidas no desafio (senhas, logins, macs, certificados digitais etc.) oferecendo níveis distintos de segurança de acordo com a necessidade da rede [Karygiannis, 2006] e [Amaral, 2004].

3.3. CONSIDERAÇÕES

Foi visto neste capítulo que existem diversas vulnerabilidades nas redes sem fio, decorrentes de falhas relacionadas tanto na configuração quanto na fragilidade dos algoritmos e dispositivos utilizados para proteção da rede.

Percebeu-se também, que os ataques a vulnerabilidades consistem em ações ativas ou passivas, diferenciadas de acordo com o objetivo do atacante e no benefício proveniente do ataque.

4. PROPOSTA DE INFRAESTRUTURA DE REDES SEM FIO

O cenário proposto para este trabalho será o de uma infraestrutura que proporcione conectividade, via rede sem fio, para as salas de aula e a área externa entre os blocos de uma unidade no campus de uma universidade, que neste trabalho será usado como exemplo o prédio do Centro de Tecnologia da UFRJ no campus da Ilha do Fundão, interligando redes de seus diversos departamentos. Essa infraestrutura será sugerida de forma que permita a expansão da área de cobertura para outras unidades dentro do campus.

4.1. PADRÃO DE COMUNICAÇÃO

Pelas características desta infraestrutura, será usado o padrão IEEE 802.11, por ser o mais indicado para uso em redes WLAN's.

Será usado também o padrão 802.11n, em função de suas características, principalmente desempenho, funcionalidades e compatibilidade.

4.2. TOPOLOGIA

Das opções de topologia avaliadas, Ad-Hoc, Mesh e Infraestrutura, a escolhida foi a de infraestrutura. A topologia Ad-Hoc não atende a redes Wlan's, a topologia Mesh é limitada ao padrão 802.11s, não sendo compatível com o padrão 802.11n. O modo de infraestrutura também permite adicionar um AP em qualquer ponto do campus universitário para uma possível expansão desta infraestrutura, desde que o AP esteja conectado, por cabo, a uma rede interna da mesma.

4.3. EQUIPAMENTOS (AP's E ANTENAS)

Como existe a possibilidade de segmentar e estender as redes sem fio e cabeadas, os AP's serão configurados em duas formas diferentes, como elementos de camadas 2 e 3 dividindo domínios de rede e de broadcast através do uso de *routers* e AP's. Este é um recurso que ajuda na segurança, pois permite isolar usuários e serviços em redes distintas.

Como são necessários testes e observações quanto à avaliação do comportamento da propagação do sinal, orientasse que, através da técnica de Site Surveys, analises quanto a localização e ajustes das antenas, ganho e potência, sejam feitos no ambiente real a ser implementada a solução a fim de definir a antena ideal.

Este trabalho considera que as redes já possuam seus equipamentos de distribuição instalados e configurados, como *switches*, roteadores e servidores de aplicativos necessários à implementação.

4.4. PARTICULARIDADE DA UNIVERSIDADE UFRJ.

Existem características comuns em ambientes universitários como, efeitos atmosféricos (chuvas, raios, maresia, neblina), paredes mais espessas devido a tratamento acústico ou a arquiteturas antigas, ruídos de equipamentos diversos, redes elétricas próximas à rede sem fio que são desafios comuns aos ambientes universitários.

É interessante segmentar a rede sem fio de acordo com o perfil de seus usuários, definindo grupos e regras de acesso de acordo com a necessidade de cada perfil quanto a serviços e acessos.

4.5. SEGURANÇA

Apesar de todos os padrões avaliados WEP, WPA e WPA-2/802.11i serem viáveis em uma infraestrutura sem fio, indica-se o uso do padrão WPA-2/802.11i por ser considerado o mais seguro entre eles.

A autenticação baseada no protocolo 802.1X com servidor do tipo RADIUS além de criptografia Tkip e AES oferecem mais segurança a rede quando comparado aos demais.

4.5.1. Autenticação

Será usado o padrão WPA-2/802.11i na autenticação dos usuários para permitir que em qualquer local atendido por esta infraestrutura, independente da administração da rede, os usuários possam ter acesso à rede, por isso, cada departamento precisará ter em sua rede um servidor de autenticação baseado no protocolo 802.1X.

Dentre as possíveis soluções destaca-se a utilização de softwares, algumas vezes em conjunto com hardware, denominadas Appliances, como meio mais prático de realizar e gerenciar a autenticação dos usuários. Pode-se citar as soluções proprietárias Mikrotik [Mikrotik, 2009], StarOS [StarOS, 2009] etc, como possíveis alternativas de soluções, ou ainda, a possibilidade de utilizar sistemas gratuitos como FreeRadius [FreeRadius, 2009], OpenRadius [OpenRadius, 2009] etc, com o auxílio de ferramentas de consulta (ex. Mysql, Oracle, Ldap etc), obtendo resultados próximos ou ainda melhores que os oferecidos pelos Appliences, proprietários, citados anteriormente.

4.5.2. Firewall

Durante a avaliação das opções de firewall, priorizaram-se os gratuitos para diminuir os custos de implementação e também a sua configuração via web, para facilitar o gerenciamento do software.

Importante também as funcionalidades do firewall (filtro de pacote, protocolo etc.), para controlar o acesso aos serviços disponíveis na rede e o serviço de Captive Portal, para gerenciar a autenticação dos clientes, já incluso no aplicativo. O objetivo foi facilitar o processo de aquisição dos dados de login, sem a necessidade de instalar softwares adicionais para este processo (ex. WiFiDog, AirMarshal, ChilliSpot, Summit etc).

O firewall PFSense foi o que melhor atendeu as necessidades do projeto, incluindo os serviços básicos de firewall (filtros pacote/protocolo), sendo o único a prover o serviço de portal de captura incluso ao software. No entanto, é sabido que no serviço captive portal há uma limitação, ele só aceita requisições de acesso de clientes com endereço IP da mesma rede da interface a qual está gerenciando. Esta limitação nos levou a utilizar o software de código aberto Chillispot, que é bastante utilizado para a função de portal de captura.

4.5.3. Servidor RADIUS

Autenticar usuários através do protocolo 802.1X, requer um aplicativo para esse fim.

As soluções Rad Series Radius [RadSeries, 2009] e Steel Belted Radius [SteelBelted, 2009], são soluções proprietárias e elevam os custos da implementação. O aplicativo não proprietário FreeRadius v.2.1.4 [FreeRadius, 2009], é uma ferramenta open source que é amplamente usado para disponibilizar acesso a rede sem fio através dos serviços de autenticação, autorização e contabilização dos usuários da rede [FreeRadius, 2009].

O FreeRadius destaca-se por operar em diferentes plataformas gratuitas como: Linux, FreeBSD, OpenBSD, OSF/Unix e Solaris além do S.O. proprietário Windows. Utiliza vários métodos de autenticação como: Eap, Chap, Ms-Chap, Ldap etc, controle de conexões simultâneas e requisições a banco de dados remoto. Outra qualidade foi observada na segurança da comunicação entre servidores externos, através de criptografia TLS (Transport Layer Security) [RFC 4346, 2006] e SASL (Simple Authentication and Security Layer) [RFC 4422, 2006].

Estas características levaram a escolha do software FreeRadius como servidor RADIUS usado na autenticação de usuários.

4.5.4. Login dos usuários de bases de dados de tipos diferentes

Um dos principais desafios encontrados na implementação de redes sem fio em ambientes universitários consiste no fato de existir um grande fluxo de clientes, às vezes separados em bases de dados diferentes, dificultando o controle e centralização das informações pertinentes a cada usuário.

Para contornar esta dificuldade e permitir o uso do servidor RADIUS para autenticação de usuários através do protocolo 802.1X, optou-se por autenticar usuários através dos serviços já existentes de autenticação de usuários em cada rede envolvida, bastando para isso adaptar o servidor RADIUS de acordo com cada rede, seja o seu método de autenticação de usuários Ldap, PAM, Shadow etc.

Assim fica garantida a interoperabilidade e facilita a implementação desta nova infraestrutura sem grandes transtornos para os administradores de redes.

4.6. EQUIPAMENTOS

A seguir especificam-se os equipamentos envolvidos nesta infraestrutura citando alguns modelos compatíveis. A quantidade de cada um vai depender da

extensão da área a ser coberta com relação ao número de unidades envolvidas do campus.

- Access Point

- Switch Cisco SRW2024

- Roteador

- Servidor RADIUS

- Notebook adicional para execução dos testes.

Abaixo as características de cada componente da rede.

4.6.1. Access Point

As configurações aplicadas a estes equipamentos limitam-se ao padrão IEEE 802.11n para comunicação com cliente e utilização de criptografia WPA-2 e autenticação via 802.1x (RADIUS) apontando para o servidor RADIUS.

Figura 12 - AP Linksys

4.6.2. Switch

Conforme visto, uma universidade possui diversas redes com suas necessidades de acessos e serviços. Assim o switch é usado nesta infraestrutura por permitir o uso de várias redes locais possibilitando uma segmentação do fluxo de dados por diferentes redes e também para adicionar novos AP`s a rede, caso a mesma necessite ser expandida.

Figura 13 - AP Linksys WRT54G

4.6.3. Roteador

Neste equipamento apenas as tabelas de roteamento serão configuradas, de forma a direcionar os dados das redes até a interface Captive Portal do servidor FPSense.

Figura 14 - Roteador cisco

4.6.4. Servidor RADIUS

As configurações deste computador são referentes ao funcionamento do gateway, onde ficarão os aplicativos com os serviços necessários ao funcionamento desta infraestrutura: PFSense, FreeRadius,Chillispot e Banco de dados com o registro dos usuários.

4.6.5. Notebook adicional para execução dos testes.

Equipamento necessário para teste da funcionalidade dos outros equipamentos e serviços que comporão toda a infraestrutura.

4.7. TOPOLOGIA DE REDE

A figura 15 representa uma topologia usando LANs sem fios com base num Captive Portal associado a um servidor RADIUS. Nesta topologia temos duas LANs virtuais: a 10.20.1.0/24 com o gateway 10.20.1.1 e a 10.30.1.0/24 com o gateway 10.30.1.1. A ligação entre os usuários das subredes e o servidor é feita através de pontos de acessos sem fios, que necessitam estar numa subrede do servidor.

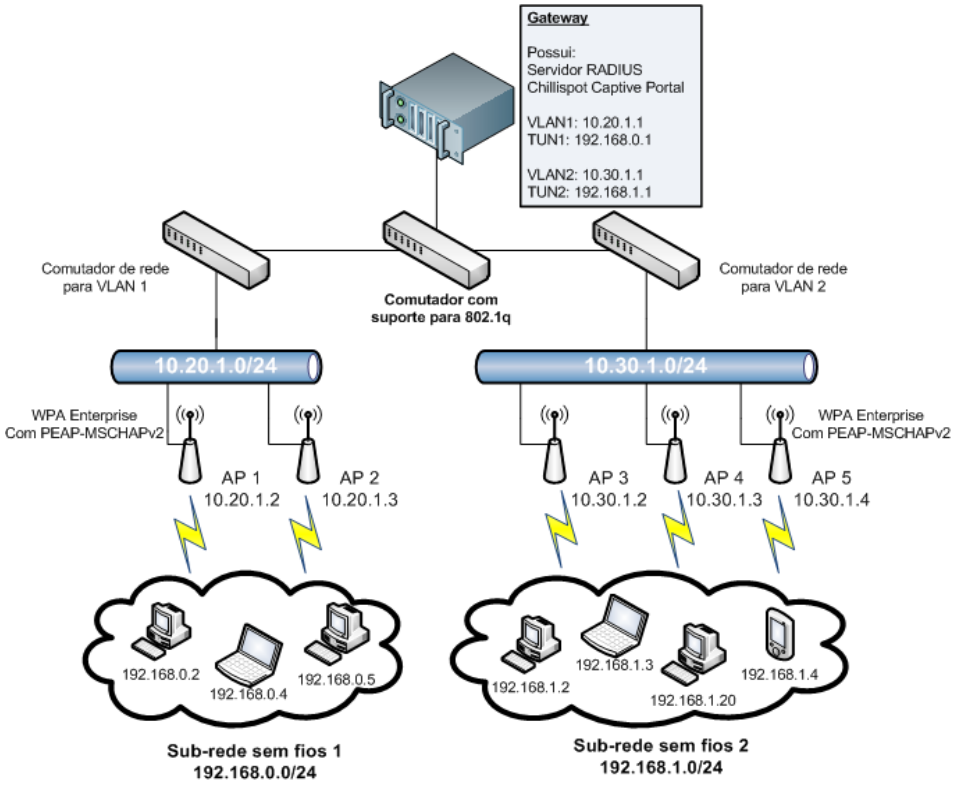


Figura 15 - Modelo de topologia de rede usando Captive Portal

4.8. VALIDANDO LOGIN DOS USUÁRIOS

Uma topologia de rede sem fios para uma comunidade de usuários de uma universidade precisa de uma solução do tipo Captive Portal, para o controle e gestão de acessos, e um servidor RADIUS para a validação das credenciais. Por se tratar de uma universidade não usaremos a contabilização.

A maioria dessas implementações de Captive Portal com código aberto usam o programa Chillispot. O Chillispot é usado para autenticar os utilizadores presentes numa LAN com/sem fios e gerir a alocação dos endereços IP. A autenticação pode ser feita através de uma página Web ou através de protocolos de autenticação e segurança usados em redes sem fios como o WPA (Wi-fi Protected Access). A autorização e contabilização são feitas pelo servidor RADIUS.

O Chillispot possui dois tipos de autenticação possíveis, Universal Access Method (UAM) e Wireless Protected Access (WPA). Com o UAM o sistema cliente pede e recebe um endereço IP ao servidor. Quando o usuário inicia um navegador Web o Chillispot irá interceptar a ligação TCP e redirecionar o navegador para um servidor Web de autenticação. O servidor Web pede um nome de utilizador e palavra-chave ao cliente. A palavra-chave é cifrada e enviada para o Chillispot.

Com o WPA a autenticação é tratada pelo ponto de acesso sem fios, e é subsequentemente reencaminhada do ponto de acesso para o Chillispot presente no servidor.

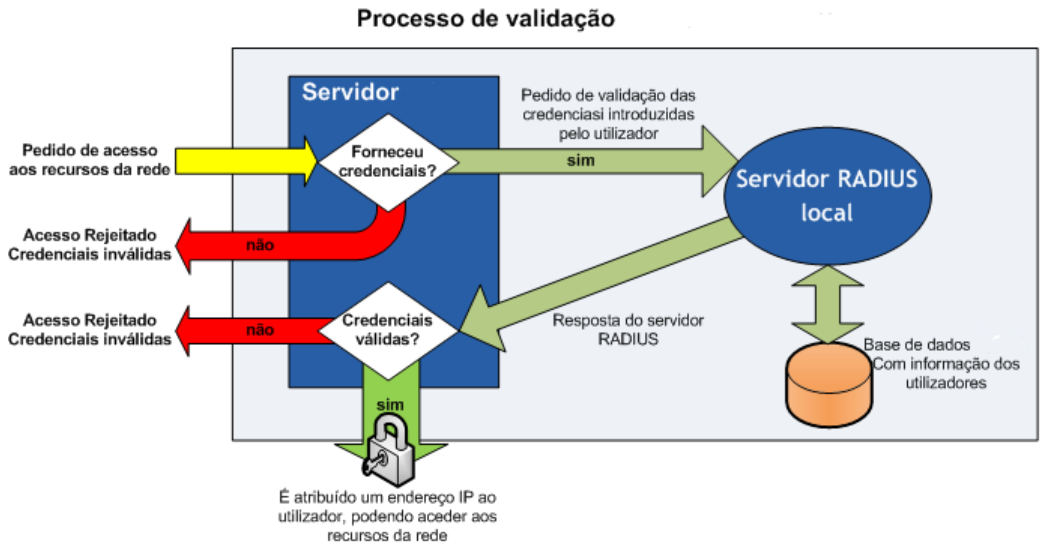


Figura 16 - Sequência de eventos para autenticação de usuário pelo Radius

Tanto para o UAM ou o WPA o Chillispot reencaminha o pedido de autenticação para o servidor RADIUS. O servidor RADIUS envia uma mensagem Access-Accept para o Chillispot se as credenciais introduzidas pelo utilizador forem válidas. Adicionalmente, pode enviar também outra informação como por exemplo um endereço de IP fixo ou o tempo máximo de ligação. Caso as credenciais não sejam válidas é enviado um Access-Reject.

Quem atribui os endereços IP aos clientes sem fios que se autenticam na rede local pelos pontos de acesso é o Chillispot. Para isso ele cria um dispositivo virtual de rede para tunelling (TUN), associado à interface VLAN. Em redes de computadores, TUN é um dispositivo de rede virtual do kernel simulando um dispositivo da camada de rede que permite implementar dispositivos de rede que são inteiramente suportados por software, que é diferente dos dispositivos de rede comuns que são suportados por adaptadores de rede físicos.

Os pacotes enviados por um sistema operativo através de um dispositivo TUN são entregues a um programa ao nível do utilizador que se associa ao dispositivo. Um programa ao nível do utilizador pode também passar pacotes para um dispositivo TUN. Neste caso, os dispositivos TUN injetam estes pacotes na camada de rede do sistema operativo.

5. CONCLUSÃO

A motivação deste trabalho foi expor a necessidade de uma melhor utilização das redes sem fio dentro de um ambiente universitário, indicando uma forma atrativa e segura que ajude a atender as necessidades cada vez maiores dos usuários em dispor de conectividade no maior tempo possível, com uma área de cobertura cada vez maior.

Após um breve estudo dos conceitos de redes sem fio relacionados ao trabalho e uma avaliação do cenário, buscamos uma solução ideal para a infraestrutura de redes sem fio, possibilitando a autenticação dos usuários de diferentes redes de forma segura.

Essa infraestrutura é flexível, porque permite que se aumente a área de cobertura da rede sem fio adicionando à topologia equipamentos como switch e AP's. Através do uso do padrão WPA-2/802.11i nos AP`s para comunicação e autenticação por RADIUS, garantimos uma segurança na utilização da rede e permitimos uma melhor autonomia entre as redes envolvidas, uma vez que as bases de dados com os cadastros dos usuários continuam com suas próprias administrações, permitindo a manutenção e gerência descentralizada. Demais restrições do sistema devem ocorrer através de firewall, representado no trabalho pelo sistema PFSense. A preferência por aplicativos gratuitos/livres é um esforço na redução dos custos com a implementação.

5.1. LIMITAÇÕES DA PESQUISA E TRABALHOS FUTUROS

O comportamento e a qualidade do sinal no perímetro da rede não pode ser avaliado de forma satisfatória.

Outra observação é quanto ao uso de endereço MAC como forma de restringir acessos indevidos e controlar múltiplas contas de acesso para um mesmo usuário.

Espera-se um sinal com qualidade que não comprometa o limite da rede ou torne a mesma vulnerável, assim propõe-se como estudos futuros o estudo mais profundo relacionado à propagação do sinal ao longo dos ambientes universitário.

6. REFERÊNCIAS

Aboba, B., Calhoun, P. **RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)**. 2003. IETF Request for Coments 3579.

Amaral, Bruno Marques.; Maestrelli, Marita.Bonatto, Aurélio.; Canto, Diego Oliveira do. **Bluetooth technology (802.15): Bluetooth**. 2007.

Amaral, Bruno Marques.; Maestrelli, Marita.Bonatto, Aurélio.; Canto, Diego Oliveira do. **Segurança em Redes Wireless 802.11**. CBPF-NT-002/04. 2004.

Andrade, L. et al. **Análise das vulnerabilidades de segurança existentes nas redes locais sem fio: um estudo de caso do projeto wlaca**. 2003. Disponível em: <http://www.cci.unama.br/margalho/artigos/wlaca.pdf>. Acesso em: 29 jan. 2014.

Angelo, Ludmila Aparecida.; Barbosa, Victor Antônio Mendonça. **Redes Wireless - Conceitos, Projetos e Especificações**. 2003. 94 f. Tese (Dissertação E. Computação) - Escola de Engenharia Elétrica e de Computação - Universidade Federal de Goiás, Goiânia. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520: informação e documentação. Citações em documentos: apresentação**. Rio de Janeiro, 2002.

Barcelos, João P. M. e Gonçalves, Raphael Guimarães e Nilton Alves Jr. **O Padrão 802.11**. CBPF-NT-003/03. 2003.

Carvalho, Leandro Ouriques M. de.; Cunha, Pablo Salino. **Seminário e Redes de Computadores II, 802.15.4 e ZigBee**. 2004.

Duarte, L.O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** 2003. 55 f. Tese (Monografia B. C. Computação) - São José do Rio Preto, SP. UNESP / IBILCE. 2003.

Farias, Paulo César Bento. **Redes Wireless - Partes 2, 9, 12, 13, 21 e 34** . 2006. Disponível em: <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless003.asp> Acesso em: 19 dez. 2013.

Karygiannis, T. e Owens, L. **Wireless Network Security. 802.11, BluetoothTM and Handheld Devices**. Publicação 800-48. NIST – National Institute of Standards and Technology. 2006.

KUROSE, James F.; ROSS, Keith W.,- **Redes de Computadores e a Internet – um abordagem Top-down**, Person, 2006.

Lakatos, Eva Maria. Marconi, Marina de Andrade. **Metodologia do trabalho científico.** 4. ed. São Paulo: Atlas, 1992.

Lima, Luciana dos Santos; et al. **WiMAX: Padrão IEEE 802.16 para Banda Larga Sem Fio. 2006. 58 f. Tese (Monografia em C. Computação)** – Departamento de Informática – Pontífica Universidade Católica, Rio de Janeiro. 2006.

Linhares, André Guedes; Gonçalves, Paulo André da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w*.** 2005.

Malafaya, Hugo.; Tomás, Luís.; Souza, João Paulo. **Sensorização Sem Fios sobre ZigBee e IEEE 802.15.4**. 2006.

Mikrotik. **Mikrotik Router and Wireless**. Disponível em: <http://www.mikrotik.com>. Acesso em: 20 dez. de 2013.

Oliveira, Ricardo Pais de; Campos, Rui Lopes. **Projeto de Redes Locais Sem Fio 802.11b. 2003. 165 f**. Projeto elaborado na Unidade de Telecomunicações e Multimédia da Faculdade de Engenharia da Universidade de Porto - Porto, Portugal. 2003.

ROSS, John. **O livro de WI-FI: Instale, configure e use Redes Wireless (sem-fio)**. Rio de Janeiro. Editora Alta Books, 2003. 246p.

Santos, Ricardo Luiz. **Segurança em Redes Sem Fio: Wlan.** 2003. 67 f. Tese (Pós-Graduação Latu Sensu em Redes de Computadores) – Universidade Estadual de Londrina – Londrina, PR. 2003.

Schiller, Felipe Ortigão Sampaio Buarque. **Redes em Malha**. 2006. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf/felipe/index.htm>. Acesso em 16 nov. 2014.

Schweitzer, Christiane M. **Tecnologias de redes sem fio: WPANs, WLANs E WMANs Desafios de Segurança, Vulnerabilidades e Soluções.** 2004.

Silva, Mônica F. da.; Câmara, Jeferson.; Abelém, Antônio J. G.; Stanton, Michael A. **Redes Sem Fio Metropolitanas Baseadas no Padrão 802.16: Um Estudo de Caso Para Belém-PA**. 2005. XXV Congresso da Sociedade Brasileira de Computação.

StarOS. **Sistema Operacional para Redes Wireless**. Disponível em:<http://staros.com.br/oproduto.htm>. Acesso em: 25 jan de 2014.

Veríssimo, Fernando. **O Problema de Segurança em Redes Baseadas no Padrão 802.11**. 2003. Disponível em: <http://www.lockabit.coppe.ufrj.br/artigo/problema-seguranca-em-redes-aseadas-no-padrao-80211>. Acesso em: 09 fev. 2014.