Estudo de caso da implantação de uma rede sem fios utilizando ferramentas de código aberto

Amauri Tiago Marx[1], Fabrício Paloschi[1], Claunir Pavan[2]

[1]Universidade do Oeste de Santa Catarina – Campus de São Miguel do Oeste
89.900-000 – São Miguel do Oeste – SC – Brazil

[2]Universidade de Aveiro
3810-193 – Aveiro – Portugal

{amauri,fabricio}@unoescsmo.edu.br, pavan@ua.pt

Abstract. *The functionality of wireless networks, allied with the low cost for network building and management, is each time more employed in the organizations. The university has an interest in providing practical and easy access to network resources on campus. However, the use of general access labs doesn't always meet the demand or practicality desired. This paper describes a case study of deploying a wireless network based on open source tools on the campus of the Universidade do Oeste de Santa Catarina, in São Miguel do Oeste. The possibility of offering this service so transparent to the end user was one of the determining factors for choice of tools of this project.*

Keywords*: Wireless Networks, Open Source Tools.*

Resumo. *A funcionalidade das redes sem fio, aliado ao baixo custo para implantação e gestão, é cada vez mais empregada nas organizações. A universidade tem interesse em prover acesso prático e fácil aos recursos de rede do campus. Contudo, o uso de laboratórios de acesso geral nem sempre atende a demanda ou praticidade desejada. Este artigo descreve um estudo de caso da implantação de uma rede sem fios baseada em ferramentas de código aberto no campus da Universidade do Oeste de Santa Catarina, em São Miguel do Oeste. A possibilidade de oferecer este serviço de forma transparente ao usuário final foi um dos fatores determinantes para a escolha das ferramentas deste projeto.*

Palavras-chave*: Redes sem Fio, Ferramentas de Código Aberto.*

1. Introdução

Atualmente o crescimento de aplicações para a Internet têm sido impressionante, tornando as redes de computadores recursos críticos em qualquer sistema de informação. A diversidade e facilidade na aquisição de dispositivos conectáveis em rede, devido ao seu baixo custo, influencia significativamente na forma como os negócios são hoje conduzidos.

Recentemente, a popularização do acesso às redes sem fio ocorreu por conta de locais de acesso livre, que são cada vez mais comuns em locais públicos – bibliotecas, parques, cafés, livrarias, hotéis. Em instituições de ensino, principalmente universidades, esta tecnologia está cada vez mais presente. Para o caso apresentado neste artigo, a instituição disponibiliza informações de interesse do aluno (tais como calendário acadêmico, consulta de notas, situação financeira, rematrícula, materiais de aula), além de permitir a inscrição em eventos, consultas ao acervo da biblioteca e vários outros serviços possíveis de serem oferecidos via Internet. Os professores, que antes entregavam apostilas para os alunos fotocopiarem, agora preferem disponibilizar o material para *download* a partir de um portal acadêmico, o qual ainda lhes permite fazer uso do diário de classe digital, fórum de discussão, acesso ao perfil dos alunos, dentre outros recursos. Por fim, os alunos de hoje preferem o método de acesso on-line à informação, uma vez que utilizando um computador portátil podem carregar todo o material das disciplinas.

Uma rede local sem fios – WLAN – é constituída de células ou conjuntos básicos de serviço, chamados de BSS (*Basic Service Set*). Cada célula é controlada por uma estação base/ponto de acesso [Ribas 2002; Gast 2002; Kurose and Ross 2007] e utiliza ondas eletromagnéticas que se propagam no ar como meio de transmissão.

Este artigo está organizado da seguinte forma: na seção 2 é apresentada a infra-estrutura de rede local física e o ambiente de implementação da rede sem fios. Na seção 3 são descritos, brevemente, alguns métodos de autenticação e segurança existentes, bem como detalhamentos do método de autenticação por portal e as ferramentas de código aberto utilizadas. A seção 4 engloba os testes de validação da rede em termos de alcance e *roaming* e na seção 5 são apresentadas as principais conclusões, juntamente com algumas considerações finais.

2. Infra-estrutura existente e ambiente de implantação

A Universidade do Oeste de Santa Catarina – Campus de São Miguel do Oeste possui, conforme dados do primeiro semestre de 2008, aproximadamente 4985 acadêmicos, distribuídos entre 30 cursos de graduação e 21 cursos de pós-graduação em nível de especialização. Existem ainda cerca de 360 funcionários, distribuídos entre técnicos administrativos e professores.

A estrutura física do Campus contém atualmente 16 blocos, onde estão situados os setores administrativos (biblioteca, laboratórios, coordenações), salas de aula, cantina, centros de conveniências e auditório, distribuídos entre aproximadamente 22.045 m² de área que compõem o campus.

2.1. Infra-estrutura para a rede sem fios

Devido ao tamanho da área geográfica a ser coberta pela rede sem fio, não seria possível cobri-la com somente um ponto de acesso. Assim sendo, optou-se pela topologia de rede sem fio infra-estruturada, fazendo uso de 28 pontos de acesso (APs) distribuídos em locais estratégicos do campus.

Os locais/pontos estratégicos foram definidos de tal maneira que a BSS criada por um AP tenha uma intersecção com APs adjacentes (fator crítico para permitir o

roaming entre as células). Ainda, foram priorizados os pontos próximos à infra-estrutura cabeada disponível.

Para aumentar a segurança entre as redes administrativas e a rede sem fio, de modo que uma não possa se comunicar com a outra, utilizou-se redes locais virtuais (VLAN). A utilização de VLANs permite maior flexibilidade no gerenciamento das redes, pois possibilita a utilização de redes diferentes em um mesmo *switch* de forma dinâmica e segura. Desta forma, pode-se utilizar a infra-estrutura existente para transportar os dados entre os pontos de acesso espalhados pelo campus, não sendo necessário um equipamento exclusivo.

3. Mecanismos de autenticação e segurança existentes

A autenticação das WLANs pode ocorrer através de diversos mecanismos, dentre eles: (a) autenticação de sistema aberto (*open-system*) – autenticação nula, o ponto de acesso aceita o pedido de associação de qualquer estação [Gast 2002; Rosnam and Leary 2003; Edney and Arbaugh 2003]; (b) autenticação por chave compartilhada (*shared-key*) – utiliza-se do sistema desafio-resposta (*challenge-response*), onde a estação deve responder corretamente a um desafio enviado pelo ponto de acesso, sob pena de não autenticar-se [Gast 2002; Rosnam and Leary 2003; Duarte 2003; Andrade 2004]; (c) autenticação por SSID (*Service Set Identifier*), também conhecido como nome da rede – consiste em desativar o recurso de envio periódico (*broadcast*) do SSID na rede sem fio, obrigando a estação a conhecer previamente a rede sem fio ao qual quer conectar-se [Grünewald 2005]; (d) autenticação por MAC (*Media Access Control*) – o controle do acesso é feito levando em consideração o endereço físico do computador do usuário [Rosnam and Leary 2003]; (e) autenticação por IEEE 802.1x e EAP (*Extensible Authentication Protocol*) – fornece um *framework* para que o sistema de autenticação escolha o método apropriado de autenticação (senhas, certificados digitais ou qualquer outro tipo de token) [Miyano Neto 2004]; (f) autenticação por portal (*hotspot*) – baseado na utilização de um portal de autenticação em conjunto com regras de *firewall*. Neste trabalho será utilizado o método de autenticação por portal, descrito na seção 3.1.

3.1. Autenticação por portal (*hotspot*)

A autenticação por portal, geralmente chamada de *hotspot*, é baseada na autenticação via interface HTTP/HTTPS, configuração de regras de *firewall* dinâmicas e outros recursos centralizados, dispostos em um dispositivo de controle – o qual deve possuir acesso à rede externa – conectado na rede local através do meio guiado. Nesse tipo de autenticação, todo tráfego vindo dos pontos de acesso será interceptado e, somente após a autenticação do cliente, liberado [Carrion 2005].

Desta forma, o acesso será totalmente bloqueado a qualquer usuário até que esse forneça credenciais válidas, verificadas em um banco de dados qualquer, para autenticação. Verificadas as credenciais, dinamicamente o *firewall* irá liberar o acesso para o cliente até que outra regra modifique essa ação (tempo de inatividade, desligamento da estação) [Fleck and Potter 2002].

Frequentemente, os ambientes de *hotspot* não oferecem segurança alguma, com exceção de usar conexão segura (HTTPS) para proteger as credenciais de ingresso, pois normalmente são utilizados em locais de acesso público, como por exemplo: hotéis,

aeroportos, centros de convenções, universidades, praças públicas. Desta forma, seu uso deve ser desencorajado para ambientes que trafegam transações ou dados sigilosos. No ambiente de estudo deste artigo, não é necessário um grande esforço na segurança, uma vez que se trata de uma rede de acesso a conteúdo exclusivamente acadêmico e não privado.

Um fato que encoraja a adoção desse mecanismo é a facilidade de acesso, pois não requer nenhum software ou configuração por parte do usuário. A autenticação por portal pode ocorrer de várias maneiras, entre elas: (a) *closed portal*, o qual pode ser utilizado para restringir o acesso a um determinado grupo de usuários com credenciais de usuário e senha, ou então exigir o pagamento para utilização por tempo determinado; (b) *open portal*, que simplesmente requer a aceitação de um termo de uso para liberação do acesso [Fleck and Potter 2002].

Assim, os passos necessários para o estabelecimento da conexão à rede sem fio pelo utilizador podem ser resumidos conforme a Figura 1: (1) usuário se conecta à rede sem fio disponível e recebe um endereço de rede automaticamente; (2) digita um endereço qualquer para navegação no *browser*. Neste momento, é solicitado as credenciais de autenticação; (3) a requisição é enviada ao *hotspot* de autenticação de forma segura (HTTPS); (4) o *hotspot* verifica em uma base de dados se as credenciais de usuário e senha conferem; (5) em caso positivo, autentica o usuário e libera o acesso à rede.

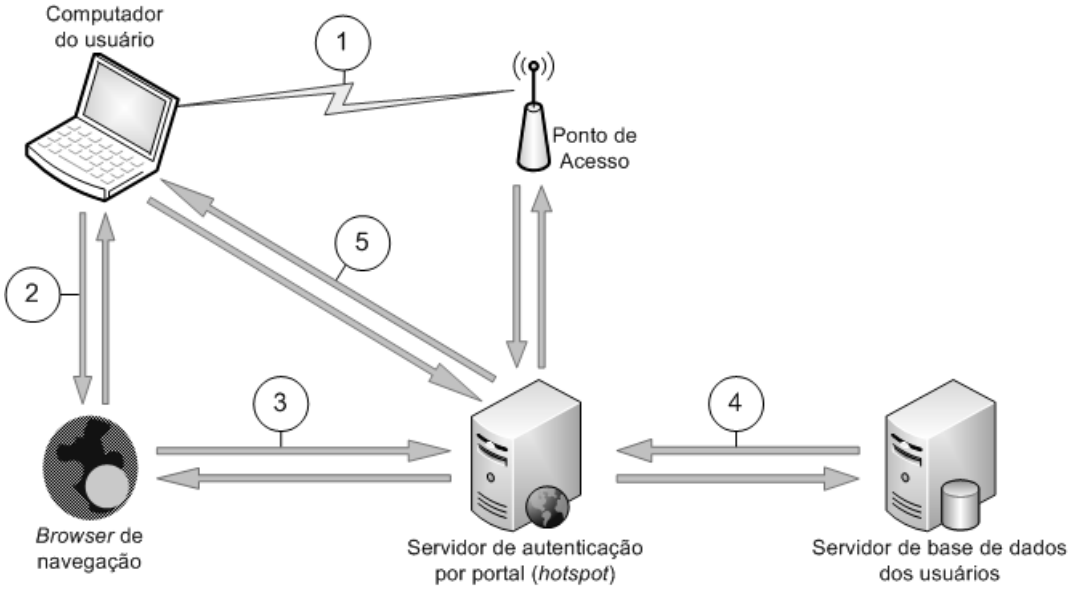

Figura 1. Fluxo do estabelecimento do acesso à rede sem fio

3.1.1. Sistema de autenticação (*hotspot*)

Para realizar a função de *hotspot* foi escolhido o CoovaChilli (Figura 2), um sistema *open source* de controle de acesso baseado no projeto ChilliSpot. O projeto ChilliSpot foi criado por Jens Jakobsen com o objetivo de autenticar usuários de redes sem fio, entretanto, seu desenvolvimento foi abandonado no ano de 2006. O desenvolvedor David Bird, que colaborava para o ChilliSpot, deu seqüência ao projeto, criando o

CoovaChilli, o qual se aproveitou de grande parte do projeto do ChilliSpot e ainda acrescentou diversos novos recursos/funcionalidades [Coovachilli 2008]. Esse foi o principal motivo da escolha por esse sistema.

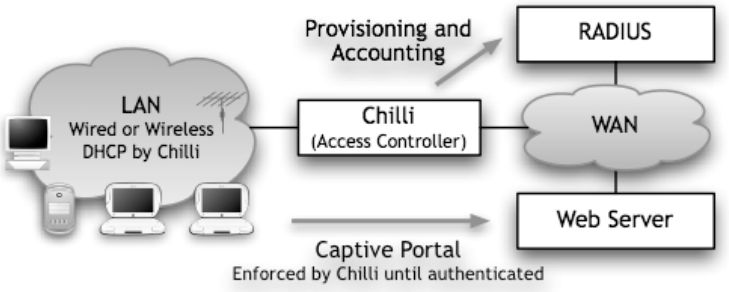

Figura 2. Estrutura do CoovaChilli

Devido ao fato do CoovaChilli rodar no sistema operacional Linux, escolheu-se a distribuição Slackware, pelo fato de ser a distribuição Linux mais antiga em atividade, comprovando, portanto, sua estabilidade, robustez e eficiência.

Para as tarefas de autenticação, autorização e contabilização dos usuários foi utilizado o FreeRADIUS, que é um dos softwares *open source* mais conhecidos e utilizados para a implementação do RADIUS, o qual é utilizado para disponibilizar acesso a redes com autenticação (comparação do nome de usuário e senha com a base de usuários), autorização (após a autenticação, determina se aceita ou não a solicitação) e contabilização (coleta informações de acessos e uso dos recursos) [Sanches 2005].

Para armazenamento das credenciais dos usuários e configurações do FreeRADIUS foi adotado o MySQL, que é um sistema gerenciador de banco de dados, também *open source*, que utiliza a linguagem SQL (*Structured Query Language*).

Além disso, foi necessária a instalação de um servidor de páginas, utilizado pelo CoovaChilli para efetuar a autenticação dos clientes. Para isso, optou-se pelo Apache, principalmente devido aos seus recursos e suporte a execução de scripts CGI (*Common Gateway Interface*) e autenticação SSL (*Secure Sockets Layer*).

4. Validação do alcance e *roaming* da rede

Para testar e validar os 28 pontos de acesso distribuídos pelo campus, foi utilizado a ferramenta NetStumbler, que é um dos mais conhecidos utilitários para detecção de redes sem fio, talvez por ser uma das primeiras ferramentas disponíveis para essa função. Além disso, gera gráficos da qualidade do sinal da rede sem fio, auxiliando no entendimento e identificação de problemas. Entretanto, somente funciona nos sistemas operacionais Windows 98/Me, 2000 e XP [Engst and Fleishman 2005; Duarte 2003]. Para o sistema operacional Linux recomenda-se a utilização da ferramenta Kismet, a qual possui função semelhante.

O NetStumber, além de identificar as redes disponíveis, informa o SSID, a qualidade do sinal através de cores (verde – excelente, verde claro – média, amarelo – boa, laranja – ruim), o canal e a existência ou não de criptografia dos dados de cada ponto de acesso detectado [Andrade 2004].

Com o auxílio dessa ferramenta, pode-se perceber que a distribuição dos pontos de acesso mostrou-se muito eficiente, pois em grande parte dos blocos a conexão à rede sem fio pode ocorrer em mais de um ponto de acesso. Isso significa dizer que, caso ocorram problemas com algum ponto de acesso, mesmo assim o serviço continuará a ser oferecido no mesmo local, pelos pontos de acesso adjacentes. Como exemplo dessa situação, pode-se citar o Auditório do campus (Figura 3), onde seis pontos de acesso foram detectados com qualidade do sinal excelente e, outros tantos com qualidade variando entre média, boa ou ruim.

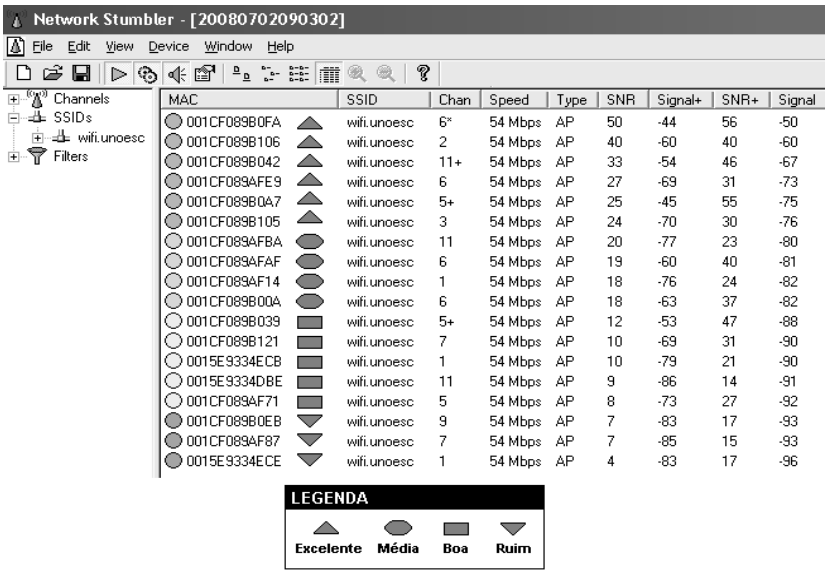

Figura 3. Detecção dos pontos de acesso da rede sem fios no Auditório

Já que em alguns locais (principalmente em áreas mais abertas) o número de pontos instalados superou o indicado pela norma IEEE 802.11g para uma mesma área, foi habilitada a opção "*Auto Channel Scan*" nos pontos de acesso. Desta forma, o próprio ponto de acesso irá procurar o melhor canal disponível, a fim de evitar interferências e melhorar a qualidade da rede.

5. Conclusão e Considerações Finais

As redes sem fio vêm apresentando um amplo crescimento, relacionado principalmente com a queda dos preços dos dispositivos, crescimento de aplicações para a Internet e facilidade de implementação deste tipo de rede.

Embora a autenticação por IEEE 802.1x forneça um nível de segurança superior, a instalação de um sistema de autenticação por portal, também conhecido como *hotspot*, oferece facilidades aos usuários finais, já que não exige dos utilizadores quaisquer conhecimentos de configuração ou solicitação de apoio técnico para a obtenção da permissão de acesso.

Visto que a autenticação é feita através de um sistema de *hotspot*, ao invés da autenticação por 802.1x ou ainda fazendo uso de criptografia WEP ou WPA/WPA2, qualquer ponto de acesso que opere na freqüência desejada irá funcionar corretamente. Entretanto, recomenda-se fortemente que sejam adquiridos pontos de acesso com

suporte à criptografia WPA/WPA2, autenticação 802.1x e suporte ao protocolo 802.1q (VLAN) e Multi-SSID, visando implementações de segurança futuras ou ainda a habilitação de mais de um tipo de autenticação na mesma área de cobertura.

Referências

Andrade, L. P. (2004), "Análise das vulnerabilidades de segurança existentes nas redes locais sem fio: um estudo de caso do projeto wlaca", Universidade Federal do Pará, Belém, http://www.lprad.ufpa.br/~margalho/wdeec/tcc.pdf, 15 abril 2008.

Carrion, D. (2005), "Avaliação de protocolos de autenticação em redes sem fio", Universidade Federal do Rio de Janeiro, Rio de Janeiro, http://www.ravel.ufrj.br/arquivosPublicacoes/tese_demetrio.pdf, 23 abril 2008.

Coovachilli (2008), "Página do projeto", http://coova.org/wiki/index.php/CoovaChilli, 08 maio 2008.

Duarte, L. O. (2003), "Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x", Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, http://www.acmesecurity.org/hp_ng/files/testes_monografias/acme–monografia–Wireless–2003–LOD.pdf, 15 abril 2008.

Edney, J. and Arbaugh, W. A. (2003), "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley.

Engst, A. and Fleishman, G. (2005), "Kit do iniciante em redes sem fio: o guia prático sobre redes Wi-Fi para Windows e Macintosh", Pearson Makron Books, São Paulo.

Fleck, B. and Potter, B. (2002), "802.11 Security", O'Reilly, 1th edition.

Gast, M. (2002), "802.11 Wireless Networks: The Definitive Guide", O'Reilly, 1th edition.

Grünewald, M. A. (2005), "Redes sem fio – Tecnologia, Segurança e Usabilidade", Faculdade de Informática e Administração Paulista, São Paulo.

Kurose, J. F. and Ross, K. W. (2007), "Redes de computadores e a internet: uma abordagem top-down", Pearson Addison Wesley, 3.ed., São Paulo.

Miyano Neto, R. (2004), "A evolução dos mecanismos de segurança para redes sem fio 802.11", Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, http://www-di.inf.pucrio.br/~endler/courses/Mobile/Monografias/04/Miyano-Mono.pdf, 21 abril 2008.

Ribas, J. C. (2002), "Perfil de link sem fio em ambiente aberto: avaliação através de medições", Universidade Federal de Santa Catarina, Florianópolis.

Rosnam, P. and Leary, J. (2003), "Wireless LAN Fundamentals", Cisco Press, 1th edition.

Sanches, C. A. (2005), "Projetando redes WLAN: conceitos e práticas", Editora Érica, Rio de Janeiro.