

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA – *CAMPUS* GUAÍBA

CURSO DE SISTEMAS DE INFORMAÇÃO



VLAN EM REDES SEM FIO
TRABALHO DE CONCLUSÃO DE CURSO I

EDUARDO DA CUNHA KAMINSKI

André Peres
Orientador

Guáiba, dezembro de 2009.

DADOS DE IDENTIFICAÇÃO

Acadêmico: Eduardo da Cunha Kaminski

E-mail: edukaminski@gmail.com

Professor Orientador: André Peres

E-mail: peres@guaiba.ulbra.tche.br

Título do Projeto: VLAN em Redes Sem fio

Período de realização: 31/08/2009 à 30/11/2009

SUMÁRIO

1	INTRODUÇÃO.....	4
2	REFERENCIAL TEORICO	6
2.1	Redes sem fio.....	6
2.2	Topologia das redes sem fio.....	7
2.2.1	<i>IBSS (AD-HOC)</i>.....	7
2.2.2	<i>BSS (Basic Service Set)</i>.....	8
2.2.3	<i>ESS (Extended Service Set)</i>	9
2.3	Segurança em redes sem fio.....	10
2.3.1	<i>Confidencialidade da Informação</i>.....	11
2.3.2	<i>Autenticidade da Informação</i>.....	12
2.4	Padrão IEEE 802.1x (<i>Port Based Network Access Control</i>).....	13
2.5	Redes Locais Virtuais – VLAN	17
3	MODELO PROPOSTO	19
4	CENÁRIO DE TESTES.....	25
5	CONCLUSÃO	28
	BIBLIOGRAFIA	29

1 INTRODUÇÃO

A tecnologia denominada rede sem fio - WLAN (*Wireless Local Network Access*) utiliza frequência de rádio para trocar informações digitais, está revolucionando o universo da computação. As redes sem fio estão dispostas hoje nos mais diversos locais como: casas, escolas, hotéis, aeroportos, empresas de grande, médio e pequeno porte. Com a mobilidade e o baixo custo para sua implementação, muitos usuários estão se beneficiando e utilizando esta tecnologia.

Os benefícios que as redes sem fio proporcionam como a mobilidade e a flexibilidade é indiscutivelmente um ganho tecnológico. Poder acessar recursos compartilhados tais como arquivos, impressoras, internet, etc. sem a necessidade de cabos é uma melhoria significativa. Entretanto a segurança e o gerenciamento necessitam estar paralelamente ligadas aos benefícios que esta tecnologia oferece.

Com a transmissão de dados através de frequência de rádio, a comunicação não está mais limitada aos cabos. Antes disto a comunicação era limitada a utilização de cabos, havia a necessidade conectar todos os dispositivos da rede ao ponto central da rede, ou seja, a mobilidade dos usuários estava limitara ao alcance dos cabos. Alguns problemas de comunicação se dão pelo fato dos cabos sofrerem com desgaste físico.

As redes sem fio são padronizadas através do órgão IEEE (*Institute of Electrical and Electronics Engineers*) que estabelece a norma IEEE 802.11 para o desenvolvimento e operação das redes sem fio.

Com a crescente propagação de redes sem fio nas instituições cria-se a necessidade de incrementar o nível de gerenciamento destas redes, um dos desafios em soluções de rede sem fio é garantir a segurança. Preocupações que profissionais de TI deveriam ter ao projetar uma rede sem fio, nem sempre estão sendo considerada, é necessário analisar os riscos e considerar que as informações poderão estar ameaças. Dos principais pontos que deveriam ser considerados estão a confiabilidade e autenticidade da informação.

Para garantir a confidencialidade da informação alguns mecanismos podem ser considerados. O WEP (*Wired Equivalent Privacy*) criado em 1999, WPA (*Wi-Fi Protected Access*) e o WPA2 são exemplo destes mecanismos que podem ser utilizados para proteger o canal de comunicação.

Mecanismos que fornecem a autenticidade da informação são utilizados para identificar qual usuário ou equipamento está transmitindo ou acessando determinada informação. Mecanismos como OSA (*Open System Authentication*), SKA (*Shared Key Authentication*) e o protocolo 802.1x fornecem esta proteção. Para aplicar em uma rede o 802.1x é necessário um servidor de autenticação como componente adicional.

Embora seja de extrema importância prover em uma rede sem fio a confiabilidade e a autenticidade da informação, é igualmente importante é sua segmentação destas redes. As redes sem fios podem ser vistas como um segmento não confiável, isto devido a não utilização em muitos casos de mecanismos de controle de acesso, desta forma qualquer usuário terá acesso sem controle algum. Segmentar uma rede é subdividi-la em grupos, estes grupos são denominados sub-redes.

Dado o exposto acima, para prover segurança a uma rede é necessária a integração de algumas tecnologias. Ao fim deste trabalho a integração destas tecnologias será apresentada.

2 REFERENCIAL TEORICO

A fundamentação teórica está descrita em cinco, partes distintas, onde está descrita a definição sobre redes sem fio, tipos de redes e topologias, segurança em rede sem fio, o padrão 802.1x que será utilizado neste trabalho para autenticação e autorização de acesso e as redes VLAN que são utilizadas para segregar redes.

Depois de descrito todas as tecnologias a serem utilizadas neste trabalho, são apresentadas o modelo proposto e o cenário de testes.

2.1 Redes sem fio

A transmissão do sinal através de frequência de radio que se difunde pelo ar é controlada individualmente de acordo com os requisitos governamentais de cada país, devido à existência de outros serviços que também utilizam frequências de rádio para comunicação. Entretanto algumas faixas definidas pela ISM (*Industrial, Scientific and Medical*) não necessitam de aprovações diretas do governo e podem ser utilizadas. Os intervalos definidos pela ISM são 902 MHz a 982 MHz; 2,4 GHz a 2,485 GHz e 5,15 GHz a 5,825 GHz que podem sofrer variações dependendo do país.

O desenvolvimento é controlado pelo padrão 802.11 que estabelece as normas para criação e para o uso de redes sem fio. Após aproximadamente sete anos de pesquisa o padrão 802.11 foi ratificado em 1997. Por utilizar frequência de radio a IEEE definiu o intervalo entre 2,4GHz e 2,485Ghz com velocidades de 1 Mbps e 2 Mbps.

O padrão 802.11b foi ratificado em 1999. Sua velocidade de transmissão pode chegar a 11 Mbps, também opera nas velocidades de 1 Mbps, 2 Mbps e 5,5 Mbps utilizando o mesmo intervalo de frequência do 802.11. O 802.11b cobre uma área de até 400 metros em um ambiente aberto e pode chegar até 50 metros em lugares fechados, quando maior a distancia menor a velocidade de transmissão.

A conclusão do desenvolvimento do padrão 802.11a ocorreu no final de 1999, o padrão 802.11b foi concluído alguns meses antes. O 802.11a opera nas seguintes velocidades: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps tendo uma alcance de até 50 metros. Utiliza a frequência de radio de 5 GHz, que tem algumas restrições quanto a sua operação em alguns países.

Operando em velocidade de até 54 Mbps o padrão 802.11g foi ratificado em 2003. Utiliza frequência de radio de 2,4 GHz compatível com o padrão 802.11b, ou seja, um equipamento com padrão 802.11b pode trocar informações com outro equipamento com padrão 802.11g, limitando apenas a velocidade máxima de 11 Mbps do padrão 802.11b.

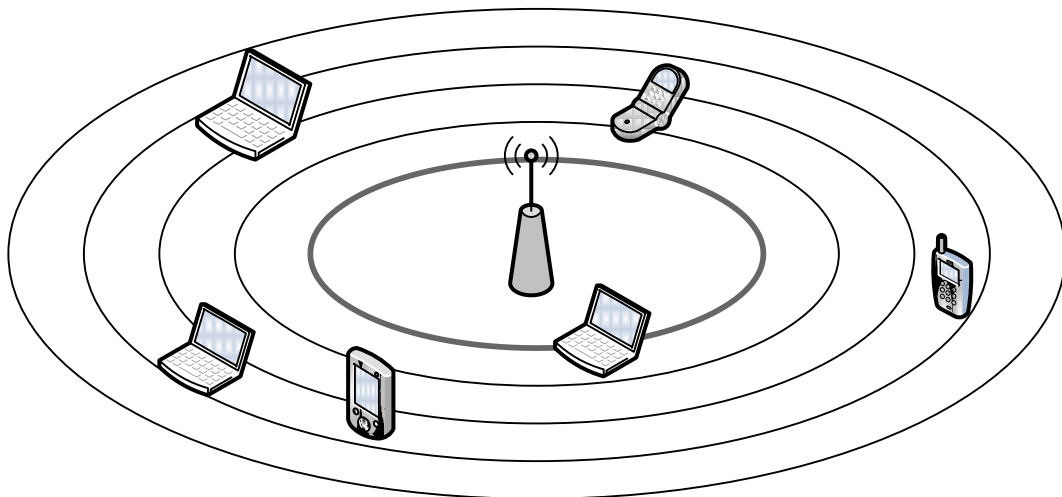


Figura 1: transmissão de dados sem fio.

2.2 Topologia das redes sem fio

2.2.1 IBSS (AD-HOC)

A rede IBSS (*Independent Basic Service Set*) é definida através das conexões ponto-a-ponto, ou seja, equipamentos trocam informações diretamente entre-si sem a necessidade de um dispositivo que centraliza o acesso. Por ser uma conexão ponto-a-ponto está tecnologia também se refere à topologia AD-HOC.

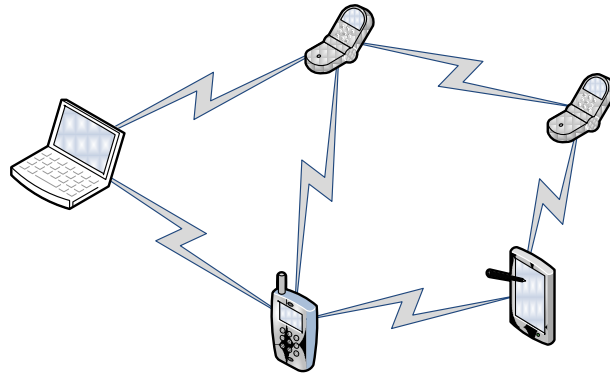


Figura 2: Topologia AD-HOC

2.2.2 BSS (*Basic Service Set*)

Uma rede BSS é definida pela utilização de equipamentos, que possam emitir e capturar sinais através da frequência de rádios, chamado de pontos de acesso (AP ou *Access Point*) para intercomunicação dos dispositivos móveis. O ponto de acesso tem a função criar uma rede sem fio, para identificação de uma rede um SSID (*Service Set Identifier*) é atribuído ao ponto de acesso. Desta forma os dispositivos móveis compatíveis com as normas citadas, irão criar um canal chamado BSS. Apenas após a criação do canal BSS um computador pode trocar informações através desta rede. Conforme descrito acima se sabe da existência de limitações da utilização de padrões diferentes em uma mesma rede sem fio.

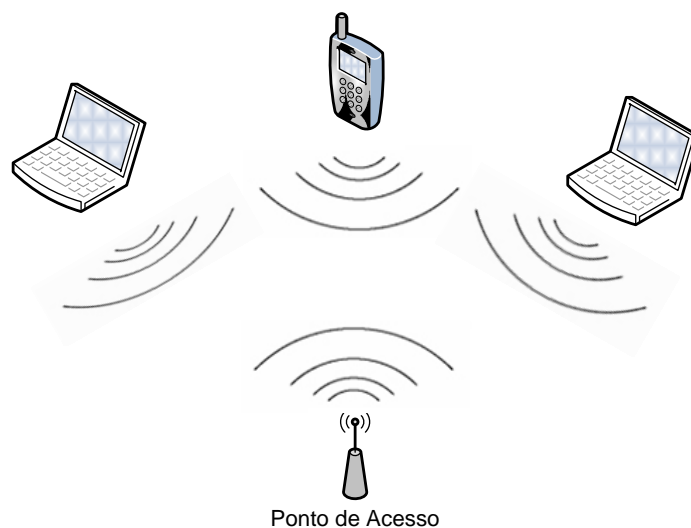


Figura 3: Basic Service Set

Existem algumas limitações físicas quanto à distância entre o dispositivo móvel e o ponto de acesso, a velocidade de conexão de um dispositivo móvel ao um ponto de acesso é definida pela qualidade do sinal.

Conforme visualizado na figura 3, quanto maior a distância entre o ponto de acesso menor será a qualidade do sinal e conseqüentemente da velocidade podendo esta ser nula.

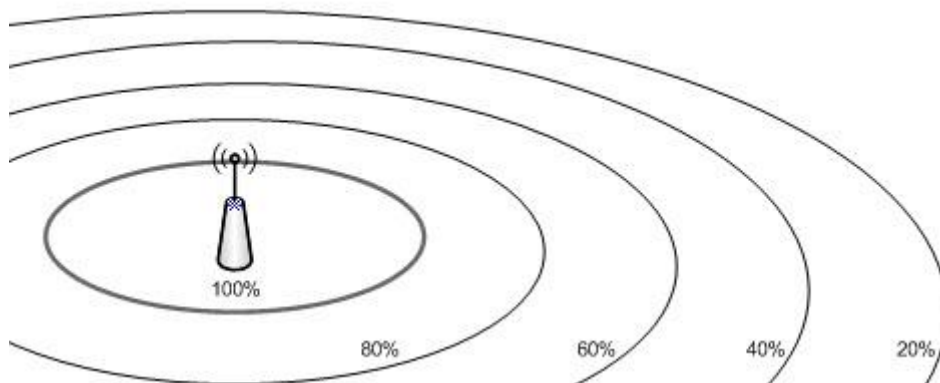


Figura 4: Qualidade do sinal

Outra limitação por uso do ar como um meio de transmissão são os obstáculos entre o ponto de acesso e o dispositivo móvel, por exemplo, as paredes que separam um setor de outro em uma empresa, serão obstáculos que irão interferir na qualidade do sinal.

2.2.3 ESS (*Extended Service Set*)

Redes BBS fornecem suporte para pequenas localidades como escritórios, pequenas empresas e casas. Esta rede não tem capacidade de fornecer uma cobertura para grandes áreas, limitada a distância disposta pela qualidade do sinal. Esta limitação pode ser suprimida com a utilização de outros pontos de acesso distribuídos utilizando o mesmo SSID, para isto o 802.11 permite que haja ligação entre diversos BBS através da core (espinha dorsal) destas grandes redes assim criando uma rede ESS.

A figura 5 ilustra esta topologia a ligação de duas redes BBS, a rede A criando o BBS-A e da rede B criando o BBS-B. Esta ligação ocorre através de cabos ligados

a um hub ou switch, criando uma ligação física e lógica entre as redes A e B. Desta forma os usuários podem compartilhar dados independente da rede em que estejam conectados, como por exemplo, a estação B compartilhando arquivos e um computador ligado a rede ethernet compartilhando uma impressora. Os usuários também poderão se locomover entre às redes sem fio sem perda de cobertura, assim como ilustra a estação A, desde que seja no perímetro de alcance dos pontos de acesso.

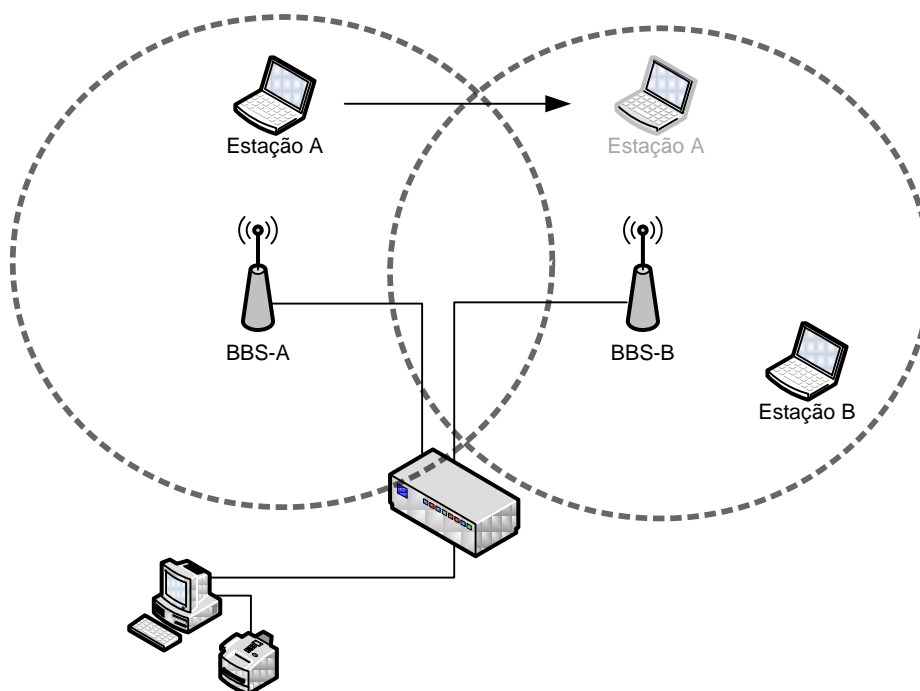


Figura 5 – A união duas BSS cria uma ESS

2.3 Segurança em redes sem fio

Prover segurança em uma rede sem fios é a garantia que os usuários não terão os dados transmitidos alterados e/ou capturados para outros fins. Informações sensíveis que precisam ter sua segurança reforçada. Abaixo estará descrito os mecanismos estudados que fornecem algum tipo de confiabilidade e autenticidade da informação em uma rede sem fio.

2.3.1 Confidencialidade da Informação

O primeiro protocolo de segurança para rede sem fio, o WEP (*Wired Equivalent Privacy*) é parte do padrão IEEE 802.11 e foi introduzido para agregar confiabilidade na informação trocada durante a comunicação entre os dispositivos sem fio e é suportado por todos os equipamentos 802.11a/b/g.

O WEP usa uma chave compartilhada entre os dispositivos de rede, ponto de acesso e clientes. A chave compartilhada é estática podendo ter 40 bits, 64 bits ou 128 bits, desta forma a chave é utilizada para codificar e para decifrar os dados. Somente terá acesso ao meio de comunicação sem fio aquele dispositivo que conter a chave compartilhada.

O desenvolvimento do WEP considerou apenas as medidas necessárias para proteger uma rede sem fio considerando as necessidades de uma rede local onde os dispositivos de rede estão interligados por cabos. Assim com a evolução e disseminação da tecnologia sem fio, o protocolo WEP acabou apresentando falhas e se tornando vulnerável a ataques.

WEP é vulnerável devido ao tamanho limitado das chaves e por serem estáticas. A natureza estática das chaves compartilhadas torna sério o problema da troca das chaves das estações, pois se a chave for alterada no ponto de acesso ela deverá ser alterada também em todos os dispositivos móveis que acessam a rede sem fio. Como consequência, muitos administradores de redes utilizam a mesma chave por semanas, meses e até anos. Criando oportunidades para que um invasor utilize ferramentas para descobrir a chave WEP em uso e assim poder ter acesso à rede. Mesmo com as falhas e vulnerabilidades, conter segurança mesmo que limitada é melhor do que não ter.

Diante dos problemas apresentados pelo WEP, em 2003 foi disponibilizada outra solução o WPA (*Wi-Fi Protected Access*) que inclui mecanismos de protocolo de integridade de chave temporal chamado de TKIP (*Temporal Key Integrity Protocol*), as mesmas são alteradas automaticamente com o passar do tempo, reduzindo a possibilidade de uma sessão ser quebrada.

Em junho de 2004, o IEEE ratificou o padrão 802.11i também conhecido como WPA2, que suporta o padrão de criptografia avançada AES (*Advanced Encryption Standard*) e características de gerenciamento de chaves com diversos tamanhos 128, 192 e 256 bits.

O WPA, assim como o WP2, provê um esquema de criptografia significativamente mais forte e pode usar diversos métodos como uma chave privada compartilhada, chaves únicas designadas para cada usuário ou mesmo certificados SSL para autenticar tanto o cliente como o ponto de acesso. As credenciais de autenticação são verificadas com o uso do padrão 802.1x, que será citado no item 2.4 deste trabalho. O WPA também pode ser usado no modo PSK (*Pre-Shared Key*). Nesse modo, há a presença de uma chave pré-determinada e a troca da chave é realizada pelo próprio ponto de acesso.

Entretanto o WPA requer pontos de acesso com hardware relativamente recente e o firmware atualizado em todos os dispositivos sem fio.

2.3.2 Autenticidade da Informação

O padrão IEEE 802.11 define dois métodos que os dispositivos sem fio se autenticam antes da comunicação iniciar. Estes dois métodos são: Autenticação de Sistema Aberto (*OSA – Open System Authentication*) e Autenticação de Chave Compartilhada (*SKA – Shared-Key Authentication*).

O método OSA não necessita que o dispositivo sem fio envie ao ponto de acesso uma chave para ter acesso à rede sem fio.

Quando o dispositivo solicitar acesso à rede é enviado um pedido de autenticação para o ponto de acesso mais próximo. O pedido de autenticação contém o tipo de autenticação que pretende utilizar (zero no caso de OSA). O ponto de acesso responde a solicitação de autenticação não requerendo nenhum tipo de desafio para conceder o acesso, assim, o dispositivo se conecta a rede.

Neste caso as redes sem fio usando OSA transmitem tudo em texto claro onde nenhuma criptografia é necessária. Neste tipo de autenticação, os dispositivos sem fio só precisam identificar o SSID da rede para ter acesso autorizado. É possível limitar em alguns produtos o acesso através do endereço MAC do dispositivo de acesso, apesar de existir um filtro a autenticação será considerada como OSA.

SKA é autenticação de chave compartilhada significa que alguma forma de autenticação ocorre antes de comunicações de rede sem fio iniciar, ou seja, o dispositivo sem fio deve ser configurado com a chave de criptografia necessária para que o ponto de acesso reconheça a autenticação e conceda acesso. O padrão 802.11 define uma técnica para SKA o WEP.

É importante notar que o ponto de acesso pode impor o uso de autenticação. Se um dispositivo de acesso envia um pedido de autenticação informando que o método que será utilizado é o OSA, o ponto de acesso pode negar o acesso à rede, isso se o ponto de acesso estiver configurado para aplicar o método SKA.

Quando um dispositivo solicita acesso à rede, ele deve enviar uma solicitação de autenticação para o ponto de acesso, que contém o tipo de autenticação que deseja utilizar (um no caso de SKA). Ao receber este pedido, o ponto de acesso envia uma resposta de autenticação para o dispositivo. Esta resposta contém um texto desafio. Quando a dispositivo recebe o desafio, ele o criptografa usando a chave WEP compartilhada e gera uma resposta ao desafio. Ao receber a resposta, o ponto de acesso descriptografa a resposta usando a chave WEP compartilhada. O ponto de acesso compara a mensagem decifrada com o desafio que enviou para o dispositivo. Se estas são as mesmas, o ponto de acesso conclui que o dispositivo que pretendem aderir à rede é um dispositivo que conhece a chave secreta e, portanto, o ponto de acesso autentica o dispositivo para se conectar a rede.

2.4 Padrão IEEE 802.1x (*Port Based Network Access Control*)

A fim de oferecer um mecanismo de autenticação mais eficiente o padrão 802.1x foi definido. A autenticação por 802.1x, utilizada em rede com fio (802.3) e redes sem fio (802.11), impede que usuários e computadores não autenticados e

não autorizados se conectem a rede. Este padrão fornece controle de acesso a redes de computadores baseado em portas (baseada em "porta" significa que a rede terá um único ponto de autenticação), ou seja, um dispositivo sem fio deve ser autenticado antes que ele possa ter acesso a outros recursos da LAN.

Para que seja possível autenticar usuários remotos é necessário um servidor capaz de realizar esta atividade. Poder gerenciar um banco de dados único de usuários, que permite a autenticação (verificação as credenciais de usuário), bem como centralizar as informações de configuração detalhando o tipo de serviço que será disponível, o servidor de autenticação RADIUS (*Remote Authentication Dial-In User Service*), realiza esta atividade.

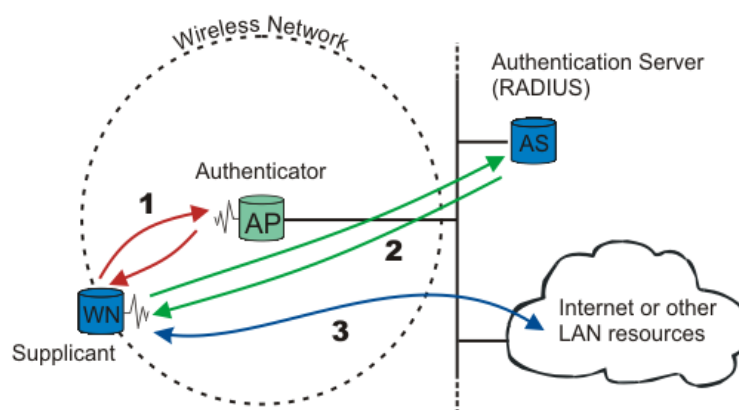


Figura 6: 802.1x (Controle de acesso baseado em porta)

- 1) Quando o suplicante (dispositivo que está solicitando a autenticação, representado pela sigla WN na figura 6) solicita acesso a um recurso da rede ao autenticador (o ponto de acesso representado na figura 6 pela sigla AP), o tráfego através do protocolo de autenticação é permitido antes do suplicante ser autenticado, pois a porta de acesso ainda está fechada para envio das credenciais de acesso.

O dispositivo sem fio que solicita autenticação é freqüentemente chamado de suplicante, embora seja correto dizer que o dispositivo sem fio contém um suplicante. O suplicante é responsável por responder aos dados do autenticador que irá requerer estabelecer as suas credenciais.

- 2) Depois que as credenciais de acesso tenham sido enviada, o processo de autenticação começa. O protocolo usado entre o suplicante e o autenticador é o EAP (*Extensible Authentication Protocol*) que encapsula a informação e encaminha ao servidor de autenticação. Durante a autenticação, o autenticador apenas retransmite pacotes entre o suplicante e o servidor de autenticação. Ao terminar o processo de autenticação, o servidor de autenticação envia uma mensagem de sucesso (ou fracasso, se a autenticação falhou). O autenticador então abre a porta para o suplicante.

Uma característica do servidor RADIUS o NAS (*Network Access Server*) descrito pelo padrão 802.1x como autenticador é o ponto de acesso que opera como um cliente RADIUS e é responsável por passar informações para servidores RADIUS.

Servidor RADIUS é responsável por receber estas solicitações de conexão, e retornar todas as informações de configuração necessárias para o cliente disponibilizando ou não o serviço para o usuário.

Transações entre o dispositivo e o servidor RADIUS são autenticadas através da utilização de um segredo compartilhado, que nunca é enviada pela rede, pois é pré-configurada no dispositivo. Além disso, as credenciais dos usuários são enviadas criptografadas entre o cliente e o servidor RADIUS, para eliminar a possibilidade de que alguém de olho em uma rede não segura pode capturar estas credenciais.

- 3) Após uma autenticação bem-sucedida, é concedido o acesso a outros recursos da LAN / Internet ao suplicante.

Mecanismos de autenticação flexível, o servidor RADIUS pode apoiar uma variedade de métodos para autenticar um usuário.

O EAP é um padrão IETF (*Internet Engineering Taskforce*) para efetuar a autenticação. Ele pode ser usado com uma variedade de diferentes métodos de autenticação com base em senhas, certificados de chaves públicas ou outras credenciais. A transmissão consiste em solicitações de informações de autenticação

feitas pelo autenticador e as respostas enviadas pelo suplicante. Os principais métodos que podem ser utilizados pelo EAP, em redes sem fio, são:

- EAP-TLS (*Extensible Authentication Protocol Transport Layer Security*) utiliza certificados de chave pública para autenticar tanto o dispositivo sem fio como o servidor de autenticação estabelecendo uma sessão de TLS criptografado entre eles.
- PEAP utiliza o método de autenticação em dois estágios. O primeiro estabelece uma sessão TLS para o servidor e permite que o cliente autentique o servidor usando o certificado digital do servidor. O segundo requer o segundo método de encapsulamento do EAP na sessão PEAP para autenticar o dispositivo ao servidor de autenticação. Isso permite que o PEAP use uma variedade de métodos de autenticação de clientes, incluindo senhas com o protocolo MS-CHAPv2 e certificados usando o EAP-TLS encapsulado no PEAP.
- TTLS consistem em um protocolo em dois estágios similar ao PEAP que usa sessão TLS para proteger uma autenticação de cliente encapsulado. O método de encapsulamento EAP, o TTLS também pode usar versões não EAP para protocolos de autenticação como o CHAP e MSCHAP.
- LEAP consiste em um método EAP proprietário desenvolvido pela Cisco, que usa senhas para autenticar clientes. Embora popular o LEAP só funcionasse com hardwares e softwares da Cisco e de outros poucos fornecedores.
- EAP-MD5 consiste apenas na autenticação do cliente sem a geração de chave dinâmica, apenas utilizam chaves estáticas estando aberto a ataques de dicionários.

As credenciais de acesso do suplicante são pré-configuradas sendo necessária a criação dos dados de acesso ao meio sem fio.

2.5 Redes Locais Virtuais – VLAN

Redes locais virtuais conhecidas pela sigla VLAN (*Virtual Local Access Network*) é a segmentação de redes locais. A segmentação de uma rede é subdividir uma rede local em dois ou mais grupos, estes grupos estarão utilizando o mesmo meio físico para transmissão dos dados, entretanto logicamente estarão separadas. A segmentação da rede é realizada na camada de enlace do modelo OSI.

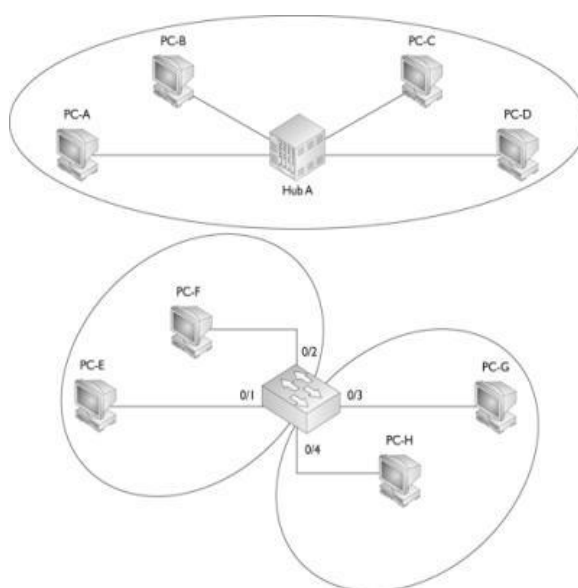


Figura 7: Único segmento e VLAN

Para facilitar o entendimento, na parte superior da figura 7 exibe o exemplo de uma rede simples, onde cada dispositivo estão no mesmo domínio de broadcast e colisão, ou seja, todos os computadores irão receber os pacotes transmitidos no meio, entretanto somente o computador de destino irá aceitar o recebimento, os demais irão descartar os pacotes, isto se, não for um atacante capturando todos os pacotes transmitidos na rede. Neste exemplo, um hub está fornecendo a conectividade.

Já na parte inferior da figura 7 é exibido um exemplo de um *switch* com quatro computadores conectados a ele. A diferença importante entre o hub e o *switch* é que todos os dispositivos conectados ao hub estão no mesmo domínio de colisão, enquanto que no exemplo *switch*, cada porta do *switch* é um domínio de colisão. Por padrão, todas as portas em um *switch* estão no mesmo domínio de broadcast. Neste

exemplo, contudo, os computadores PC-E e PC-F estão em um domínio de broadcast (VLAN_1) e PC-H e PC-G e estão em outro domínio de broadcast (VLAN_2), ou seja, o segmento está dividido em 2 VLANs.

Há algumas formas de se segmentar uma rede, as seguintes VLAN podem ser criadas:

- 1) Uma VLAN de nível 1 baseada em porta (*Port-Based VLAN*) define uma rede virtual em função das portas de conexão no comutador (*switch*);
- 2) Uma VLAN de nível 2 (VLAN MAC, *MAC Address-Based VLAN*) consiste em definir uma rede virtual em função dos endereços MAC dos dispositivos de acesso. Este tipo de VLAN é flexível que a VLAN por porta, porque a rede é independente da localização da estação, redes baseadas em MAC são configuradas no *switch*;
- 3) Uma VLAN de nível 3: distinguem-se vários tipos de VLAN de nível 3: A VLAN por subrede (*Network Address-Based VLAN*) associa subredes de acordo com o endereço IP.
- 4) O VLAN por protocolo (*Protocol-Based VLAN*) permite criar uma rede virtual por tipo de protocolo (por exemplo, TCP/IP, IPX, AppleTalk, etc.), agrupando assim todas as máquinas que utilizam o mesmo protocolo numa mesma rede.

Alguns dos benefícios de se criar VLANs estão:

A segurança é incrementada em segregar grupos de usuários. Cada grupo tem acesso apenas aos recursos que são necessários para o desenvolvimento de suas atividades e responsabilidades dentro da organização.

A gestão da rede é ampliada devido ao controle que o gestor terá sobre cada grupo de usuários, permitindo que as alterações a estes grupos, funções e membros não necessitam quaisquer alterações à topologia física da rede.

3 MODELO PROPOSTO

A tecnologia sem fio em redes de computadores não é mais uma novidade. O grande desafio para os usuários, e principalmente para os profissionais de TI que gerenciam estas redes, é garantir segurança às informações que estão trafegando no “ar”. O objetivo deste trabalho é auxiliar os profissionais de TI a agregar segurança e gerenciamento em redes sem fio.

Existem mecanismos de autenticação e confiabilidade que ao serem utilizados agregam segurança às informações transmitida. Além de agregar segurança no canal de comunicação, este trabalho também tem o objetivo de segregar redes sem fio, desta forma delimitando logicamente o acesso dos usuários.

Agregar segurança em informações que estão sendo transmitidas pelo ar, onde qualquer dispositivo tem a capacidade de capturar todos os pacotes da transmissão, é uma tarefa que requer análise do ambiente em que está sendo administrado e também dos usuários que irão utilizar o meio. Para isto este trabalho irá propor uma análise no acesso há rede sem fio da universidade, onde professores, alunos e visitantes utilizam uma rede sem fio com método de autenticação OSA, ou seja, qualquer usuário que tenha um dispositivo compatível com a tecnologia sem fio poderá acessar a rede.

Com a segmentação da rede, cada segmento define um novo domínio de *broadcast*, ou seja, um dispositivo irá receber apenas o tráfego de sua própria VLAN. Hoje na universidade as redes LAN nas salas do LABIN estão segmentadas através de VLAN tipo três, ou seja, utilizam sub-redes IP que definem qual VLAN os computadores estão. Este tipo de configuração é definido como VLAN estática, onde cada sala é uma sub-rede. A rede sem fio também está separada das demais redes sendo uma rede isolada, a figura 8 está um esboço da rede do LABIN, apenas três salas estão descritas no exemplo, as demais salas seguem a mesma topologia.

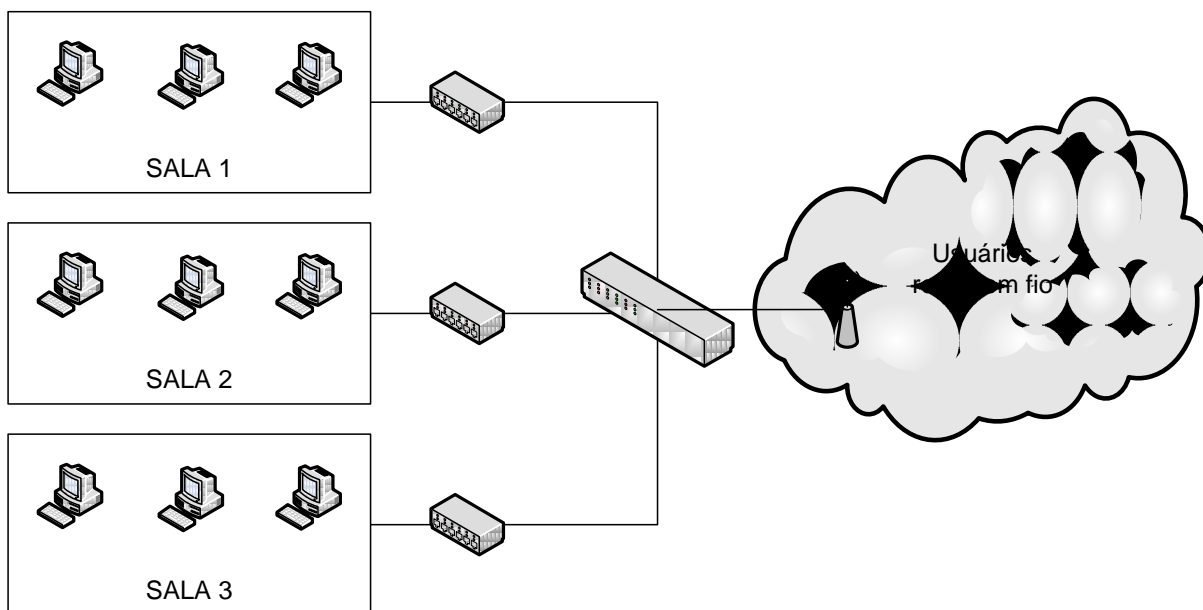


Figura 8: Rede Labin

Para a rede sem fio será aplicada VLANs dinâmicas. Com esta é possível atribuir automaticamente uma VLAN para um usuário de acordo com as informações do dispositivo, como seu endereço MAC, endereço IP, ou mesmo credenciais do usuário (um nome de usuário e grupo). Para isto será utilizado o padrão 802.1x, que irá fornecer a autenticação do acesso de a um ponto de acesso sem fio.

A primeira etapa é a definição da segmentação da rede sem fio de forma dinâmica. A rede sem fio será segmentada em três VLAN, ou seja, será necessário criar no mesmo ponto de acesso três SSID, contendo cada SSID uma configuração específica.

Ao ativar múltiplas VLANs em uma rede sem fio, onde vários SSIDs são criados, apenas um SSID pode gerar *broadcast*. Para isto será necessário definir um SSID como primário, todos os outros SSIDs como secundários e não irão gerar *broadcast*.

Os grupos que serão criados são:

SSID	Primário / Secundário	Descrição
PROFS	Secundário	Designada os professores universidade que necessitam ter acesso a dados sensíveis e informações acadêmicas.
ALUNOS	Secundário	Alunos da universidade, que precisam ter acesso às máquinas de pesquisa. Eles muitas vezes estão trabalhando de em grupos e necessitam que seus computadores possam trocar informação entre si.
ULBRA	Primário	Universidade recebe freqüentemente alunos de outros campi para trabalhos de pesquisa, estes alunos irão ser considerados visitantes.

Para cada SSID será atribuído um endereço de rede específico para que a segmentação lógica da rede seja aplicada. Caso os três SSID a ser criado, utilizarem o mesmo endereço de rede não estará definido uma VLAN.

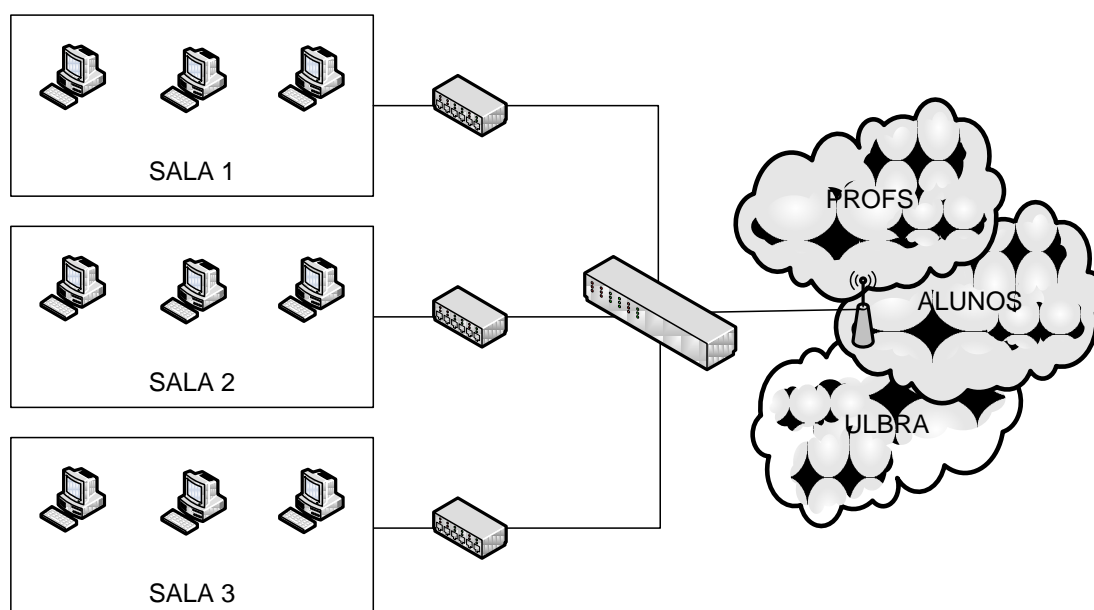


Figura 9: Proposta para rede sem fio do LABIN

Para que Multi-SSID sejam criadas em um ponto de acesso, é necessário que o equipamento suporte esta tecnologia. Alguns dos equipamentos são: O D-Link DWL-2100AP, Linksys WAP54GP, EliteConnect 2.4GHz 802.11g, HP ProCurve 10ag, Alcatel-Lucent OmniAccess AP125. Entretanto hoje o LABIN não tem um equipamento com esta funcionalidade.

Para isto será necessário emular um ponto de acesso utilizando servidor Linux em um computador com placa de rede sem fio. Um driver chamado Host AP é capaz de simular um ponto de acesso, entretanto o Host AP não suporta Mult-SSID, o que inviabiliza a sua utilização para a finalidade de criar VLANs.

Há uma distribuição Linux chamada ZeroShell que não necessita ser instalada no computador para funcionar, já que pode operar diretamente a partir do CD-ROM em que é distribuída ou diretamente de um driver USB. Os dados de configuração estão em um banco de dados, que pode ser armazenados em unidades de disco ou USB. Correções de falhas de segurança são disponibilizadas automaticamente através da internet e são instaladas na base de dados. Depois de iniciado e pré-configurado com endereçamento IP a sua administração pode ser realizada através da interface da Web. ZeroShell é uma distribuição Linux *open source*. A licença com a qual ele é distribuído é a GPL versão 2.

Entre as funcionalidades disponíveis nesta distribuição está o modulo de ponto de acesso permitindo a configuração com múltiplos SSID suportando VLAN, usando placas de rede sem baseada no *chipset Atheros*.

Apenas segregar a rede não irá garantir a confiabilidade e autenticidade do dado transmitido, a associação destas redes a métodos de segurança irá fornecer um canal de comunicação seguro.

A segunda etapa logo após a criação das VLANs será a configuração individual com controle de acesso usando o 802.1X. O beneficio desta configuração será que um usuário pode "saltar" de uma VLAN para outra, de acordo com o grupo que estiver associado. As credenciais de usuários e os grupos de acesso serão

armazenados no serviço de diretórios da Microsoft, conhecido como AD (*Active Directory*), este serviço já existe no LABIN.

Quando um usuário iniciar o acesso à LAN sem fios, o servidor RADIUS irá verificar em qual grupo este usuário está e atribuir a VLAN correspondente. Para controle de acesso através do padrão 802.1x é necessário considerar o servidor RADIUS, algumas hipóteses estão descritas abaixo:

O IAS (*Internet Authentication Service*) é a solução da Microsoft de um servidor RADIUS. Como um servidor RADIUS, o IAS executa autenticação centralizada, autorização e contabilidade para vários tipos de acesso à rede, incluindo a rede sem fio e privada virtual (VPN).

O NAP (*Network Access Protection*) é uma solução lançada pela Microsoft no sistema operacional Windows Server 2008 que controla o acesso a recursos de rede baseado na identidade do dispositivo ou usuário. O NAP permite que os administradores definam níveis de segurança de acesso à rede NAP inclui uma interface de programação de aplicativos (API) possibilita que desenvolvedores criem soluções adicionais limitação o acesso à rede ou de comunicação. Porém a plataforma NAP requer servidores executando o Windows Server 2008 e clientes que executam o Windows Vista, Windows Server 2008 ou Windows XP com *Service Pack 3*.

Baseado no software FreeRADIUS o ZeroShell implementa o servidor RADIUS suportando os métodos de autenticação do protocolo 802.1x através de uma distribuição *open source*.

A autenticação a ser utilizada está baseada em três métodos fornecidos pelo padrão 802.1x. Serão utilizados para aplicar autenticação dos usuários os métodos EAP-TLS, PEAP-MS-CHAP e EAP-MD5.

SSID	Método de Autenticação
PROFS	EAP-TLS
ALUNOS	PEAP-MS-CHAP
ULBRA	PEAP-MS-CHAP

O método EAP é apenas um método de autenticação que dá ao suplicante e o servidor de autenticação a tarefa de estabelecer o método de autenticação para uso real.

EAP-TLS que usar TLS para autenticação mútua entre suplicante e ponto de acesso. Tanto o servidor RADIUS e suplicante deve ter um certificado. Além da tarefa de ter de configurar cada usuário com um certificado, este é certamente o mais seguro método de autenticação, já que nenhuma senha de usuário precisa ser digitada. A autenticação EAP-TLS requer uma infra-estrutura de chave pública (PKI) para emitir certificados e mantê-los atualizados.

O PEAP usa TLS para autenticar o ponto de acesso e estabelecer um túnel criptografado onde será usado o MS-CHAPv2 para autenticar o suplicante com um nome de usuário e senha. A vantagem deste método é que apenas o servidor RADIUS precisa ter o certificado.

Se a autenticação for do tipo EAP-TLS o nome do usuário fornecido pelo certificado será utilizado para associação a VLAN. No caso do PEAP o grupo do usuário será utilizado para definir a qual VLAN será atribuído o acesso.

4 CENÁRIO DE TESTES

Para demonstrar o modelo proposto será criado um cenário de teste, com as definições já citadas. Criação das VLAN utilizando ZeroShell, a configuração o servidor RADIUS para fornecer acesso seguro aos usuários e os métodos de autenticação, utilizando o serviço de diretórios já existente para credencias de usuários.

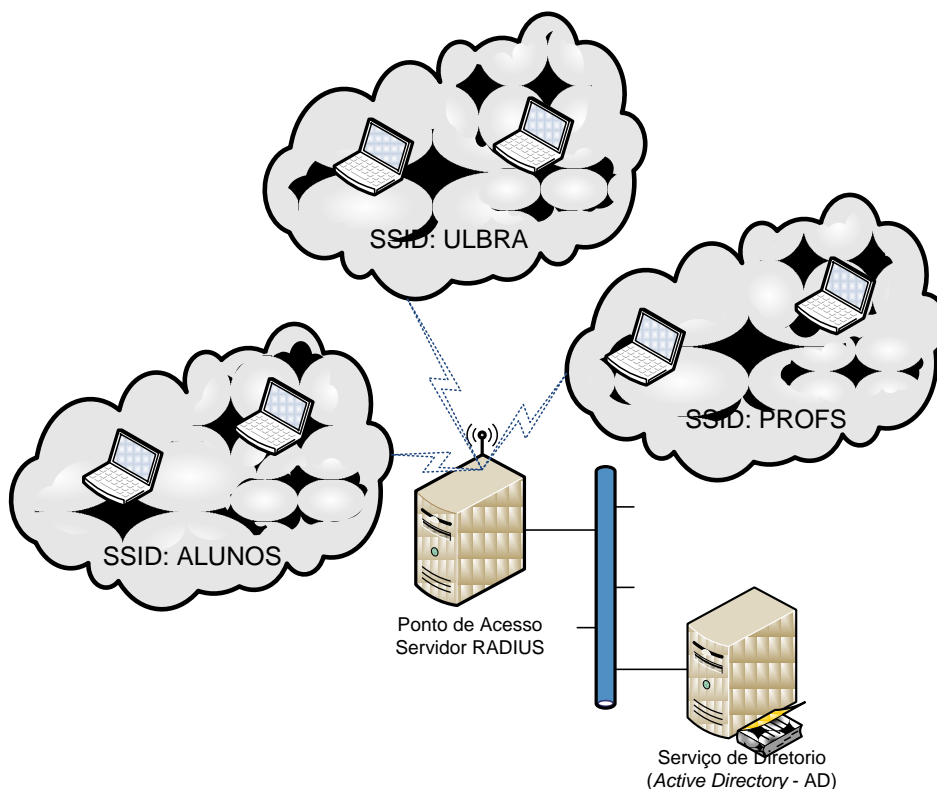


Figura 10: Cenário de teste

Para chegar ao cenário de testes será necessário conduzir a instalação e configuração da seguinte forma:

1) Configuração básica ZeroShell

Instalação do ZeroShell em uma máquina com placa de rede sem fio baseada no *chipset Atheros*. Atribuir a este equipamento um endereço IP e ativar a interface web para gerenciamento remoto.

2) Configuração do modulo de BBS e Configuração das VLAN

A ativação do modulo *wifi-manager*, que permite o gerenciamento de interfaces sem fio. Serão criadas as três redes VLAN sem fio e a estas serão atribuídos os métodos de autenticação.

3) Configuração do servidor RADIUS

A utilização do NAP não será possível, visto que para sua implementação completa todas as máquinas que irão acessar a rede sem fio deve ter um dos sistemas operacional Microsoft, hoje muitos usuários já adotaram uma distribuição Linux como sistema operacional. Desta forma será possível utilizado como servidor RADIUS o Microsoft IAS ou o ZeroShell. Na criação do cenário de teste estas duas hipóteses serão utilizadas, a que apresentar maior eficiência será utilizada.

4) Integração do servidor RADIUS com o AD;

O IAS fornece uma interface direta de conexão com o AD o que de certa forma facilitaria a integração do servidor RADIUS, entretanto é necessário avaliar o desempenho do ZeroShell que para a integração com o AD utilizar o protocolo de segurança *Kerberos*.

5) Configuração da infra-estrutura de PKI

Para a utilização do método de autenticação EAP-TLS, uma infra-estrutura de PKI será utilizada. Esta infra-estrutura irá fornecer certificados digitais que é utilizado no método EAP-TLS.

6) Criação dos grupos de acesso e usuários

Através da ferramenta *Active Directory User and Computers* os grupos e usuários serão criados.

7) Testes iniciais;

Utilizando um computador portal serão realizados os testes de acesso nos três SSID criados. Os testes a que serão realizados são de acesso aos recursos da rede, como impressoras, servidor de arquivos, compartilhamento de arquivos entre usuários da mesma VLAN e acesso à internet. Também será realizado teste de acesso entre as VLANs o que não deve ser permitido.

8) Movimentação de usuários nos grupos, validação da funcionalidade de VLAN dinâmica;

Após a conclusão dos testes iniciais, será realizada a movimentação dos usuários nos grupos de acesso, e assim possibilitando a alteração dinâmica dos usuários nas VLANs já definidas.

9) Captura dos pacotes da rede sem fio;

Simular o acesso as redes VLAN e utilizar ferramentas de captura de tráfego com intuito de analisar os pacotes transmitidos e se neles será possível identificar a chave de criptografia do canal para futuras invasões.

10) Teste de invasão a rede;

Para demonstrar que as VLANs de acesso incrementaram a segurança no meio de acesso sem fio, será realizados testes de invasão. Somente desta forma será possível medir o nível de segurança de cada uma das VLANs que serão criadas.

11) Relatar Problemas encontrados

Após a conclusão da instalação, configuração, integração e testes serão relatos no relatório final os problemas, dificuldades e benefícios provados.

5 CONCLUSÃO

A conclusão deste trabalho será apresentada no TTC II, onde o cenário de teste do modelo proposto irá ser desenvolvido para demonstração dos benefícios de incrementar segurança e gerenciamento de uma rede sem fio. Entretanto após finalizar a pesquisa é possível considerar alguns pontos fundamentais.

Atualmente professores, alunos e demais usuários compartilham sem nenhum mecanismo de controle de acesso e segurança a rede sem fio do LABIN Guaíba. Estes usuários estão propensos a terem seus dados capturados por atacantes que dificilmente serão identificados, assim como recursos da rede estão expostos a possíveis ameaças, ou seja, o acesso ilimitado a rede sem fio está expondo de certa forma a rede de computadores do LABIN de Guaíba a ataques. Para prover segurança é necessário criar barreiras que dificultem os ataques independente de sua origem. Desta forma o modelo propõe duas soluções que irão auxiliar no gerenciamento dos usuários e na segurança das informações que são trocadas através do meio de comunicação sem fio.

Com a utilização de redes VLAN será criada uma barreira lógica entre os grupos de usuários que compartilham o acesso sem fio, que será incrementada com segurança através do padrão 802.1x utilizando autenticação centralizada em um servidor RADIUS. Desta forma serão agregadas confiabilidade e autenticidade na transferência de dados através da rede sem fio, também será possível controlar os usuários que terão acesso, assim como negar o acesso a determinado usuário a qualquer momento. Estes grupos de acesso estarão ligados diretamente as redes VLANs criadas. Assim será possível movimentar usuários através dos grupos de acesso dinamicamente.

Com isto a rede do LABIN Guaíba estará criando dificuldades para que atacantes possam capturar dados importantes e até mesmo violar algum recurso da rede inviabilizando o acesso pelos usuários.

BIBLIOGRAFIA

Geier, Jim; Wireless-Nets, Ltd. Implementing 802.1X Security Solutions for Wired and Wireless Networks Networks. Publicado por Wiley Publishing, Inc. Indianapolis, Indiana, publicado simultaneamente no Canada, 2008

Harold F. Tipton; Krause, Micki. Information Security Management Handbook, Sixth Edition, Purchase Hardcopy, Auerbach Publications 2007

Hideki Imai; Mohammad Ghulam Rahman; Kazukuni Kobar., Wireless Communications Security. Artech House 2006

David D. Coleman; David A. CWNA: Certified Wireless Network Administrator Study Guide (Exam PW0-100). Westcott. Sybex. 2006

Harris, Shon. CISSP: All-in-One Exam Guide, Fourth Edition, McGraw-Hill/Osborne. 2008

Harris, Shon. CISSP Certification Passport. McGraw-Hill/Osborne. 2002

Chandra, Praphul. Wireless Networking: Know It All. Newnes. 2008

Joseph Davies. Deploying Secure 802.11 Wireless Networks with Microsoft Windows, Microsoft Press. 2004.

Moraz Eduardo. Treinamento Profissional Anti-Hacker. São Paulo: Digerati books. 2006

Stewart, James Michael. Tittel, Ed. Chapple, Mike. CISSP: Certified Information Systems Security Professional Study Guide, Fourth Edition. Sybex. 2008

Davies, Joseph. Northrup, Tony. Windows Server 2008 Networking and Network Access Protection (NAP). Microsoft Press. 2008

McGraw-Hill. CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0-100, Third Edition. Osborne. Planet3 Wireless. 2005

Deal, Richard. CCNA Cisco Certified Network Associate Study Guide (Exam 640-802), 4th edition. McGraw-Hill/Osborne. © 2008.

Conlan, Patrick J.. Cisco Network Professional's Advanced Internetworking Guide. Sybex. © 2009

Lammle, Todd. CCNA: Cisco Certified Network Associate Study Guide, Deluxe Edition, Fifth Edition. Sybex. © 2007

MALINEN, Jouni. Host AP driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant. Disponível em <<http://hostap.epitest.fi>>. Acessado em 18 de novembro de 2009.

RACCIARDI, Fulvio. Router/Bridge Linux Firewall. Disponível em <<http://www.zeroshell.net/eng>>. Acesso em 18 de novembro de 2009.

CARVALHO, Hugo Eiji Tibana. PKI - Infra-estrutura de Chaves Públicas. Trabalho desenvolvido para a disciplina Redes de Computadores II, da UFRJ, no período 2008.2. Disponível em <http://www.gta.ufrj.br/ensino/eel879/trabalhos_v1_2008_2/hugo/Infra-estruturadeChavesPblicas.html>. Acesso em: 18 de novembro de 2009.