

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

CONTROLE DE SEGURANÇA E ACESSO EM REDES WIRELESS
(Um estudo de caso em ambiente Microsoft utilizando 802.1x)

CONTROLE DE SEGURANÇA E ACESSO EM REDES WIRELESS
(Um estudo de caso em ambiente Microsoft utilizando 802.1x)

Monografia apresentada ao curso de
Bacharelado em Sistemas de Informação
da Faculdade Natálense para o
Desenvolvimento do Rio Grande do
Norte como requisito parcial para a
obtenção do título de Bacharel em
Sistemas de Informação.

Orientador:

Agenor C. Galliza Neto

Agenor C. Galliza Neto

AGENOR C. GALLIZA NETO

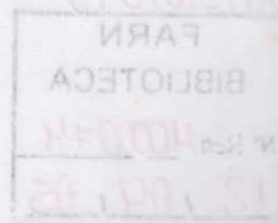
CONTROLE DE SEGURANÇA E ACESSO EM REDES WIRELESS
(Um estudo de caso em ambiente Microsoft utilizando 802.1x)

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto

NATAL/RN
2004



Catalogação na Pública – Bibliografia da FARN
Setor de Processos técnicos

Galliza Neto, Agenor C.

Controle de segurança e acesso em redes Wireless / Agenor

C. Galliza Neto. – Natal : FARN, 2004.

46p.

Orientador: Aluizio Ferreira da Rocha Neto (M. Sc.)

Monografia (Graduação em Sistemas de Informação) –

Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes sem fio – Wireless – monografia 2. segurança de redes –
monografia I. Título

RN/FARN/BC

CDU 004.7

RB-21343

FARN
BIBLIOTECA
Nº Rec 400074
12 / 04 / 05

M
004.7
616LC
2004

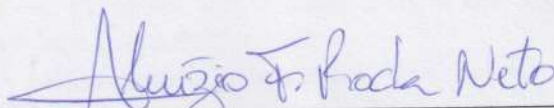
NATALIAN
2004

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE BACHARELADO EM SISTEMA DE INFORMAÇÃO**

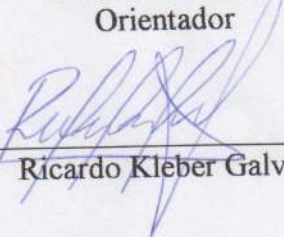
**CONTROLE DE SEGURANÇA E ACESSO EM REDES WIRELESS
(Um estudo de caso em ambiente Microsoft utilizando 802.1x)**

Agenor C. Galliza Neto

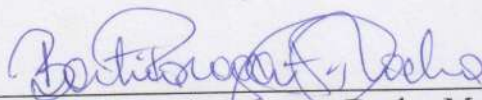
Monografia apresentada e aprovada em 13 de
DEZEMBRO de 2004 pela banca examinadora composta pelos seguintes
membros.



Aluizio Ferreira da Rocha Neto, Msc.
Orientador



Ricardo Kleber Galvão



Bartira P. Falcão Dantas Rocha, Msc.

Natal, _____ de _____ de _____

AGRADECIMENTOS

Agradeço obviamente a Deus, esse ser que vive e mostra sua grandezas todos os dias com o surgir e o desaparecer do sol, respaldando-nos com luz sobre todos nós, pois sem esse Deus nada existiria, sem a força que me motivou para lutar por mais esse capítulo da vida.

Especialmente à minha avó Clotilde, que com todo o seu amor e esforço se agarrava a mim e ao meu sonho como se fosse seu, me dando toda a força que podia e o que não podia, para me ver mais um degrau acima rumo a uma vida futura de prosperidade. Te amo.

Aos meus pais Antonio Gellian e Fátima, que nunca poderiam deixar de serem citados em todas as ocasiões da minha vida, pois sem a união de palavras citadas aqui não seriam vocês.

Ao meu eterno amor Raquel, que mais do que uma parceira de estudos na reta final do término da faculdade, foi uma compreensiva e amorosa nas horas que precisei me apoiar.

Ao meu grande amigo e mais do que tudo, um irmão, que me deu as melhores horas da minha vida, tanto de estudo quanto de lazer, e sei que sou a sua inspiração e vitória entre tantas outras que ele esteve e vai estar.

Aos meus padrinhos, Juci e Anailza, que sempre estiveram ao meu lado, me dando total ajuda, apoio e força.

A minha irmã Andréa, que por mais que esteja longe, sempre me dá força e me inspira.

Ao meu grande orientador e agora amigo, que me ajudando dias e noites com os problemas que tive, me fez entender que o trabalho é uma grande satisfação.

A todos que participaram direta e indiretamente da minha vida, pois sem vocês não estaria aqui hoje, e sei que a vida nos separa, mas a amizade permanece.

E claro a toda a minha família que sempre me deu força para lutar, e para seguir em frente.

Amo todos vocês...

À minha amada mãe, dedico em especial esta monografia, pois sei que nunca em minha vida me deixou só, nem que fosse em seus pensamentos.

Ao meu Pai que sempre me deu força.

À minha vovó que se desdobrou em mil para que eu fosse o que hoje sou.

À minha doce filha.

À minha amada Raquel, que me apoiou e sei que me apoiará sempre, me dando total confiança de que tudo dará certo em nosso futuro.

A mim mesmo...

AGRADECIMENTOS

Agradeço obviamente a Deus, esse ser que vive e mostra sua grandeza todos os dias com o surgir e o desaparecer do sol, resplandecendo sua luz sobre todos nós, pois sem esse Deus nada existiria, nem a força que me motivou para lutar por mais esse objetivo de vida.

Especialmente a minha avó Cidinha, que com todo o seu amor e esforço se agarrou a mim e ao meu sonho como se fosse seu, me dando todo apoio que podia e o que não podia, para me ver mais um degrau acima rumo a uma vida futura de prosperidade. Te amo.

Aos meus pais Antonio Galliza e Edinha, que nunca poderiam deixar de serem citados em todas as ocasiões da minha vida, pois sem eles não seria nada, obrigado por tudo pois milhões de palavras colocadas aqui não seriam a verdadeira expressão do meu amor por vocês.

Ao meu eterno amor Raquel, que mais do que ninguém me suportou com os mais altos níveis de estresse na reta final do término da minha monografia, sempre sendo compreensiva e amorosa nas horas que precisei me dando o devido apoio.

Ao meu grande amigo e mais do que tudo, irmão, Fernando, que nunca se absteve nas piores e melhores horas da minha vida, nunca deixando a peteca cair com seu bom humor insuportável, e sei que sem a sua imprescindível ajuda não teria conseguido galgar mais essa vitória entre tantas outras que ele esteve e vai estar presente.

Aos meus padrinhos, Juca e Anatózia, que sempre se dispuseram amorosamente para o que eu precisasse me dando total ajuda, adoro vocês.

A minha irmã Andréa, que por mais que estejamos separados e às vezes chateados um com o outro, nos amamos e sabemos disso.

Ao meu grande orientador e agora amigo, Aluizio Rocha, que teve toda a paciência do mundo me ajudando dias e noites com os problemas que tive para finalizar essa monografia, confiando em mim mesmo sabendo que o trabalho era árduo.

A todos que participaram direta e indiretamente de tudo isso como os meus colegas de faculdade que também me aturaram todos esses anos, e que mesmo que a vida nos separe sempre estaremos unidos pela força da amizade.

E claro a toda a minha família que sempre, sempre me deu forças para lutar, e para seguir em frente.

Amo todos vocês.....

RESUMO

As redes *Wireless* estão sendo amplamente utilizadas por instituições com o propósito de baratear seus custos de infra-estruturas de cabeamento, além de prover maior mobilidade e flexibilidade para seus usuários. Entretanto, esta é uma tecnologia ainda muito recente e que ainda possui algumas falhas de segurança, demandando uma preocupação adicional de como se proteger de prováveis invasões de pessoas mal intencionadas. Tais invasões crescem a cada dia, devido à facilidade de se conectar às redes *Wireless*. Neste contexto, esse trabalho aborda as diversas técnicas de proteção para as redes sem fio, e em especial, o protocolo 802.1x integrado a outros, como o WEP e IAS, para o controle de acesso de tais redes, tanto na parte física quanto na parte lógica.

Palavras chaves: Redes sem fio; Segurança; Proteção.

SUMÁRIO

1	INTRODUÇÃO	12
1.1	MOTIVAÇÃO	13
1.2	OBJETIVOS	13
1.3	JUSTIFICATIVA	14
1.4	ORGANIZAÇÃO DO TRABALHO	14
2	REFERENCIAL TEÓRICO	16
2.1	REDES <i>WIRELESS</i>	16
2.1.1	Configurações de Redes <i>Wireless</i>	16
2.1.2	Associação de estações	16
2.2	APLICAÇÃO DE REQUISITOS DE SEGURANÇA	17
2.3	MECANISMOS DE SEGURANÇA	17
2.4	CONTROLE DE ACESSO ÀS REDES	18
2.4.1	Controle de acesso ao meio físico	18
2.4.2	Controle de acesso aos dados que estão trafegando	19
3	SEGURANÇA EM REDES <i>WIRELESS</i>	20
3.1	ATAQUES	20
3.1.1	Associação Maliciosa	20
3.1.2	ARP <i>Poisoning</i>	20
3.1.3	MAC <i>Spoofing</i>	21
3.1.4	D.o.S.	21
3.1.5	<i>Wardriving</i>	21
3.1.6	<i>Warchalking</i>	21
3.2	O PROTOCOLO WEP (<i>Wider Equivalent Privacy</i>)	21
3.3	REDES <i>WIRELESS</i> SEGURAS	22
3.3.1	Planejar o local ideal da antena	22
3.3.2	Utilizar o protocolo WEP	22
3.3.3	Mudar o SSID e desabilitar o broadcast	23
3.3.4	Desabilitar o DHCP	23
3.3.5	Desabilitar ou modificar os parâmetros SNMP	23
3.3.6	Utilizar " <i>Access list</i> "	23
3.3.7	Redes <i>Wireless</i> seguras em grandes corporações	23
3.4	O PROTOCOLO 802.1X	24
3.5	Terminologias	27
4	USANDO O 802.1X E A CRIPTOGRAFIA PARA PROTEGER WLANs	28
4.1	DECIDINDO SOBRE A FORMA DE AUTENTICAÇÃO	29
4.1.1	Selecionando autenticação baseada por usuário e/ou computador	29
4.1.2	Determinando os requisitos da autorização de rede	31
4.1.3	Determinando critérios de conexão	31
4.1.4	Determinando restrições à conexão	31
4.2	DETERMINANDO A CRIPTOGRAFIA DE TRÁFEGO COM O WEP	33
4.3	USANDO O IAS PARA GERENCIAR O ACESSO À REDE	33
4.3.1	Identificando os requisitos da organização de acesso à rede	33
4.3.2	Usando o IAS para gerenciar o acesso sem fio à rede	34
4.3.3	Determinando a função do IAS como servidor RADIUS	35
4.4	CONFIGURAÇÃO <i>WIRELESS</i> EM AMBIENTE WINDOWS XP	36
4.4.1	Processo de autenticação 802.1X	41
4.4.2	Credenciais armazenadas automaticamente	43
5	CONCLUSÕES	44

LISTA DE FIGURAS

Figura 1 - Funcionamento da Autenticação	26
Figura 2 - Menu de uma interface de rede <i>wireless</i> no Windows XP.....	37
Figura 3 - Verificando as opções de endereços IP	37
Figura 4 - Colocando os endereços automáticos	38
Figura 5 - Habilitando a configuração da rede <i>wireless</i>	39
Figura 6 - Habilitando a chave WEP	39
Figura 7- Configurando o componente de autenticação	40
Figura 8 - Escolhendo Método de Autenticação.....	41
Figura 9 - Retirando o visto de <i>logon</i> automático	41
Figura 10 - Tela de <i>Logon</i> do Windows.....	42
Figura 11 - Abrindo a conexão da rede.....	42
Figura 12 - Verificando o sucesso da autenticação.....	42

LISTA DE TABELAS

Tabela 1 - Considerações para a autenticação do computador.....	30
Tabela 2 - Exemplos de restrições à conexão WLAN	32
Tabela 3 - Funções do RADIUS IAS.....	35
Tabela 4 - Tipos de autenticação	36

LISTA DE ACRÔNIMOS

AP	<i>Access Point</i>
BSSID	<i>Basic Service Set Identifier</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
Firewall	Programa Anti-Invasão
MAC	<i>Media Access Control</i>
PDA's	<i>Personal Digital Assitent</i>
SSID	<i>Service Set Identifier</i>
SNMP	<i>Simple Network Management Protocol</i>
TI	Tecnologia de Informação
WEP	<i>Wider Equivalent Privacy</i>

1 INTRODUÇÃO

A família de especificações de tecnologias para redes sem fio, IEEE 802.11, tem sido amplamente utilizada por instituições e empresas com a finalidade de economia em infraestrutura de cabeamento, além de prover interligação, maior mobilidade e flexibilidade para redes locais. Em contrapartida, existem algumas preocupações adicionais em segurança que são inerentes a um meio de comunicação sem fio.

Por ser uma tecnologia relativamente recente, muitas vulnerabilidades podem ser encontradas e outras poderão ser descobertas. É justamente explorando estas vulnerabilidades que atacantes se infiltram nas redes sem fio. A forma comumente utilizada para explorar estas vulnerabilidades é através do uso de ferramentas desenvolvidas especificamente para esta finalidade.

Ataques direcionados às redes sem fio além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Estas redes tornaram-se um alvo fácil e almejado por pessoas mal intencionadas para o comprometimento de sistemas. A tecnologia *wireless* provê diversos atrativos aos atacantes, como dificuldade na identificação exata da origem do ataque, imaturidade dos gerentes na instalação das mesmas sem a habilitação de um protocolo de segurança, e principalmente pela facilidade em obter acesso à rede cabeada através de uma conexão ao ar livre.

Esta monografia analisa as vulnerabilidades presentes nas redes sem fio, assim como os métodos de ataques e como protegê-las. Um outro fator relevante nas redes sem fio abordado neste trabalho é o controle de acesso aos diversos usuários que a utilizam. Como garantir que somente pessoas autorizadas terão acesso à mesma de forma confiável? A utilização de protocolos de criptografia (Arte de escrever em cifra, em alfabeto oculto) requer o uso de chaves (ou senhas) que habilitam um determinado usuário entrarem na rede. Disponibilizar estas chaves para um grande número de usuários de redes *wireless* é um problema considerável.

1.1 MOTIVAÇÃO

A tecnologia não é tangível, não tem limites, e mesmo após décadas de desenvolvimento e revoluções no mercado de informática, as necessidades no mundo dos negócios estão muito longe de serem solucionadas. Com o crescimento exponencial do desenvolvimento tecnológico versus a competitividade que leva as empresas a uma redução de custos, as áreas de TI são forçadas a possuírem cada vez mais agilidade na administração dos recursos e aumento de produtividade.

Diante deste ciclo vicioso, o desenvolvimento de ferramentas que aperfeiçoem os recursos existentes e implantem técnicas de auditoria e controle na infra-estrutura de TI é cada vez maior; necessidades estas que levam as empresas de tecnologia a quebrarem paradigmas e derrubarem fronteiras, desenvolvendo mecanismos cada vez mais próximos da realidade virtual, isto é, mecanismos que controlem e monitorem em tempo real as atividades humanas impactantes no negócio.

Baseado nesta filosofia tecnológica surgiu o padrão IEEE 802.1x, padrão este que pode ser considerado um marco no surgimento de uma nova era de dispositivos de *Networking*.

O rápido aumento da utilização das redes sem fio 802.11 no decorrer dos últimos anos é comparado com o crescimento da Internet nas últimas décadas (WADLOW 2000, pág. 50). Estas redes são cada vez mais utilizadas como um auxílio precioso para as LANs "*Local Area Networks*" (DORMAN 2001, pág. 30) convencionais, seja por prover uma alternativa economicamente viável, seja por prover taxas de transmissão comparáveis a redes guiadas.

Este projeto estuda os protocolos que dão suporte às redes 802.11, analisando suas vulnerabilidades, as técnicas de ataques e as ferramentas mais utilizadas por pessoas mal intencionadas para o comprometimento destas redes, tendo como objetivo fornecer a base conceitual necessária para que ferramentas de segurança para redes 802.11 possam ser desenvolvidas.

1.2 OBJETIVOS

A análise das vulnerabilidades é voltada ao estudo das falhas de segurança presentes na estruturação dos protocolos 802.11. Soma-se a esta Análise, outra onde se leva em consideração à comunicação entre os dispositivos de rede sem fio.

O estudo das técnicas utilizadas para explorar estas vulnerabilidades também é realizado. Com esse estudo, são identificados o grau de conhecimento do atacante, informações de vulnerabilidades ainda não conhecidas e formas eficazes de se identificar quando algum destes ataques está sendo disparado contra determinada rede.

Outro estudo que é feito diz respeito ao controle de acesso às redes sem fio mediante a identificação do usuário através de um *login* e uma senha. Neste aspecto, são analisados os protocolos relacionados ao protocolo IEEE 802.1x, desenvolvido para esta finalidade.

1.3 JUSTIFICATIVA

Este projeto envolverá o estudo de protocolos, comportamentos intrusivos em redes sem fio e estudo das ferramentas de uso malicioso. A necessidade de um estudo em diversas áreas diferentes do conhecimento possibilitará um grande aprendizado nestas áreas.

A insegurança que será analisada nesta pesquisa afeta cotidianamente as redes sem fio de computadores, haja visto o resultado de outros estudos desenvolvidos em laboratórios no sentido de quantificar e qualificar estas redes. Entretanto, muitos grupos de pesquisa têm estudado formas de banir as vulnerabilidades e não permitir que os ataques ocorram.

Apesar do extremismo em afirmar as vulnerabilidades existentes nas redes sem fio, algumas destas não podem ser trivialmente exploradas. Ou seja, somente um atacante com um bom grau de conhecimento da tecnologia é capaz de dispará-los, o que de certa forma mantém estas vulnerabilidades ocultas.

Atualmente, há uma ampla variedade e suporte para conexões *wireless* em PDAs (*Personal Digital Assitent*) que são computadores do tipo *handhelds*, o que faz com que atacantes possam passar despercebidos em ambientes de redes sem fio e ter maior mobilidade.

1.4 ORGANIZAÇÃO DO TRABALHO

Esta monografia está organizada da seguinte forma. O capítulo 2 apresenta o referencial teórico, abordando sobre o que são redes *wireless*, quais as formas de configuração, tendo como principal objetivo requisitos de segurança para um melhor controle e confiabilidade no tráfego e na parte física dessas redes.

O capítulo 3 apresenta aspectos de funcionamento das redes sem fio, as formas de ataques e quais as conhecidas no momento, visto que todos os dias aparecem novidades, as

vulnerabilidades que essas redes oferecem, mostrando meios de se prevenir, dando exemplos de tecnologias e alguns protocolos de segurança, mais especificamente WEP e o 802.1x.

O capítulo 4 aborda o estudo de protocolos de criptografias para proteger wlans, dando exemplos de como são feitas as configurações de segurança, com a proposta de um controle de acesso bem planejado, mesclando tecnologias, critérios e requisitos de segurança e também analisando toda a estrutura dessas redes para chegar a uma proteção específica para cada uma delas.

Por fim, o capítulo 5 faz as considerações finais chegando a conclusões importantes sobre a segurança no controle de acesso às redes sem fio, deixando sempre a idéia que teremos que estar em constante evolução ao que se refere a segurança em rede de um modo geral.

Existem três formas de configurações de uma WLAN. Modo Ad Hoc (ARCOMANO 2002, pág. 36) (VOLBRECHT 2002, pág. 40), onde existem somente estações sem fio que se comunicam mutuamente, sem a presença de access points. Todas as estações possuem o mesmo BSSID (Basic Service Set Identifier) que corresponde ao identificador da célula sem fio. O termo próprio do 802.11 para este tipo é IBSS (Independent Basic Service Set). Este tipo de configuração pode ser comparada a comunicações peer-to-peer em redes cabeadas.

Modo de infra-estrutura básica (VOLBRECHT 2002, pág. 41), onde as estações sem fio se comunicam com um simples AP. Este access point pode funcionar como um bridge entre a rede sem fio e a rede guiada. O termo utilizado para este tipo de rede é BSS (Basic Service Set).

Modo infra-estruturado (ARCOMANO 2002, pág. 36) (VOLBRECHT 2002, pág. 26), onde redes distintas (com BSSIDs diferentes em cada uma) se comunicam através de APs criando uma única rede. Este modo tem como objetivo fazer com que o usuário possa mudar seu ponto de acesso e mesmo assim permanecer conectado. O termo mais utilizado para este modo de rede é ESS (Extended Service Set).

2.1.3 Associação de estações

Segundo (MURIELLO 2002, pág. 37), em redes guiadas, é necessário que uma estação esteja fisicamente ligada a outro dispositivo desta rede para poder se conectar a esta rede. Em redes sem fio, é necessário que a estação tenha qual o SSID (Service Set Identifier – Identificador do domínio do serviço) para poder se conectar.

2 REFERENCIAL TEÓRICO

2.1 REDES WIRELESS

Segundo (DORMAN 2001, pág. 24) é possível entender como as redes sem fio são implementadas e como os protocolos de comunicação atuam nestas redes. Também são apresentadas as diferenças entre as redes convencionais e as sem fio, para que se possa entender quais ataques são realmente inerentes a redes sem fio.

2.1.1 Configurações de Redes Wireless

Existem três formas de configurações de uma WLAN:

Modo Ad Hoc (ARCOMANO 2002, pág. 36) (VOLBRECHT 2002, pág. 40), onde existem somente estações sem fio que se comunicam mutuamente, sem a presença de *access points*. Todas as estações possuem o mesmo BSSID (*Basic Service Set Identifier*) que corresponde ao identificador da célula sem fio. O termo próprio do 802.11 para esta rede é IBSS (*Independent Basic Service Set*). Este tipo de configuração pode ser comparada a conexões *peer-to-peer* em redes cabeadas.

Modo de infra-estrutura básica (VOLBRECHT 2002, pág. 41), onde as estações sem fio se comunicam com um simples AP. Este *access point* pode funcionar como um *bridge* entre a rede sem fio e a rede guiada. O termo utilizado para este tipo de rede é BSS (*Basic Service Set*).

Modo infra-estruturado (ARCOMANO 2002, pág. 36) (VOLBRECHT 2002, pág. 26), onde redes distintas (com BSSIDs diferentes em cada uma) se comunicam através de APs criando uma única rede. Este modo tem como objetivo fazer com que o usuário possa mudar seu ponto de acesso e mesmo assim permanecer conectado. O termo mais utilizado para este modo de rede é ESS (*Extended Service Set*).

2.1.2 Associação de estações

Segundo (MURILLO 2002, pág. 37), em redes guiadas, é necessário que uma estação esteja fisicamente ligada a outro dispositivo desta rede para poder se conectar a esta rede. Em redes sem fio, é necessário que a estação saiba qual o SSID (*Service Set Identifier* – Identificador do domínio de serviço) para poder se conectar.

Existem várias formas de um cliente saber o SSID da rede na qual vai se conectar. Uma destas formas é a configuração manual de todos os dispositivos que podem se conectar na rede. Esta forma não é muito utilizada, pois a simples mudança de um SSID acarretaria na modificação das configurações dos dispositivos autorizados.

2.2 APLICAÇÃO DE REQUISITOS DE SEGURANÇA

Segundo (WADLOW 2000, pág. 13) existem alguns requisitos de segurança. Entre eles prevalece a confiabilidade, disponibilidade, controle de acesso, integridade, pontualidade, confidencialidade e autenticação. As restrições computacionais presentes nas redes sem fio são grandes limitadores das soluções de segurança que podem ser executadas neste ambiente, especialmente a distribuição de chaves WEP.

Requisitos de segurança são essências para redes sem fio, para garantirem aos cidadãos envolvidos a privacidade a quem tem direito, bem como impedir o uso indevido e o acesso não autorizado às informações. Como exemplos, sistemas projetados para controle do trânsito podem ser usados para facilitarem assaltos e fugas de criminosos; sistemas de espionagem podem ser adulterados enviando informações incorretas que prejudiquem o trabalho. E várias outras aplicações de redes de sensores sem fio estão sujeitas à ação de invasores caso não estejam protegidas por rigorosos mecanismos de proteção.

2.3 MECANISMOS DE SEGURANÇA

(WADLOW 2000, pág 32) também afirma que mecanismos de segurança visam garantir o uso da rede na forma como ela foi concebida, eliminando a ação do inimigo. Os principais são:

- Métodos criptográficos;
- Protocolos de gerência de chaves criptográficas;
- Detecção de intrusão;
- Filtros de pacotes e de conteúdos das mensagens.

Os requisitos de segurança para redes de sensores sem fio dependem da criticidade da aplicação. Assim, uma rede de sensores pode necessitar de alguns ou todos os requisitos abaixo.

- **Confidencialidade:** Oculta as informações do inimigo. Em muitas aplicações, a obtenção das informações por parte do inimigo pode ser prejudicial;
- **Autenticidade ponto-a-ponto:** Garante a origem das informações em comunicação ponto-a-ponto;
- **Autenticação em modo de difusão:** Garante a origem das informações em modo de difusão;
- **Integridade:** Garante que a mensagem tem o conteúdo exato que foi enviado, sem alteração;
- **Pontualidade:** possibilita o descarte de mensagens antigas repetidas que podem ser inseridas pelo inimigo;
- **Disponibilidade:** Garante que as aplicações conseguiram utilizar os recursos de rede.

2.4 CONTROLE DE ACESSO ÀS REDES

Ao que se refere ao acesso às redes podemos classificar dois níveis de controle de acesso: controle de acesso ao meio físico e controle de acesso aos dados que estão trafegando na rede.

2.4.1 Controle de acesso ao meio físico

Este aspecto é bastante relevante em redes sem fio, visto que o meio físico de tais redes, o ar atmosférico, é extremamente acessível, comparando a uma rede convencional. A rede sem fio tem uma dinamicidade muito grande. Seus usuários não precisam de pontos de rede para se conectar a ela. Basta-o estar na área de cobertura do sinal dessa rede que ele pode se conectar se não houver nenhum tipo de controle de acesso.

Em redes sem fio de grande amplitude, como a de um campus em uma instituição de ensino, onde comumente tais redes são encontradas, isto pode ser um problema sério se analisarmos que a vizinhança de tal instituição provavelmente estará recebendo o sinal da rede *wireless* do campus. Dessa forma, pessoas que não têm nenhum vínculo com a instituição poderão estar usando o acesso à rede para fins totalmente alheios aos da instituição que provê a rede.

Mecanismos de autenticação dos usuários normalmente deverão ser utilizados em tais redes *wireless*. O Capítulo 4 abordará tal assunto apresentando o protocolo 802.1x que é um

protocolo de autenticação, integrado a outros protocolos de criptografia para fornecer a segurança necessária a esse meio.

2.4.2 Controle de acesso aos dados que estão trafegando

Este controle tanto serve para protocolos de redes sem fio quanto para redes convencionais. Muitas vezes este controle é deixado para as *camadas de protocolo*¹ superiores. Isto é, a nível da camada de enlace, o dado é transmitido do jeito que ele vem das camadas superiores. Se os dados já vêm criptografados da camada de aplicação, por exemplo, não há necessidade de criptografá-los novamente. Mas, se a aplicação não provê algum esquema de embaralhamento dos dados, e também, se esse esquema não é feito na camada de rede, alguém poderá estar observando (capturando) as várias informações sigilosas que estão trafegando na rede.

Portanto, para garantir maior segurança no tráfego de dados pela rede, é interessante utilizar um protocolo de criptografia a nível da camada de enlace. Entretanto, isto não garante que em aplicações que utilizem conexões com a Internet, isto é, fora do âmbito da rede da organização, exista segurança. Como exemplo, considere as aplicações de *Internet Banking*. Como a informação sigilosa, que são os dados bancários, irá trafegar em uma rede insegura, que é a Internet, a aplicação neste caso, o protocolo HTTP de navegação na *Web*, deve prover segurança. Assim, os bancos normalmente disponibilizam seus sites através do protocolo HTTPS, que é uma variação do HTTP, o qual provê criptografia no tráfego entre o navegador do usuário e o servidor do banco.

3.1.1 Associação Maliciosa

A associação maliciosa ocorre quando um atacante passando-se por um acesso point, invade outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real (DORMAN 2001, pág. 22).

3.1.2 ARP Poisoning

O ataque de envenenamento do protocolo de resolução de endereços (ARP) é um ataque na camada de enlace de dados que se pode dar quando um atacante está conectado na mesma rede local que a vítima.

¹ Modelo de Referência de 7 camadas da ISO (*International Standard Organization*): 1 – Físico, 2 – Enlace, 3 – Rede, 4 – Transporte, 5 – Sessão, 6 – Apresentação e 7 – Aplicação.

3 SEGURANÇA EM REDES WIRELESS

3.1 ATAQUES

(MURILLO 2002, pág. 18) afirma que os ataques às redes sem fio não são novos. Ao invés disso, eles são baseados em ataques anteriormente descobertos em redes cabeadas. Alguns destes ataques não sofreram nem uma modificação, já outros sofrem algumas modificações para que possam ser disparados e obter melhores resultados.

Na realidade, o objetivo dos ataques nem sempre são para o comprometimento das redes sem fio, mas sim ganhar acesso ou comprometer a rede guiada. Como as redes guiadas tradicionais tem sido duramente atacadas durante mais de trinta anos, muitas desenvolveram excelentes defesas. Por exemplo, o uso de um *firewall* propriamente configurado pode aumentar sensivelmente o nível de segurança da instituição. Entretanto, se esta mesma instituição possuir uma rede sem fio mal configurada atrás deste *firewall*, é como se existisse um *backdoor* (programa que se instala de maneira furtiva em um computador e permite que um hacker assuma controle total do sistema por meio de uma rede local ou da Internet) (MURILLO 2002, pág. 19) devidamente instalado. Atualmente, a maioria das WLANs irão certamente sofrer de pelo menos um tipo de ataque (PEIKARI, FOGIE 2002, pág. 34). Estes ataques não são limitados às instituições, visto que o maior número de equipamentos deste tipo de rede é vendido para consumidores domésticos. Os quais procuram aumentar sua largura de banda ou distribuir sua conexão em toda sua residência. Esses são os ataques que mais se destacam atualmente nas redes sem fio.

3.1.1 Associação Maliciosa

A associação maliciosa ocorre quando um atacante passando-se por um *access point*, ilude outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real. (DORMAN 2001, pág. 22)

3.1.2 ARP Poisoning

O ataque de envenenamento do protocolo de resolução de endereços (ARP) é um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vítima.

3.1.3 MAC Spoofing

Consiste em alterar o endereço físico da placa de rede (MAC Address) para se passar por outro computador na rede, colocando o endereço MAC deste outro computador. Estes endereços são gravados em EPROM nestas placas, mas podem ser forjados via software.

Existem muitas instituições que criam *access list* (lista de acesso) para todos os dispositivos explicitamente permitidos à conexão. Estas instituições costumam fazer este controle através do endereço MAC da placa do cliente, banindo desta forma o acesso de outras placas não autorizadas.

3.1.4 D.o.S

Ataques de *Denial of Service* (D.o.S – Negativa de Serviço) como o nome próprio indica, procura tornar algum recurso ou serviço indisponível. Em redes sem fio estes ataques podem ser tão perturbadores quanto maior sua sofisticação.

3.1.5 Wardriving

Wardriving é o nome dado à técnica de se dar um pequeno "passeio" de carro, rastreando e invadindo redes a rádio. A origem do nome vêm de uma brincadeira com *Wardialing*, uma técnica utilizada por invasores para se descobrir telefones "conectáveis" em alguma empresa. O *Wardriving* se aproveita dos fracos recursos da tecnologia Wi-Fi de rádio, oficialmente de nome 802.11. Essa tecnologia possui um recurso de criptografia chamado WEP que é fácil de ser quebrado, facilitando a ação.

3.1.6 Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de *wardriving* e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. Isto para que outros atacantes possam de antemão saber quais as características da rede.

3.2 O PROTOCOLO WEP (Wider Equivalent Privacy)

O WEP é um protocolo de segurança para redes locais sem fio (WLANs) definido no padrão 802.11b. WEP foi concebido para proporcionar o mesmo nível de segurança que um

LAN conectado. Nas redes 802.11 o tráfego é criptografado através da utilização do algoritmo WEP. O algoritmo é simétrico uma vez que usa chaves compartilhadas. As chaves criptográficas, chamadas de chaves WEP, devem ser as mesmas no cliente e no *access point*. O WEP é baseado em um processo criptográfico RC4. A criptografia RC4 é simétrica, ou seja, a mesma chave utilizada para a criptografia também é utilizada para a decriptografia. Além disso, este padrão criptográfico utiliza uma cifra conhecida como *Stream Cipher* que faz com que cada mensagem seja criptografada com uma chave diferente. Isto é possível, pois é inserido um elemento adicional à chave criptográfica.

O WEP emprega uma chave secreta de 40 ou 104 bits que é compartilhada entre os clientes e o *access point* da rede.

Durante a transmissão do pacote um vetor de inicialização de 24 bits é escolhido randomicamente e é anexado a chave WEP para formar a chave de 64 ou 128 bits.

3.3 REDES WIRELESS SEGURAS

Nos últimos tempos, movimentos como o *wardriving* e *warchalking* serviam de alerta para a necessidade de se aumentar o fator segurança na implementação das redes sem fio. Segundo (DORMAN 2001, pág. 15), existem seis aspectos principais para construção de uma rede de maneira segura, os quais serão abordados nas sessões seguintes.

3.3.1 Planejar o local ideal da antena

O primeiro passo para implementação de pontos de acesso fechado a uma rede wireless está no local em que a antena, que oferece o sinal para os pontos de acesso, vai estar. Não é recomendável que a antena fique perto de janelas – ao menos que o vidro da janela bloqueie tais sinais. O ideal é colocar a antena no centro da área que se quer cobrir.

3.3.2 Utilizar o protocolo WEP

O WEP é um método criptográfico em redes sem fio. O problema é que muitos revendedores de redes wireless desabilitam o WEP para facilitar a instalação. No entanto, *crackers* (ou pessoas mal intencionadas) podem ter acesso imediato em redes sem o WEP habilitado.

3.3.3 Mudar o SSID e desabilitar o broadcast

O SSID (*Service Set Identifier*) é uma string de identificação utilizada em pontos de acesso a redes sem fios pelo qual os clientes podem iniciar suas conexões. Este identificador vem de fábrica com uma string que o fabricante padroniza, como “3Com” para dispositivos da 3Com. Muitos *crackers* conhecem e utilizam facilmente estes identificadores para fazer uso sem autorização dos serviços de redes sem fio.

3.3.4 Desabilitar o DHCP

O DHCP (*Dynamic Host Configuration Protocol*) é o protocolo de configuração automática e dinâmica de computadores ligados a uma rede TCP/IP, no que tange aos inúmeros parâmetros de rede. A princípio, isto parece uma tática de segurança estranha, mas para redes sem fios, faz sentido. Com este passo, os *crackers* seriam forçados a decifrar seu endereço IP, a máscara de rede e outros parâmetros de TCP/IP exigidos. Se mesmo assim um *cracker* puder fazer uso de seu ponto de acesso por qualquer razão, ele precisará ainda entender como configurar de maneira correta o endereço IP.

3.3.5 Desabilitar ou modificar os parâmetros SNMP

O SNMP (*Simple Network management Protocol*) é o protocolo de gerenciamento de rede da arquitetura Internet TCP/IP que opera na camada de aplicação. Se a rede suporta o protocolo SNMP, é recomendável desabilitá-lo ou modificar seus parâmetros. Se a organização não der este passo, *crackers* poderão usar o SNMP para ganhar informações importantes sobre sua rede.

3.3.6 Utilizar “Access list”

Como visto na sessão 3.1.3, o uso da lista de acesso especifica exatamente quais máquinas poderão se conectar ao ponto de acesso da rede (quando disponível).

3.3.7 Redes Wireless seguras em grandes corporações

Somente o uso do protocolo WEP não é a solução para controlar o tráfego em redes sem fio, pois em *grandes redes wireless*, considerando sua amplitude de sinal e número de

estações clientes, existe a necessidade de compartilhamento da chave para todos os clientes. Além do quê, em tais redes os clientes são extremamente dinâmicos e móveis.

Na sessão seguinte, abordaremos um protocolo que resolve tais problemas.

3.4 O PROTOCOLO 802.1X

O protocolo IEEE 802.1x implementa controle de acesso com base em **portas** de equipamentos de conectividade. No caso de uma WLAN, uma porta é somente uma conexão entre um AP e uma estação. Existem dois tipos de portas no protocolo IEEE 802.1x: não controladas e controladas. Habitualmente os administradores de rede utilizando uma porta não controlada. Ela permite que o dispositivo conectado a ela se comunique com qualquer outro dispositivo da rede. Uma porta controlada, por outro lado, limita os endereços da rede com os quais o dispositivo conectado pode se comunicar. O 802.1x permite que todos os clientes se conectem a portas controladas, mas essas portas somente transmitem o tráfego a servidores de autenticação. Depois que o cliente tiver sido autenticado, será permitido que ele comece a usar a porta não controlada. A diferença do 802.1x é que portas não controladas e controladas são entidades lógicas que podem existir na mesma porta de rede física.

Com relação à autenticação, o 802.1x define adicionalmente duas funções para dispositivos de rede: Um suplicante é um dispositivo (como um laptop com uma placa 802.11b) que solicita acesso a recursos da rede. Um autenticador é um dispositivo que autentica os clientes e decide se concederá ou não o acesso a eles. Um AP sem fio pode ser um autenticador; entretanto, seria mais flexível usar o protocolo *RADIUS* (*Remote Authentication Dial-In User Service*, serviço de autenticação remota para usuário de acesso discado), padrão da indústria, convenientemente incluído no Windows Server 2000 e 2003. Com o RADIUS, o AP aceita a solicitação de autenticação e a distribui a um servidor RADIUS, que autentica o usuário junto ao *Active Directory* (sistema de diretório de contas do Windows Server).

O 802.1x não usa WEP para a autenticação. Em vez disso, ele usa o EAP (*extensible authentication protocol*, protocolo de autenticação extensível) padrão da indústria ou uma variante mais recente, o PEAP (*protected EAP*, EAP protegido). Nos dois casos, a principal vantagem do EAP/PEAP é que eles permitem uma escolha dos métodos de autenticação. Por padrão, o 802.1x usa EAP-TLS (EAP-segurança da camada de transporte), na qual todas as trocas do EAP protegido são asseguradas pelo protocolo TLS. O fluxo total do processo de autenticação tem a seguinte aparência:

1. A estação sem fio tenta conectar-se ao *Switch* (que poderia ser um AP) pela porta não controlada. (como a estação não foi autenticada ainda, ela não pode usar a porta controlada). O *Switch* emite um desafio de texto sem formatação à estação.
2. A estação responde identificando-se.
3. O *Switch* encaminha a mensagem de identidade da estação ao autenticador, usando o RADIUS, pela LAN com fio.
4. O servidor RADIUS procura a conta especificada para determinar que tipo de credencial é exigida (por exemplo, a instituição pode ter configurado o servidor RADIUS para aceitar somente certificados digitais). Essas informações são transformadas em uma solicitação de credencial e são retornadas à estação.
5. A estação envia suas credenciais pela porta não controlada no *Switch*.
6. O servidor RADIUS valida as credenciais; se elas passarem, uma chave de autenticação é enviada ao *Switch*. A chave é criptografada, de modo que apenas o *Switch* possa descriptografá-la.
7. O *Switch* descriptografa a chave e a usa para criar uma nova chave específica para aquela estação. Essa chave é enviada à estação, onde é usada para criptografar a chave de autenticação global mestre para a estação.

E como já falamos em intervalos periódicos, o AP ou *Switch* pode gerar uma nova chave de autenticação mestre e enviá-la aos clientes. Isso nitidamente resolve o problema do 802.11 de ter uma chave fixa de vida útil longa que os invasores podem facilmente atacar usando a força bruta.

Quando implementado o 802.1x na rede, um cliente deve primeiramente autenticar-se no agente autenticador que fornece o meio de acesso à LAN. O autenticador mantém um controle do status da porta para cada cliente que ele está enxergando, e no caso do cliente ser autenticado, então a porta passa para o status autorizado, e o cliente pode enviar os dados da aplicação para a LAN através do *Network Access Server* – NAS (*switch* de acesso). Porém quando o cliente não é autorizado, o status da porta no autenticador permanece como não autorizado, e o cliente não consegue enviar dados de sua aplicação através do *Network Access Server* – NAS (*switch* de acesso).

Na Figura 1 é demonstrado todo o processo de autenticação do usuário.

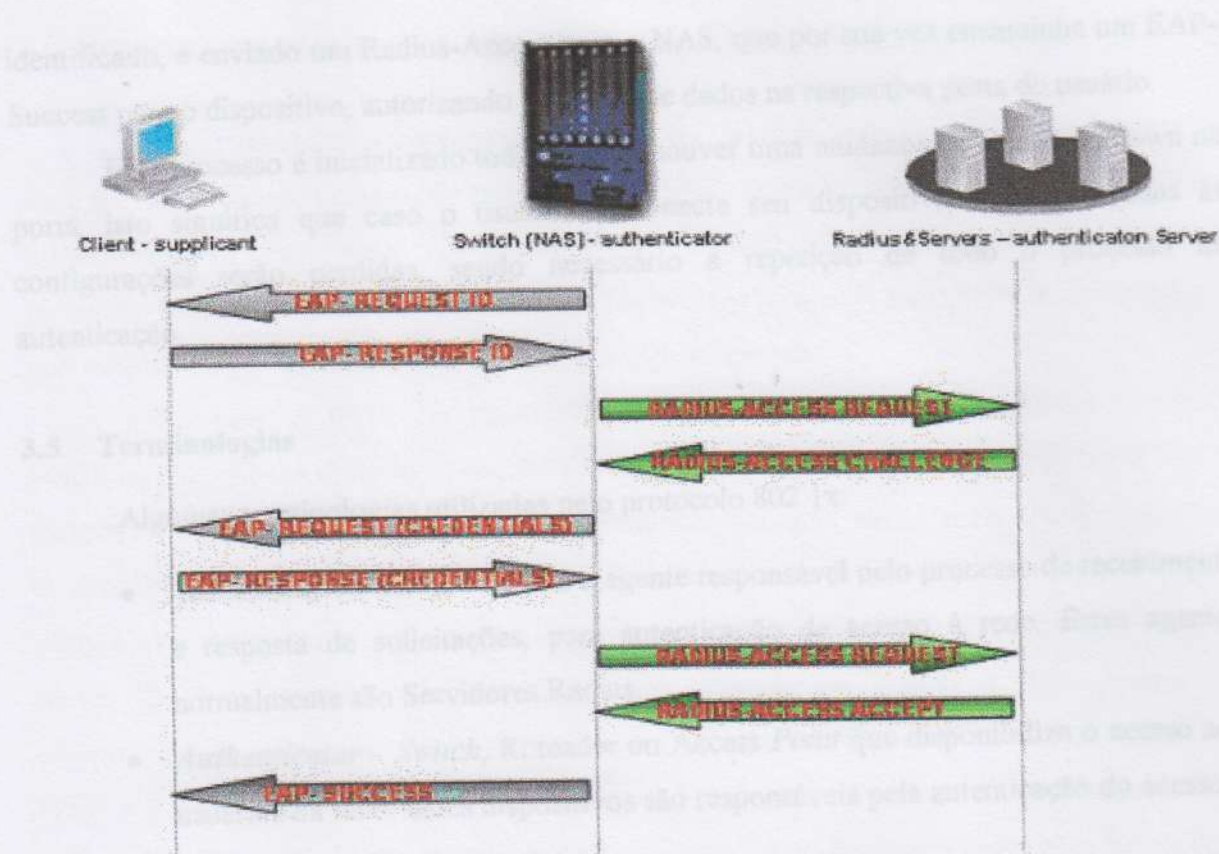


Figura 1 - Funcionamento da Autenticação

Quando o NAS detecta uma atividade na porta, ele envia um *EAP-RequestID* para identificação do usuário do dispositivo. Lembramos que o EAP é um protocolo de autenticação que executa antes da transmissão de outros protocolos no link. Quando o dispositivo recebe esta requisição (e possui um cliente 802.1x instalado), ele responde com sua identificação para o autenticador que por sua vez encaminha a mesma para um servidor de autenticação (por exemplo um Radius). Neste caso o servidor de autenticação estará trabalhando como um identificador e fornecedor de perfil de acesso, através do qual o usuário pode estar em localidades diferentes, porém acessando o mesmo perfil dentro do mesmo servidor de autenticação.

Em resposta ao *AccessRequest* o servidor de autenticação envia ao autenticador um *AccessChallenge*, e o NAS neste momento, encaminha *EAP-Request* para o dispositivo que por sua vez responde com um *EAP-Response* com a identificação do usuário. Então o NAS encaminha esta identificação do usuário para o servidor de autenticação, que determina se o mesmo possui acesso ou não à rede, baseado na sua identificação. No caso do usuário ser

identificado, é enviado um Radius-Accept para o NAS, que por sua vez encaminha um EAP-Success para o dispositivo, autorizando o tráfego de dados na respectiva porta do usuário.

Este processo é inicializado toda vez que houver uma mudança de estado up/down na porta, isto significa que caso o usuário desconecte seu dispositivo da porta, todas as configurações serão perdidas, sendo necessário a repetição de todo o processo de autenticação.

3.5 Terminologias

Algumas terminologias utilizadas pelo protocolo 802.1x:

- **Authentication Server** – Este é o agente responsável pelo processo de recebimento e resposta de solicitações, para autenticação de acesso à rede. Estes agentes normalmente são Servidores Radius.
- **Authenticator** – *Switch*, Roteador ou *Access Point* que disponibiliza o acesso aos usuários da rede. Estes dispositivos são responsáveis pela autenticação do acesso à rede.
- **Supplicant** – Dispositivo de rede que necessita ser autenticado na rede. Na maioria dos casos são estações de trabalho, mas podem ser também *switches* que devem autenticar-se em outros "*Authenticators*".
- **EAP** – EAP é um protocolo genérico que permite que os pontos de acesso à rede suportem múltiplos métodos de autenticação, entre eles estão: *smart cards*, *transport layer security – TLS*, *Kerberos Microsoft*, etc..
- **EAPOL** – EAP over LAN como definido pelo padrão IEEE 802.1x

4 USANDO O 802.1X E A CRIPTOGRAFIA PARA PROTEGER WLANs

Neste capítulo será apresentada uma proposta de controle de acesso para redes sem fio. Esta proposta baseia-se no uso do protocolo IEEE 802.1x para restringir o acesso dos clientes à rede mediante um Login e uma Senha. Como já foi abordado nos capítulos anteriores, o protocolo IEEE 802.11 de WLAN (*Wireless Local Area Network*) tem várias vulnerabilidades que exigem a utilização de esquemas de segurança adicionais.

Felizmente, o IEEE em conjunto com a Microsoft, a Cisco e outros líderes da indústria, perceberam os defeitos do 802.11. Como resultado, o protocolo padrão IEEE 802.1x fornece um suporte para autenticação dos usuários da rede muito mais robusto, além de mecanismos de segurança para WLANs e LANs comuns. É possível implantar o 802.1x usando uma combinação dos controladores de domínio do Windows 2000 ou do Windows Server 2003 e clientes Windows XP. Este controle de acesso à rede poderá ser complementado com o uso de outras tecnologias, tais como o IAS da Microsoft e o protocolo WEP, a fim de evitar a visualização do tráfego por parte de usuários mal intencionados.

Atualmente os pontos de acesso (AP – *Access Point*) de muitas redes sem fio utilizam uma simples chave WEP que é compartilhada para todos os clientes. Com isso, a integridade e o sigilo desta chave global são quase impossíveis de serem gerenciadas. A chave, na realidade, não consegue ser mantida em segredo. Como esta chave deve ser programada em todos os dispositivos autorizados, é praticamente impraticável para redes com muitos clientes. Outro ponto importante é a mudança desta chave. Caso seja necessário, isso demandaria a modificação em todos os clientes. Além disso, qualquer dispositivo subtraído coloca em risco a chave WEP global o que torna o ambiente potencialmente inseguro.

O WEP também não conta com gerenciamento de chaves de criptografia e possuem falhas de criação que com o tempo podem expor as chaves de criptografia a determinados usuários mal-intencionados.

A partir do Windows Server 2000, a Microsoft disponibilizou o IAS (*Internet Authentication Service*), que é uma das implementações de um servidor e *proxy* RADIUS. Como servidor RADIUS, o IAS executa, de forma centralizada, *Autenticação*, *Autorização* e *Acompanhamento* de conta (AAA) de vários tipos de conexões de rede. Como *proxy* RADIUS, o IAS pode encaminhar as solicitações RADIUS a outro servidor RADIUS para o AAA. O IAS pode ser usado em servidores de VPN (Rede Virtual Privada), no serviço de “Roteamento e Acesso Remoto” do Windows Server, ou com outra infra-estrutura de acesso à

rede, como pontos de acesso sem fio e *switches* Ethernet de autenticação. O IAS não necessariamente foi desenvolvido para segurança em redes *wireless*. Mas, como ele lida com questões de criptografia e autenticação, o mesmo foi adaptado para funcionar em redes *wireless* provendo a troca dinâmica das chaves WEP mediante *login* e senha dos usuários.

O IAS permite que chaves WEP de alta segurança sejam atribuídas dinamicamente aos computadores cliente que executam o Windows XP durante a autenticação por certificados. Além disso, as chaves WEP podem ser atualizadas em intervalos regulares para impedir que sejam descobertas por ferramentas de ataque.

Existe ainda o protocolo WPA, que é um subconjunto do próximo padrão de segurança 802.11i para WLAN (*Wireless LAN*) baseado no 802.11. Ele inclui criptografia avançada, criada para solucionar problemas de segurança com o WEP. Os produtos ativados para funcionarem com o WPA não estão totalmente disponíveis e, assim, por enquanto a solução se concentra na utilização do WEP mesmo.

4.1 DECIDINDO SOBRE A FORMA DE AUTENTICAÇÃO

A Microsoft oferece suporte original a vários tipos de protocolos de autenticação de modo que eles sejam usados com o 802.1X. O mais comum é que as empresas selecionem métodos de autenticação do cliente WLAN baseadas em senha ou em certificado.

A seleção do método de autenticação necessário para uma empresa pode ter um efeito significativo sobre a infra-estrutura que a solução escolhida exige. O padrão 802.1X utiliza um esquema de autenticação conectável denominado EAP que é um protocolo genérico que permite que os pontos de acesso à rede suportem múltiplos métodos de autenticação.

4.1.1 Selecionando autenticação baseada por usuário e/ou computador

A autenticação do usuário é uma opção natural quando se considera a identificação para a infra-estrutura de WLAN. No entanto, na maioria dos casos, talvez a organização prefira implementar uma autenticação do computador (ou dispositivo) para garantir uma solução completa.

Existem vários recursos no Windows XP Professional que só funcionarão corretamente com uma conexão de rede ativa. A utilização da autenticação do computador 802.1X garante que essa conexão de rede seja estabelecida durante uma sequência de inicialização e antes que os usuários finais vejam a tela inicial de *logon* do Windows. A

Tabela 1 mostra as diversas situações no Windows XP que requerem a autenticação do computador.

Tabela 1 - Considerações para a autenticação do computador

Recurso	Situação que requer a autenticação do computador
Diretiva de Grupo de computador com o Active Directory	A Diretiva de Grupo baseada em computador é aplicada durante a inicialização do computador e em intervalos de tempo regulares, mesmo quando ninguém tenha feito logon no Windows.
Scripts de logon de rede	Os scripts de logon de rede são executados durante o logon inicial do usuário.
Agentes de gerenciamento de sistemas	Os agentes de aplicativo do gerenciamento de sistemas, como aqueles que acompanham o Microsoft SMS (Systems Management Server), em geral, precisam de acesso à rede sem a intervenção do usuário.
Conexão da área de trabalho remota	É possível acessar os computadores pela Conexão da área de trabalho remota quando ninguém tiver feito logon no Windows.
Pastas compartilhadas	Os arquivos e pastas compartilhados de um computador ainda se encontram disponíveis mesmo quando nenhum usuário tiver feito logon.

A melhor estratégia é usar a autenticação por usuário, quando possível, e a autenticação por computador, quando necessário. Esta orientação é baseada no comportamento padrão do cliente 802.1X no Windows XP Professional. Esse comportamento é usado para executar a autenticação do computador quando os usuários não tiverem feito *logon*, a autenticação do usuário quando eles fazem *logon* no Windows e novamente a autenticação do computador quando os usuários fazem *logoff*. Isso garante que o acesso à rede utilize as credenciais de conta do usuário, onde for possível o uso de contas, garantindo ainda que os recursos do Windows que requerem o acesso à rede funcionem corretamente.

4.1.2 Determinando os requisitos da autorização de rede

Os principais objetivos da criação de diretivas de gerenciamento de acesso à rede incluem a correspondência de diretivas de segurança organizacional, feita da forma mais estrita possível ao mesmo tempo em que minimiza o custo do gerenciamento. Uma representação centralizada da diretiva de autorização de rede, como as diretivas de acesso remoto IAS, é bem adequada à tarefa.

4.1.3 Determinando critérios de conexão

As diretivas de acesso remoto podem validar várias configurações de conexão antes de autorizar a conexão, inclusive os seguintes critérios:

- Permissão de acesso remoto
- Participação em um grupo
- Tipo de conexão
- Horário
- Métodos de autenticação

Além disso, podem ser usadas as seguintes condições avançadas:

- Identidade do servidor de acesso
- Número de telefone do cliente de acesso ou endereço MAC (*Media Access Control*)
- Se as propriedades de discagem da conta de usuário forem ignoradas
- Se o acesso não autenticado for permitido

Esta solução usa critérios de conexão IAS baseados no tipo de rede de grupo ou de rede de origem do *Active Directory* em vez de horário, método de autenticação ou outra condição. Isso garante que as diretivas de acesso remoto sejam criadas para um tipo específico de acesso à rede (como sem fio, VPN, cabeado ou dial-up) ou agrupamento de clientes enquanto permanece amplo o suficiente para minimizar a quantidade de diretivas de acesso remoto necessárias.

4.1.4 Determinando restrições à conexão

Após a autorização de uma conexão, as diretivas de acesso remoto podem ser usadas para especificar as restrições à conexão que podem incluir o seguinte:

- Intervalo de tempo limite ocioso
- Tempo máximo da sessão
- Nível de criptografia
- Filtros de pacote IP (Internet Protocol)

Além disso, podem ser aplicadas as seguintes restrições avançadas:

- Endereço IP para conexões do protocolo PPP (Protocolo Ponto a Ponto)
- Rotas estáticas

Tabela 2 - Exemplos de restrições à conexão WLAN

Tipo de grupo de usuários	Exemplo de restrição à conexão
Funcionários que trabalham em período integral	Acesso autenticado e irrestrito à rede corporativa.
Prestadores de serviço e parceiros comerciais	Acesso autenticado e restrito a redes e aplicativos específicos.
Visitantes	Acesso não autenticado apenas a segmentos da Internet para navegação na Web ou acesso VPN de volta à empresa de origem.

Esta solução apenas configura o suporte a funcionários autenticados e que trabalham em período integral. Por essa razão, será necessária uma única diretiva de acesso remoto com perfil de restrição à conexão simplificada. Caso a organização possua outros requisitos, como a necessidade de oferecer suporte ao visitante para acessar a rede sem fio, recomenda-se o uso de diretivas de acesso remoto adicionais.

O que realmente determina a quantidade de diretivas de acesso remoto necessária é a quantidade de tipos diferentes de pessoas que requerem acesso à rede sem fio. Por exemplo, em muitas empresas, os funcionários que trabalham em período integral necessitam de acesso irrestrito à toda rede corporativa. No entanto, talvez os prestadores de serviço e os parceiros comerciais precisem apenas acessar aplicativos específicos em sub-redes de redes específicas.

Os perfis de restrição à conexão são específicos a cada diretiva de acesso remoto. Por isso, se houver necessidade de vários tipos de perfis de restrição à conexão, serão necessárias várias diretivas de acesso remoto. A seleção da diretiva de acesso remoto correta e, portanto, do perfil correto de restrição à conexão baseia-se nos critérios de conexão.

4.2 DETERMINANDO A CRIPTOGRAFIA DE TRÁFEGO COM O WEP

A primeira estratégia para reduzir ameaças ao uso de chaves WEP é garantir que as chaves de sessão do cliente sejam atualizadas em intervalos de tempo inferiores ao tempo necessário para descobrir a chave e capturar o tráfego, executando operações de força bruta. Isso pode ser realizado por meio da funcionalidade de atualização de chave em APs sem fio ou pela definição das opções do RADIUS, de modo que seja aplicada a reautenticação automática do cliente, que inicia a atualização da chave WEP.

Esta solução configura as opções IAS RADIUS de modo que seja aplicada a reautenticação do cliente do Windows XP Professional a cada 10 minutos, garantindo chaves de sessão WEP de curta duração.

Segundo (MICROSOFT 2004, pág 1), a taxa máxima de transferência do 802.11a é de 60% do valor teórico de 54 Mbps (megabits por segundo); deste modo, 32 Mbps corresponde à taxa real de transferência. Isso equivale a 4 Mbps, uma vez que o WEP criptografa apenas pacotes de dados e a média desses pacotes é de 80 bytes. O 802.11 possui cerca de 40 bytes de sobrecarga por pacote de dados, inclusive uma ACK (Mensagem de Confirmação). Portanto, o resultado é de 50.000 pacotes por segundo. Por isso, o tráfego do 802.11a protegido pelo WEP é considerado seguro com um valor de reautenticação de 10 minutos, baseado nos ataques conhecidos.

4.3 USANDO O IAS PARA GERENCIAR O ACESSO À REDE

O planejamento e a implantação de uma infra-estrutura IAS que atenda as necessidades atuais e futuras da organização requerem atenção. O IAS não se destina a fornecer acesso a uma única rede isolada. Ao contrário, ele deve ser implantado para fornecer acesso à rede estratégico para diversas situações de acesso à rede.

4.3.1 Identificando os requisitos da organização de acesso à rede

O IAS do Windows Server 2003 comporta inúmeros cenários de acesso à rede, incluindo:

- **Acesso sem fio.** Pontos de acesso sem fio com capacidade para 802.1X podem ser configurados para dinamizar os serviços de AAA do IAS para o controle de acesso à WLAN de 802.11, bem como fornecer o gerenciamento principal.

- **Acesso por cabo.** *Switches* Ethernet com capacidade para 802.1X podem ser configurados para dinamizar os serviços de AAA do IAS para o controle de acesso por porta em redes locais cabeadas.
- **Acesso por VPN.** Servidores de VPN, como o RRAS para Windows, podem ser configurados para dinamizar os serviços de AAA do IAS para o controle de acesso à rede corporativa, bem como fornecer o gerenciamento principal.
- **Acesso dial-up.** Servidores *dial-up*, como o RRAS para Windows, podem ser configurados para dinamizar os serviços de AAA do IAS para o controle de acesso à rede corporativa.
- **Acesso por extranet.** Servidores de acesso por extranet podem dinamizar os serviços de AAA do IAS ao fornecer aos parceiros comerciais acesso restrito a recursos compartilhados.
- **Acesso terceirizado à rede corporativa.** Provedores de soluções de rede podem dinamizar os serviços de AAA do IAS para integrar a infra-estrutura de rede terceirizada a bancos de dados de contas dos clientes e à diretiva de controle de acesso. O IAS pode fornecer as informações sobre as contas necessárias para cobrar os clientes pelo serviço.
- **Acesso pela Internet.** Os provedores de serviços de Internet podem dinamizar os serviços de AAA do IAS para fornecer acesso à Internet *dial-up* e de alta velocidade ao mesmo tempo em que dinamizam os bancos de dados de contas individuais da organização e a diretiva de controle de acesso. O IAS pode fornecer as informações sobre as contas necessárias para cobrar os clientes pelo serviço.

Para maximizar o investimento no IAS e reduzir a necessidade de alteração futura na infra-estrutura do IAS, devem-se avaliar esses cenários para as organizações. Embora o IAS nesta solução seja utilizado somente para acesso sem fio à rede, a solução pode ser expandida para acomodar cada uma dessas situações.

4.3.2 Usando o IAS para gerenciar o acesso sem fio à rede

Para contornar o primeiro risco de segurança, a organização pode configurar os pontos de acesso sem fio como clientes RADIUS e, em seguida, configurá-los para enviar as solicitações de acesso e as mensagens do acompanhamento de conta para um servidor

RADIUS central com IAS. Para contornar o segundo risco de segurança, pode-se criptografar os dados transmitidos entre os dispositivos sem fio e os pontos de acesso.

O IAS oferece uma segurança aprimorada para WLANs ao funcionar como um servidor RADIUS para pontos de acesso e dispositivos clientes sem fio padrão IEEE 802.1X e fornecendo chaves de criptografia dinâmicas por meio de protocolos de autenticação com base em certificados, como EAP-TLS.

4.3.3 Determinando a função do IAS como servidor RADIUS

Os servidores IAS podem ser implantados para desempenharem uma destas funções conceituais RADIUS:

- Servidor RADIUS
- Proxy RADIUS
- Servidor e proxy RADIUS

A Tabela 3 detalha alguns dos recursos dos servidores configurados para essas funções e identifica sua utilidade em situações reais.

Tabela 3 - Funções do RADIUS IAS

Função do RADIUS IAS	Funções	Cenário
Servidor RADIUS	- Verifica as credenciais diretamente no <i>Active Directory</i>; - Dinamiza o RAP para determinar o acesso à rede.	Necessário em todos os cenários de gerenciamento de acesso à rede.
Proxy RADIUS	- Roteia a solicitação de acordo com suas propriedades; - Pode modificar as propriedades RADIUS das solicitações em trânsito; - Proporciona balanceamento de carga das solicitações RADIUS aos grupos de servidores RADIUS.	- Útil em casos de várias florestas, quando o equipamento de acesso à rede é compartilhado; - Útil para implantação de arquiteturas AAA de rede de <i>front-end/back-end</i> de grande escala.
Servidor e proxy RADIUS	Combinação dos dois recursos anteriores.	Combinação dos dois cenários.

Nem todas as funções do RADIUS são necessárias em todos os cenários de gerenciamento do acesso à rede. Por exemplo, o gerenciamento do acesso à WLAN precisará apenas da função de servidor do RADIUS em muitas organizações. No entanto, se a

organização planeja usar a infra-estrutura de rede sem fio para atender usuários e dispositivos de várias florestas do *Active Directory*, ela precisará também da função de *proxy* RADIUS para rotear as solicitações para servidores RADIUS distintos de cada floresta.

Esta solução inclui servidores IAS configurados somente como servidores RADIUS e não o implementa como *proxy* RADIUS. A Tabela 4 mostra os diversos tipos de autenticação e como são tratadas estas autenticações pelo servidor IAS.

Tabela 4 - Tipos de autenticação

Tipo de autenticação	Comentários
Autenticação inicial do computador	O cliente executa a autenticação completa no IAS.
Autenticação inicial do usuário	O cliente executa a autenticação completa no IAS.
Reautenticação do usuário quando ele passa de um ponto de acesso sem fio para outro	O cliente executa a autenticação completa uma vez em cada servidor IAS e depois usa a reconexão rápida nas demais autenticações.
Reautenticação do dispositivo quando ele passa de um ponto de acesso sem fio para outro	O cliente executa a autenticação completa uma vez em cada servidor IAS e depois usa a reconexão rápida nas demais autenticações.
Reautenticação marcada do computador	O cliente usa a autenticação em <i>cache</i> no IAS.
Reautenticação marcada do usuário	O cliente usa a autenticação em <i>cache</i> no IAS.

4.4 CONFIGURAÇÃO WIRELESS EM AMBIENTE WINDOWS XP

Antes de iniciar o processo de configuração da conexão *wireless* para uma rede com o SSID "e-U", deve-se verificar as configurações TCP/IP da ligação *wireless*. Selecionar a opção "**Properties**". Com o botão direito do mouse sobre a conexão *wireless*. A Figura 2 apresenta uma tela de exemplo destas opções.

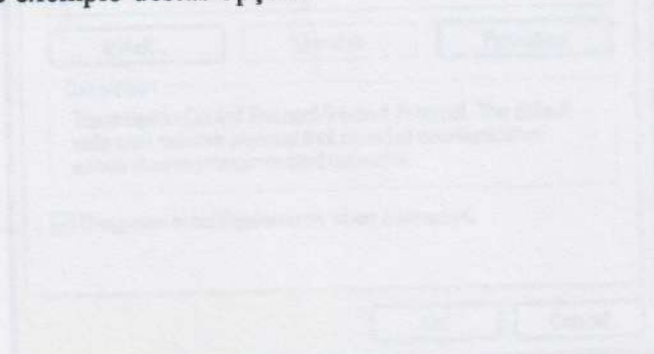


Figura 2 – Tela de exemplo das opções de configuração de rede

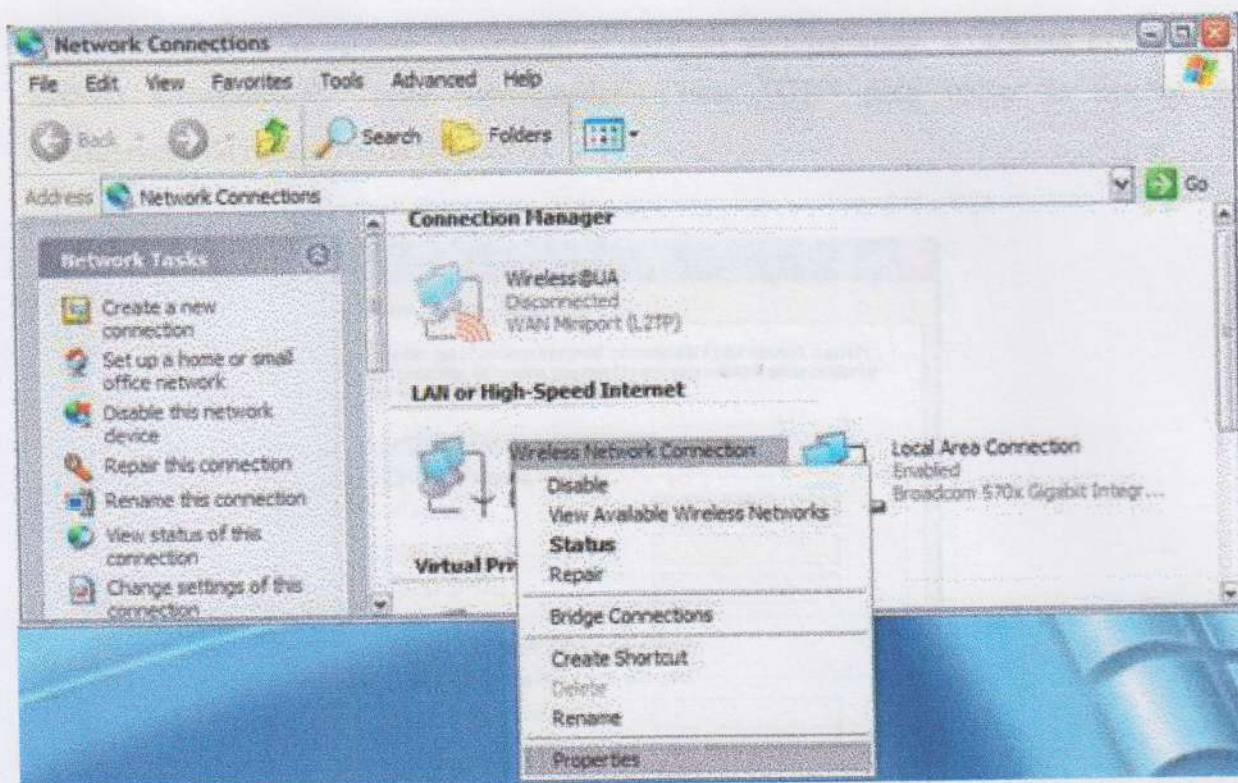


Figura 2 - Menu de uma interface de rede wireless no Windows XP

Na aba "**General**" selecionar "**Protocolo Internet Protocol (TCP/IP)**" e clicar no botão "**Properties**" (Figura 3).

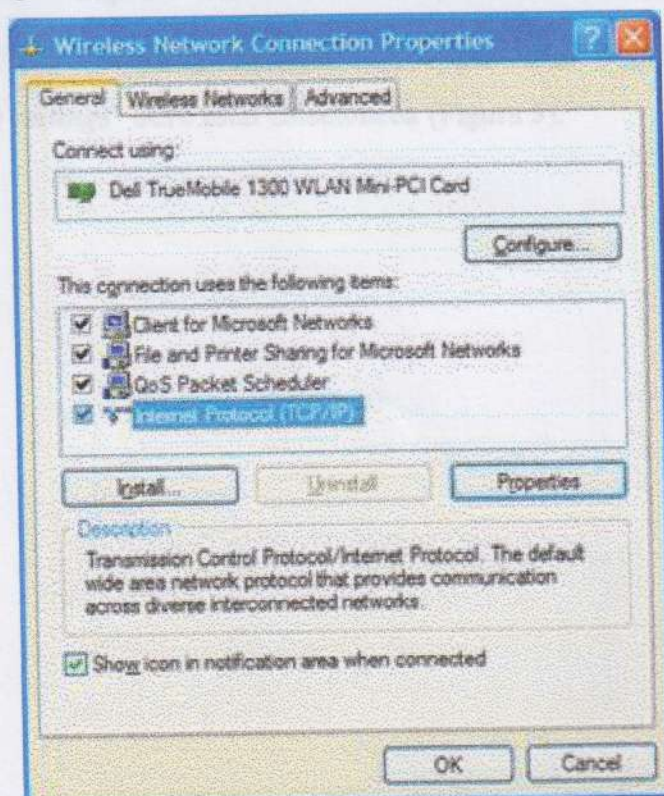


Figura 3 – Verificando as opções de endereços IP

Verificar se as opções "*Obtain an IP address automatically*" e "*Obtain DNS server address automatically*" estão seleccionadas. Clicar "OK" para voltar às opções de configuração da rede *wireless* (Figura 4).

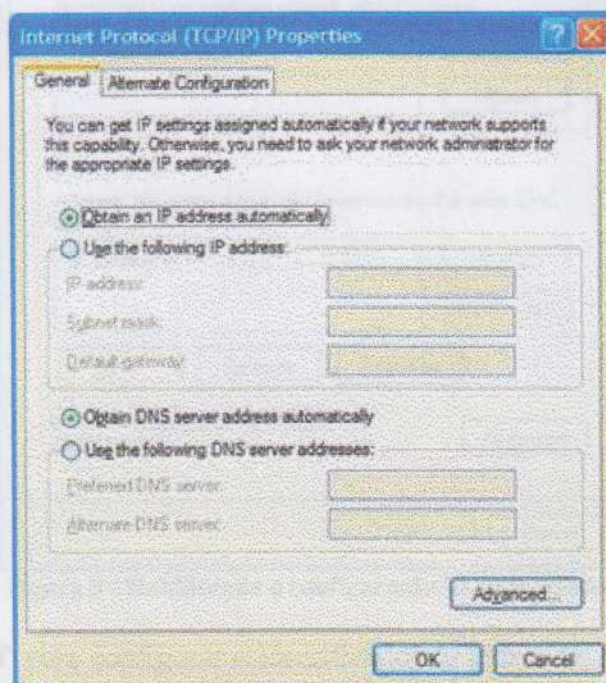


Figura 4 - Colocando os endereços automáticos

Seleccionar a aba "*Wireless Networks*". A opção "*Use Windows to configure my wireless networking settings*" deve estar seleccionada (Figura 5).



Figura 5 - Mantendo a opção WPA

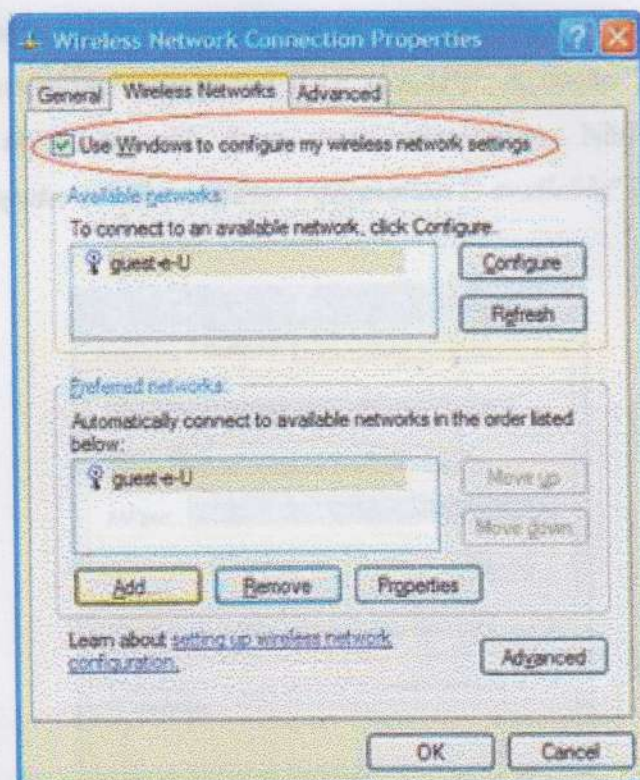


Figura 5 - Habilitando a configuração da rede wireless

Clicar em "Add" para configurar o identificador da rede *e-U*. Preencher o identificador de rede em "Network name (SSID)" com o valor *e-U*. Na opção "Network Authentication", selecionar Open e em "Data Encryption" a opção "WEP". A opção "The key is provided for me automatically" deve estar selecionada (Figura 6).

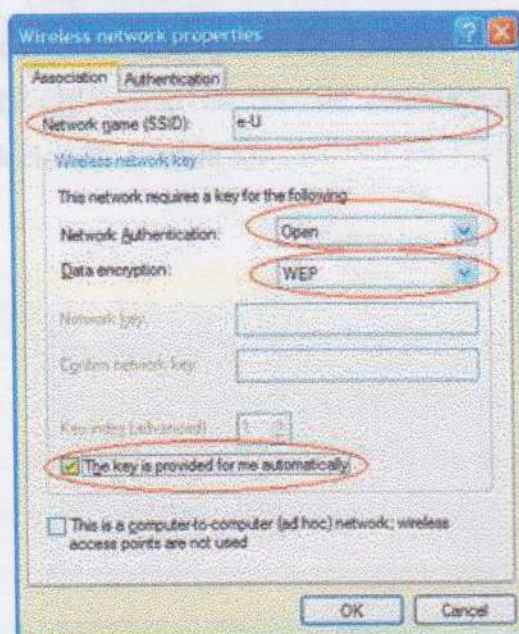


Figura 6 - Habilitando a chave WEP

Para configurar a componente de autenticação selecionar Tab "**Authentication**". Na opção "**EAP Type**" selecionar "**Protected EAP (PEAP)**". A opção "**Enable IEEE 802.1x authentication for this network**" deve estar selecionada. Não selecionar a opção "**Authenticate as computer when computer information is available**" (Figura 7).

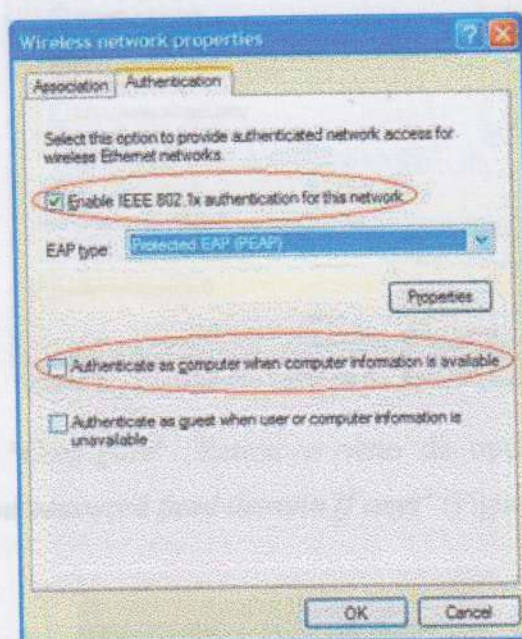


Figura 7- Configurando o componente de autenticação

Clicar em "**Properties**" para configurar as opções do protocolo de Autenticação.

Selecionar a opção "**Validate Server Certificate**". Na lista "**Trusted Root Certification Authorities**", escolha a entidade certificadora "**GTE CyberTrust Root**". Selecionar "**Secured Password (EAP-MSCHAP-v2)**" como método de autenticação. A opção "**Enable Fast Reconnect**" deve estar selecionada (Figura 8).

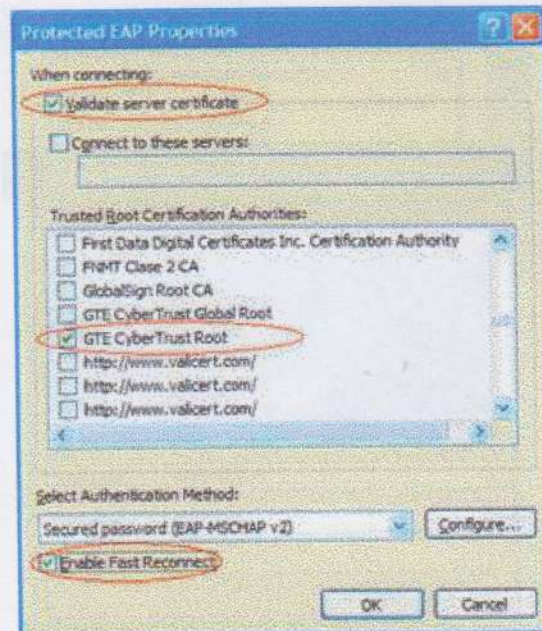


Figura 8 - Escolhendo Método de Autenticação

Clicar no botão "Configure". Retirar o visto da opção "Automatically use my Windows logon name and password (and domain if any)" (Figura 9).

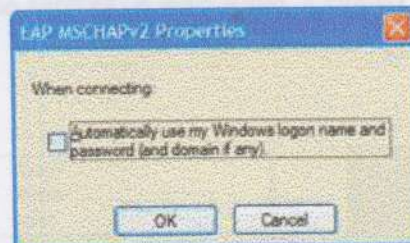


Figura 9 - Retirando o visto de logon automático

Clicar "OK" em todas as janelas abertas, para concluir a configuração do identificador da rede e-U. Quando concluir as configurações, é possível autenticar-se na rede wireless por 802.1X.

4.4.1 Processo de autenticação 802.1X

Uma vez completo o processo de configuração, deverá aparecer uma indicação no canto inferior direito com a seguinte instrução: "Click here to select a certificate or other credentials for connection to the network e-U".

Clicar em qualquer zona do aviso para aparecer o pedido de login e password. Inserir o login e password da conta de acesso do sistema de autenticação central da UA. Selecionar "OK" (Figura 10).

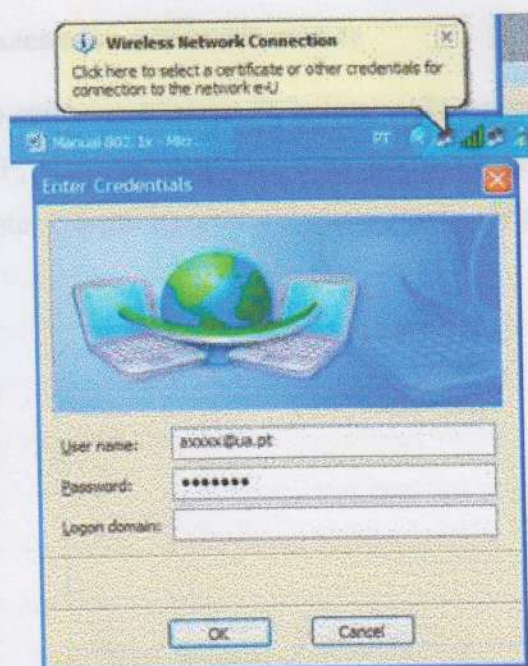


Figura 10 - Tela de Logon do Windows

Para confirmar o sucesso da autenticação, clicar com o botão do lado direito no ícone da ligação Wireless na barra de tarefas, e seleccionar a opção **"Open Network Connections"** (Figura 11).



Figura 11 - Abrindo a conexão da rede

No painel **"Details"**, verifica-se o sucesso da autenticação, **"Authentication succeeded"** (Figura 12).



Figura 12 - Verificando o sucesso da autenticação

5. CONCLUSÃO

4.4.2 Credenciais armazenadas automaticamente

E por fim, após o primeiro sucesso de autenticação na rede wireless e-U, o sistema operacional Windows XP, armazena automaticamente as credenciais (*login/password*) da conta. Nos acessos seguintes o *login* e *password* não voltam a ser pedidos.

5 CONCLUSÕES

Esta monografia envolveu o estudo de protocolos e técnicas de Controle de Acesso para as redes sem fio, mostrando também formas de ataques a estas redes.

Baseando-se especificamente no protocolo 802.1x, uma tecnologia muito recente, não conseguimos informações ao que se refere a resultados em seu uso, mas conseguimos muitas informações valiosas especificando a segurança no controle de acesso.

No início da monografia, mostramos a insegurança que afeta cotidianamente as redes *Wireless*, no entanto no decorrer da pesquisa, analisamos várias formas de se proteger usando tecnologias de controles de acesso, tecnologias essas que nos proporcionam além de tudo uma melhor administração de tais redes.

Os protocolos estudados e citados acima, são facilmente encontrados nos Sistemas Operacionais Windows Servers e máquinas XP clientes, mas é necessário um bom conhecimento para administrá-los e configurá-los.

Assim sendo, chegamos à devida conclusão de que quanto mais essas tecnologias avançam, mais temos que nos aperfeiçoar nos métodos de segurança, por isso, com essa monografia conseguimos aprender que só com o uso de várias tecnologias integradas como as apresentadas aqui, é que se pode garantir um nível mais alto de proteção, pois temos que estar sempre um passo a frente das pessoas mal intencionadas visando impedi-las de qualquer ação.

REFERÊNCIAS BIBLIOGRÁFICAS

- ATMEL. **SEGURANÇA** em Redes Wireless. Disponível em: <http://www.atmel.com/dyn/products/product_card.asp?part>. Acesso em: 20 de Agos. 2003.
- ARCOMANO, R. *WIRELESS How?*. Disponível em: <<http://tldp.org>>. Acesso em: 02 abr. 2003.
- AIRDEFENSE White Paper. *WIRELESS LAN Security – What Hackers Know That You Don't*. Disponível em: <<http://www.airdefense.net>>. Acesso em: 02 abr. 2003.
- DORMAN, A. **WIRELESS** Communication – Rio de Janeiro, Campus, 2001.
- FABRÍCIO A. S., THAIS R. M. B., LINNYER B. R., et all. **TECNOLOGIA** de Novos Sensores Sem Fio. 2003 – Relatório técnico DCC/UFGM 001 / 2003.
- MENEZES, A.; OORSCHOT, P.; VANSTONE, S. **HANDBOOK** of applied Cryptography – California, CRC Press, 1996.
- MICROSOFT, **PROJETANDO** segurança de lan sem fio usando 802.1x: <<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod172.msp>> Acesso em: 18 Nov. 2004.
- MICROSOFT, **MICROSOFT** Windows Server 2003 Resource Kit: <<http://www.microsoft.com/windowsserver2003/techinfo/reskit/resourcekit.msp>> Acesso em: 19 Nov. 2004.
- MICROSOFT, **MICROSOFT** Windows Server 2003 Deployment Kit: <<http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.msp>> Acesso em 19 Nov. 2004.
- MURILLO, N. **SEGURANÇA** Nacional, Novatec Editora Ltda., 2002.
- PEIKARI, C. e FOGIE S. *WIRELESS Maximum Security*, Sams, 2002
- PERRIC, A; SZEWCZYK, R TYGAR, J.D.; et all. **SECURITY** Protocols form Sensor Networks. Wireless Networks 8. Netherlands: Kluwer Academic Publisher, 2002.
- VOLBRECHT, J. e MOSKOVITZ, R. *WIRELESS LAN Access control and Authentication*: <<http://www.interlinknetworks.com>> Acesso em: 02 abr. 2003.
- WADLOW, T. A. **SEGURANÇA** de redes .Projeto e gerenciamento de redes seguras – Rio de janeiro, Campus, 2000.
- WOOD, A. D.; STANKOVIC, J. A. **DENIAL** of Service em sensor Networkks – IEEE Computer, Outubro de 2002.

WI-FI alliance, **SOLUÇÕES WLAN:** <<http://www.wi-fialliance.org>> Acesso em 10 Nov. 2004.

WLANA, **PROGRAMAS** de treinamento: <http://www.wlana.org/learning_center.html> Acesso em 11 Nov. 2004.