

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

USO DO PROTOCOLO 802.1X EM REDES LOCAIS SEM FIO (WLAN)

USO DO PROTOCOLO 802.1X EM REDES LOCAIS SEM FIO (WLAN)

Monografia apresentada ao curso de
Especialização em Redes de Computadores da
Faculdade Natalense para o Desenvolvimento
do Rio Grande do Norte como requisito
parcial para a obtenção do título de
Especialista em Redes de Computadores.

André Felipe Carvalho de Oliveira

Orientador:

Aluizio Ferreira da Rocha Neto

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

USO DO PROTOCOLO 802.1X EM REDES LOCAIS SEM FIO (WLAN)

ANDRÉ FELIPE CARVALHO DE OLIVEIRA

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto

RB 30292
FARN
BIBLIOTECA
Nº Reg M000756
14,12 07

M
004.72
B45u
2007
ex01

Ficha Catalográfica

OLIVEIRA, André Felipe Carvalho

Uso do Protocolo 802.1X em Redes Locais Sem Fio (Wlan). André Felipe Carvalho. - Natal: FARN, 2007.
38 f

p.

Orientador: Aluizio Ferreira da Rocha Neto, M.Sc.

Monografia (Pós-Graduação em Redes de Computadores) - Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – monografia. I. Título

RN/FARN/BC

CDU

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

*União este trabalho ao meu Deus, Senhor de toda sabedoria, único Onipotente, pois,
o seu poder e divindade são presentes e perceptíveis em tudo o que foi criado. Único
Onipotente, detentor de todo o poder e força. Onipotente, pois, toda «ilusão» provém da tua
sabedoria que esparges nos homens.*

USO DO PROTOCOLO 802.1X EM REDES LOCAIS SEM FIO (WLAN)

ANDRÉ FELIPE CARVALHO DE OLIVEIRA

Monografia apresentada e aprovada em 19 de outubro de 2007, pela banca examinadora
composta pelos seguintes membros

Aluízio Ferreira da Rocha Neto, M.Sc.
Orientador

Gleydson Azevedo Ferreira de Lima, M.Sc.
Examinador

DEDICATÓRIA

Dedico este trabalho ao meu **Deus**, Senhor de toda sabedoria, único **Onipresente**, pois, o seu poder e divindade são presentes e perceptíveis em tudo o que foi criado. Único **Onipotente**, detentor de todo o poder e força. **Onisciente**, pois, toda ciência provém da sua sabedoria que esparge nos homens.

Ao professor Aluísio, pela colaboração com os conhecimentos necessários ao desenvolvimento deste trabalho.

Aos colegas de curso, pelo companheirismo demonstrado.

AGRADECIMENTOS

Aos meus familiares, pelo apoio, compreensão e carinho.

A instituição, coordenadores e corpo funcional. *Aos professores*, os quais ao longo do curso foram verdadeiros colaboradores.

Ao professor Aluizio, pela colaboração com os conhecimentos necessários ao desenvolvimento deste trabalho.

Aos colegas de curso, pelo companheirismo demonstrado.

RESUMO

Considerando a questão da comunicação em redes wireless, o padrão IEEE 802.1X, é conceituado como uma solução que define, em relação ao aspecto segurança, o controle de entrada à uma rede de computadores fornecendo o acesso de forma autenticada. Neste sentido, esta pesquisa contempla o uso do padrão 802.1X em redes locais sem fio (wlan), tendo como objeto de estudo o processo de autenticação com criptografia de alta segurança. De forma que, busca compreender o processo, como também, até que ponto a solução corrige os problemas para o acesso às redes sem fio e suas vulnerabilidades em relação a segurança na comunicação.

Palavras-chaves: redes sem fio, segurança, autenticação

ABSTRACT

Relating to the issue of communication in wireless networks, the IEEE 802.1X pattern is considered a solution that defines, concerning to security viewpoint, the entering control into a network of computers by offering authenticated access. In this sense, this research contemplates the use of 802.1X in wireless local network (WLAN) focusing the study of the high security cryptography authentication process pursuing to comprehend the whole process as well as up to what point this solution corrects the problems of access to wireless networks and their vulnerabilities relating to communication security.

Key-words: wireless, security, authentication

LISTA DE FIGURAS

Figura 1: Elementos do sistema de autenticação	27
Figura 2: Troca de Mensagens Estação/Switch/Servidor de Autenticação	28
Figura 3: Funcionamento do RADIUS	29
Figura 4: Troca de Mensagens Estação/AP/Servidor de Autenticação	30

1.2.2 Objetivos Específicos	12
1.3 JUSTIFICATIVA	13
2. REFERENCIAL TEÓRICO	14
2.1 CARACTERIZAÇÃO E CONTEXTUAÇÃO DAS REDES WIRELESS	14
2.1.1 Padrões de Uso em Redes Wireless	14
2.2 SEGURANÇA EM REDES WIRELESS	17
2.2.1 Autenticação e Criptografia	21
2.3 O PADRÃO 802.1X	23
2.3.1 Funcionamento do Padrão 802.1X	26
2.4 O PROTOCOLO RADIUS	28
2.4.1 Integração com o 802.1X	29
2.5 FRAGILIDADES DO PADRÃO 802.1X	30
3. DESENVOLVIMENTO	32
3.1 CONFIGURAÇÕES DE SOFTWARE PARA WLANS COM 802.1X	32
3.2 O PROCESSO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO	32
3.3 VULNERABILIDADES DA SOLUÇÃO 802.1X	34
4. CONCLUSÃO	36
5. FONTES BIBLIOGRÁFICAS	37

SUMÁRIO

1	INTRODUÇÃO	10
1.1	PROBLEMA DE PESQUISA.....	11
1.2	OBJETIVOS	12
1.2.1	Objetivo Geral.....	12
1.2.2	Objetivos Específicos	12
1.3	JUSTIFICATIVA.....	13
2	REFERENCIAL TEÓRICO	14
2.1	CARACTERIZAÇÃO E CONCEITUAÇÃO DAS REDES WIRELESS	14
2.1.1	Padrões de Uso em Redes Wireless.....	14
2.2	SEGURANÇA EM REDES WIRELESS	17
2.2.1	Autenticação e Criptografia	21
2.3	O PADRÃO 802.1X	23
2.3.1	Funcionamento do Padrão 802.1X.....	26
2.4	O PROTOCOLO RADIUS.....	28
2.4.1	Integração com o 802.1X.....	29
2.5	FRAGILIDADES DO PADRÃO 802.1X	30
3	DESENVOLVIMENTO	32
3.1	CONFIGURAÇÕES DE SOFTWARE PARA WLANS COM 802.1X	32
3.2	O PROCESSO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO.....	32
3.3	VULNERABILIDADES DA SOLUÇÃO 802.1X.....	34
4	CONCLUSÃO	36
	REFERÊNCIAS BIBLIOGRÁFICAS	37

1 INTRODUÇÃO

Inegavelmente, os serviços baseados na tecnologia de rede sem fio já fazem parte do nosso dia-a-dia há um bom tempo. Basta citar as conexões sem fio mais comuns, tais como controle remoto e telefones celulares. Dentre esses serviços, as redes *wireless* (do inglês, sem fio) tornaram-se também uma realidade como alternativa às redes convencionais, ou seja, com cabeamento (fibra ótica ou cobre) que complementam e fornecem as mesmas funções destas, destacando-se porém, a sua conveniência, praticidade e mobilidade, como solução, onde uma estrutura convencional não pode ser utilizada.

A conveniência da utilização das redes sem fio em ambientes como aeroportos, *shoppings*, instituições educacionais, hotéis, é caracterizada, à medida da sua mobilidade de comunicação em qualquer lugar e a qualquer momento, o que sob esse aspecto, torna-se evidente a sua praticidade como uma solução complementar às redes estruturadas.

Do ponto de vista comercial pode-se constatar em linhas gerais, benefícios que refletem a melhoria da produtividade funcional proporcionando um fluxo de negócios mais rápido à medida que funcionários que se deslocam externamente economizam tempo, caracterizando flexibilidade no processo de trabalho, promovendo redução de custos. Dessa forma, as redes sem fio quebram as fiações que prendem funcionários ao ambiente físico, pois, sem fios, os escritórios podem estar em qualquer lugar.

Porém, com todas essas vantagens e comodidade, a adoção de redes sem fio traz a preocupação com a segurança da informação, considerando que esta abrange um complexo de fatores desejáveis para uma comunicação segura. Nesse sentido, acessos indevidos, leitura ou alteração de dados em trânsito são alguns dos diferentes tipos de ameaças que transitam nas redes sem fio, às quais os recursos de segurança são considerados precários caracterizando uma vulnerabilidade na transmissão de dados. Essas ameaças e riscos implícitos na comunicação em redes *wireless*, requer de fabricantes e pesquisadores de organismos institucionais, soluções que disponibilizem mecanismos para garantir a segurança nas comunicações.

Assim sendo, como propostas, há uma variedade de soluções e, dentre as principais, encontra-se como opção a que se fundamenta na solução 802.1X, no protocolo EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensiva*) e na criptografia Wi-Fi (*Wireless Fidelity – Fidelidade Sem Fio*).

Em linhas gerais, trata-se de uma solução baseada nos padrões do IEEE (*Institute of Electrical and Electronics Engineers – Instituto de engenharia Elétrica e Eletrônica*) - uma das principais instituições de âmbito internacional que promove conferências e publicam periódicos sobre redes - para autenticação do acesso a uma rede sem fio, com a opção de gerenciamento de chaves criptografadas para proteção do tráfego entre o cliente e o hardware de acesso à rede. Essa solução, como outras tantas, objetivam corrigir os pontos vulneráveis à comunicação segura, visando garantir um ambiente com a segurança mais próxima do ideal.

Considerando a questão da segurança na comunicação de redes wireless, a presente pesquisa científica investigou como objeto de estudo a autenticação do padrão IEEE 802.1X com criptografia de alta segurança, sendo este, conceituado como uma solução que define, em relação ao aspecto segurança, o controle de entrada à uma rede de computadores fornecendo o acesso de forma autenticada.

1.1 PROBLEMA DE PESQUISA

Considerando o objetivo de assegurar um ambiente de rede com segurança no tráfego dos dados, necessário se faz compreender quais os requisitos que possam garantir uma comunicação segura. Nesse sentido, segundo Kurose & Ross (2003 p. 441), intrínseco está o *sigilo, autenticação e integridade da mensagem*. De modo que, em se tratando de sigilo significa dizer que, somente o *remetente e o destinatário* pretendido devem entender o conteúdo da mensagem. Consideram ainda, que o aspecto *sigilo* é, provavelmente, o significado mais percebido em ‘comunicação segura’.

Do ponto de vista de autenticação, entendem que o *remetente* e o *destinatário* precisam confirmar a identidade da outra parte envolvida na comunicação, ou seja, confirmar que a outra parte é, quem realmente diz ser. Em razão de que na comunicação em redes, as entidades comunicantes trocam mensagens por um meio que não podem ‘ver’ a outra parte, sendo necessário técnicas de autenticação no sentido de provar a identidade a alguém.

Quanto a integridade da mensagem inserem que, mesmo que o *remetente* e o *destinatário* consigam se autenticar reciprocamente, eles querem assegurar que o conteúdo da mensagem não seja alterado no tráfego ou por acidente ou má intenção.

Compreende-se então, à luz desse fundamento que as propriedades desejáveis de uma comunicação segura estão relacionadas ao *sigilo, autenticação e integridade*. Assim sendo,

como estruturar um ambiente de rede sem fio que comporte essas propriedades de modo a deixá-lo com a segurança mais próxima da ideal?

Entende-se, que uma solução que se proponha a corrigir as vulnerabilidades de segurança na comunicação de redes sem fio, certamente, vai depender de conceitos de autenticação e criptografia, nesse sentido, até que ponto a solução proposta como objeto de estudo atende a esses requisitos? Como se dá o processo de autenticação com criptografia na solução proposta? A solução proposta, corrige problemas de segurança para o acesso às redes sem fios? Quais são as suas vulnerabilidades?

Considerando a pertinência desses interrogativos, caracterizou-se o problema de pesquisa, que teve como pergunta de partida: Qual a redução dos riscos em relação às ameaças de segurança oferecida pela solução proposta no Padrão IEEE 802.1X com EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensível*) e na criptografia Wi-Fi (*Wireless Fidelity – Fidelidade*), no controle de acesso à redes wireless (sem fio).

Nesse sentido, investigou-se a solução proposta, seus recursos e benefícios, tendo como guias de condução os objetivos a seguir relacionados.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Constatar a redução dos riscos em relação às ameaças de segurança oferecida pela solução do Padrão IEEE 802.1X com EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensiva*) e na criptografia Wi-Fi (*Wireless Fidelity – Fidelidade*), no controle de acesso à redes wireless (sem fio).

1.2.2 Objetivos Específicos

- Descrever as configurações de software para WLANs do 802.1X
- Compreender o processo de autenticação do padrão IEEE 802.1X em redes sem fio;
- Identificar as vulnerabilidades da solução IEEE 802.1X;
- Elaborar um parecer técnico com base nos resultados obtidos;
- Contribuir com a pesquisa científica na área de segurança das informações.

1.3 JUSTIFICATIVA

Em relação a uma rede que utiliza cabeamento convencional, percebe-se que os benefícios atrelados à adoção das redes sem fio trazem muitas vantagens desde o aspecto comercial ao operacional, tendo em vista a conveniência, mobilidade e praticidade inerentes à tecnologia. Contudo, esses benefícios e vantagens imediatamente percebidos, apresentam riscos que podem gerar problemas de ordem complexa relacionados à questão da segurança dos dados trafegados, expondo a rede a ataques de diversas natureza.

Em se tratando de segurança na comunicação em redes, sabe-se que esta evidencia uma natureza complexa e envolve uma série de medidas e, nesse sentido, Rufino (2005), adverte que, em se tratando de redes sem fio esse aspecto se torna ainda mais relevante à medida que a área de abrangência “física” aumenta substancialmente. Em outras palavras, o anteriormente estabelecido e controlado acesso via portaria e/ou recepção e, ainda, a necessidade de obter um ponto de rede cabeada ou acesso a um computador da rede-alvo, agora devem ser pensados em termos de dezenas ou centenas de metros ao redor do ambiente.

Nestas perspectivas, esta pesquisa buscou o conhecimento de uma solução que traz em seu conceito a definição de controles de acesso à redes sem fio, propondo recursos no sentido de reduzir problemas de segurança no tráfego das informações, através do Padrão IEEE 802.1X com EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensiva*) e na criptografia Wi-Fi (*Wireless Fidelity – Fidelidade*).

Neste sentido, almeja-se que este estudo possa contribuir tanto para o meio acadêmico, administradores de redes e usuários domésticos, à medida que contém informações técnicas necessárias para um conhecimento mais complexo do objeto de pesquisa, haja visto que, por serem ainda uma novidade, as redes sem fios demandam a necessidade de maior segurança.

Assim sendo, com o conhecimento mais claro desse cenário, no tocante as suas particularidades e vulnerabilidades em relação a questão segurança, torna-se mais fácil buscar e adequar soluções para minimizar os riscos implícitos, no sentido de criar um ambiente o mais próximo da segurança ideal.

2 REFERENCIAL TEÓRICO

2.1 CARACTERIZAÇÃO E CONCEITUAÇÃO DAS REDES WIRELESS

Conforme afirmação disposta no Tutorial Wireless (2007), as redes sem fio, caracterizam-se por qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Sendo conceituadas como um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Nesta categoria de redes, há vários tipos que são:

- *WLAN (Wireless Local Area Network - Redes Locais sem Fio);*
- *WMAN (Wireless Metropolitan Area Network - Redes Metropolitanas sem Fio);*
- *WWAN (Wireless Wide Area Network Redes de Longa Distância sem Fio -);*
- *WLL (Wireless Local Loop); e*
- *WPAN (Wireless Personal Area Network - Redes Pessoais Sem Fio).*

As aplicações de rede estão divididas em dois tipos: aplicações *indoor* (interior) e aplicações *outdoor* (exterior). Basicamente, se a rede necessita de comunicação entre dois ambientes, a comunicação é realizada por uma aplicação *outdoor* (dois prédios de uma mesma empresa). A comunicação dentro de cada um dos prédios é caracterizada como *indoor*.

No entendimento de Pinheiro (2005), as redes Wireless atualmente constituem-se em uma alternativa às redes convencionais com cabeamento, complementando e fornecendo as mesmas funcionalidades destas de forma flexível e apresentando boa conectividade em áreas prediais ou de campus. No ambiente corporativo, explica o autor, existem diversas aplicações possíveis para as redes wireless, pois estas como outras tecnologias, têm seu lugar dentro da infra-estrutura das redes locais. Sua utilização é justificável onde não é possível instalar o cabeamento convencional como prédios tombados pelo patrimônio histórico; aplicações que envolvam solução de software mais computadores portáteis; acesso a Internet em locais públicos.

2.1.1 Padrões de Uso em Redes Wireless

Tomando por guia a ótica de Rufino (2005), descreve-se nesta seção, uma visão geral dos padrões que orientaram o modelo de uso para redes sem fio, e, posteriormente, atem-se à

solução proposta como temática de pesquisa. Nesse sentido, para as definições de uso de redes sem fio, tem-se como responsável o IEEE (*Institute of Electrical and Electronics – Instituto de Engenharia Elétrica e Eletrônica*), que desenvolveu como pioneiro o padrão denominado IEEE 802.11, reunindo neste, uma série de definições para especificar como deve ser uma comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes. O padrão 802.11 é conhecido como WI-FI (*Wireless Fidelity – Fidelidade em Rede Sem Fio*), em termos de velocidade de transmissão, provê, no máximo, 2Mbps (*megabyte por segundo*) e trabalha com a frequência de 2,4 GHz.

- Padrão 802.11b – definida como a primeira extensão do padrão 802.11 e permite 11Mbps de velocidade de transmissão máxima, porém, pode comunicar-se a velocidades mais baixas, como 5,5,2 ou mesmo 1 Mbps. Opera com frequência de 2,4 GHz e usa somente DSSS (*Direct Sequence Spread Spectrum – Espectro de Extensão de Sequência Direta*), permitindo no máximo 32 clientes conectados. Foi ratificado em 1999 e definiu padrões de interoperabilidade bastante semelhante aos da redes Ethernet. Há limitação em termos de utilização de canais, porém, é considerado o mais popular e com maior base instalada, com mais produtos e ferramentas de administração disponíveis. Contudo, esse padrão chegou ao limite sendo preterido em novas instalações e em atualizações.
- Padrão 802.11a – definido após os padrões 802.11 e 802.11b com o objetivo de resolver os problemas existentes nestes, e tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), mas podendo operar em velocidades mais baixas. Outra diferença é a operação na faixa de 5GHz, uma faixa com poucos concorrentes, porém, com menor área de alcance. Oferece aumento significativo de clientes (64 conectados). O principal problema relacionado a expansão desse padrão foi a incompatibilidade com a base instalada 802.11b, já que utiliza faixas de frequência diferentes.
- Padrão 802.11g - este padrão é mais recente que os comentados anteriormente e equaciona a principal desvantagem do 802.11a, que é utilizar a faixa de 5GHz e não permitir inter-operação com 802.11b. O fato de 802.11g operar na mesma faixa (2,4 GHz) permite até que equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado. Além disso, o 802.11g incorpora várias das características

positivas do 802.11a, como utilizar também modulação OFDM e velocidade a cerca de 54Mb nominais.

- Padrão 802.11i – homologado em junho de 2004, esse padrão diz a respeito a mecanismo de autenticação e privacidade e pode ser implementado em vários de seus aspectos aos protocolos existentes. O principal protocolo de rede definido neste padrão é chamado RSN (*Robust Security Network – Rede de Segurança Robusta*), que permite meios de comunicação mais seguros que os difundidos atualmente. Esta inserido neste padrão também o protocolo WPA (*Wi-fi Protected Access*), que foi desenhado para promover soluções de segurança mais robustas, em relação ao padrão WEP (*Wired Equivalent Privacy*), além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (*Advanced Encryption Standard*).
- Padrão 802.11n - também conhecido como WWiSE (*World Wide Spectrum Efficiency*), este é um padrão em desenvolvimento, cujo foco principal é o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM, conhecida como MIMO-OFDM (*Multiple Out-OFDM*). Outra característica deste padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 Mhz e, também, manter compatibilidade com os 20MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135Mbps.
- Padrão 802.1X - mesmo não sendo projetado para redes sem fios, o padrão 802.1X, possui características complementares a essas, pois, permite autenticação baseada em métodos já consolidados como o RADIUS (*Remote Authentication Dial-in User Service*), de forma escalável e expansível. De maneira que, é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discadas etc.), e manter a base de usuários em um repositório único, quer seja em banco de dados convencional, ou qualquer outro reconhecido pelo servidor de autenticação. Esse padrão pressupõe a presença de um elemento autenticador, tipicamente um servidor RADIUS, e um requerente, ou seja, o elemento que requer autenticação, no caso o equipamento cliente. Essa autenticação é feita antes de qualquer outro serviço de rede estar disponível ao usuário requerente.

Mediante a descrição de Rufino (2005), percebe-se nos padrões subseqüentes ao 802.11, que em cada extensão definida, buscou-se corrigir problemas existentes relacionados às características operacionais e técnicas. O que gerou, em determinados casos, incompatibilidade, em outros, a inter-operação desejada no sentido de possibilitar a coexistência com a base já instalada. Nesse sentido, o caráter expansivo dos padrões de uso de rede sem fio, permitiu ao administrador, a possibilidade de combinação de padrões para atender a diferentes demandas, possibilitando assim, uma evolução da base instalada sem muitas implicações.

2.2 SEGURANÇA EM REDES WIRELESS

Os benefícios das redes sem fio são inegáveis tanto do ponto de vista comercial como operacional, conforme já disposto na introdução deste trabalho, o que tem tornado a opção pelas tais, cada vez mais crescente no meio corporativo. Contudo, sua utilização demanda aspectos relevantes relativos à segurança, haja vista, as ameaças e riscos implícitos na transmissão de dados.

Considerando as assertivas de 'Decisão sobre uma Estratégia de Rede sem Fio Protegida', artigo publicado pelo Centro de Orientações de Segurança da Microsoft, "os perigos de transmitir os dados desprotegidos da rede para alguém que esteja nas proximidades podem parecer óbvios, mais ainda existe um número surpreendente de instalações de *WLAN* sem nenhuma segurança ativada". Outra afirmação, diz respeito ao número de diferentes ameaças para as quais os recursos de segurança básicos são vulneráveis, e assim, relaciona e traduz como principais as seguintes:

- Espionagem dos dados transmitidos – que resultam na revelação de dados confidenciais, revelação de credenciais de usuário desprotegidas e potencial roubo de identidade. Também permite que habilidosos usuários mal intencionados coletem informações sobre seus sistemas, as quais podem ser usadas para organizar um ataque a outros sistemas ou dados que poderiam não estar vulneráveis;
- Interceptação e modificação de dados transmitidos – caso um invasor obtenha acesso à rede poderá inserir um computador invasor para interceptar, modificar e retransmitir as comunicações entre duas partes legítimas;

- *Spoofing* (Falsificação) – o acesso imediato à rede permite que um usuário mal-intencionado envie dados que possam parecer provenientes de um usuário legítimo (por exemplo, uma mensagem de email falsa) de maneiras que não seriam possíveis fora da rede. As pessoas (inclusive os administradores de sistema) tendem a confiar muito mais em itens de origem interna do que em algo que se origina fora das redes da empresa;
- *Parasitismo* – o uso que um intruso faz de uma rede como ponto de acesso livre para a Internet. Apesar de não ser tão danosa quanto outras ameaças, essa poderá reduzir o nível de serviço disponível para seus usuários legítimos;
- *DoS (Denial of Service - Negação de Serviço)* – trata-se das muitas opções que um usuário mal-intencionado pode utilizar para inundar uma rede sem fio, que vai desde a interrupção do sinal de rádio que pode ser feita usando coisas de tecnologia tão banal quanto um microondas, como também, ataques mais sofisticados que visam os próprios ‘protocolos sem fio’ de nível inferior e os menos sofisticados que visam as redes, simplesmente inundando a WLAN com tráfego aleatório.

Estas portanto, são consideradas as principais ameaças as quais as redes sem fio estão vulneráveis, entretanto, na visão de Pinheiro (2005), quando configuradas em ataques possuem graus de dificuldade dependentes da características de implantação da rede, o que significa dizer que, para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismo de autenticação de dispositivos e confidencialidade de dados. Nesse sentido, afirma que, a segurança que deve ser adicionada encontra-se ao nível de enlace de dados e que isso se deve ao fato de que os aplicativos e protocolos dos níveis superiores foram desenvolvidos considerando a segurança física disponível nas redes com fios. Assim sendo, recomenda, que o nível de enlace das redes sem fio deve, prover características de segurança que compatibilizem estes dois tipos de conexão e possibilitem a execução de aplicativos sem riscos.

Considerando ainda, o artigo publicado pelo Centro de Orientação de Segurança da Microsoft, consta que, uma solução que possa corrigir o problema de como garantir a segurança das comunicações em rede sem fio, deverá ter os seguintes recursos:

- Autenticação de clientes que deverá ser mútua, o PA (ponto de acesso) sem fio e um servidor RADIUS (*Remote Authentication Dial-in Use Service* -);

- Processo de autorização para determinar quem está autorizado ao acesso à rede sem fio;
- Criptografia de alta segurança no tráfego da rede sem fio;
- Gerenciamento seguro de chaves de criptografia;
- Resistência a ataques de DoS (*Denial of Service – Negação de Serviço*).

Analisando as abordagens mencionadas compreende-se, que as características de implantação de uma rede sem fio é fator determinante de segurança em razão das ameaças que a circundam. Concernente aos recursos para corrigir o problema da segurança, entende-se que estes, devem partir do princípio lógico que para acrescentar segurança a qualquer ambiente é preciso identificar quem chega. Sob esse aspecto, no controle de acesso à redes, a autenticação do usuário está para o que se pode reconhecer como verdadeiro. Em relação a confidencialidade está a criptografia, que cifra a mensagem assegurando que somente as partes comunicantes entendam o conteúdo da mesma.

Nesse sentido, Rufino (2005 p. 40), vem confirmar, expressando que, “*a maneira tradicional de adicionar segurança ao ambiente é promover autenticação do usuário e/ou equipamento que deseja utilizar recursos da rede*”. Insere ainda, que a maioria dos mecanismos de autenticação em redes sem fio baseia-se em senhas fixas, existindo também, outras alternativas, que vão desde a associação com endereços MAC dos equipamentos, senhas dinâmicas, uso de certificados digitais, porém, cada uma, com diferentes níveis de riscos associados.

Parafraseando com o argumento do autor para o uso de criptografia, o mesmo adverte que, independentemente do que a infra-estrutura de rede sem fio local prover, o usuário em algum momento (em trânsito, convenções) poderá encontrar-se em um ambiente completamente aberto e sujeito aos mais variados tipos de ataque.

Explica então, que nessa situação, há dois pontos a ser protegidos: o acesso ao equipamento do usuário e o conteúdo das informações que ele trafegar. Nesse momento, o uso de criptografia poderá resolver o segundo problema, porém, se o atacante conseguir acessar o equipamento do usuário, grande parte da segurança obtida com a criptografia poderá perder-se, já que em geral, as senhas de uso dos sistemas criptográficos ficam armazenadas em meio

magnético (disco rígido, dispositivos de memória etc) ou podem ser capturadas pelo monitoramento das teclas digitadas e/ou dos cliques do mouse.

Mediante esta abordagem, permite-se retornar ao contexto introdutório deste trabalho, especificamente, para ratificar o fundamento teórico que caracterizou o 'Problema de Pesquisa' mediante as propriedades desejáveis de uma comunicação segura. Nesse sentido, segundo Kurose & Ross (2003 p. 441), intrínseco está o *sigilo, autenticação e integridade da mensagem*. Em se tratando de sigilo somente o *remetente e o destinatário* devem entender o conteúdo da mensagem. Consideram ainda, que o aspecto *sigilo* é, provavelmente, o significado mais percebido em 'comunicação segura'.

Do ponto de vista de autenticação, o *remetente e destinatário* precisam confirmar a identidade da outra parte envolvida na comunicação, ou seja, confirmar que a outra parte é, quem realmente diz ser no sentido de provar sua identidade.

Quanto a integridade da mensagem, que o *remetente e o destinatário* consigam se autenticar reciprocamente, assegurando que o conteúdo da mensagem não seja alterado no tráfego ou por acidente ou má intenção.

Dessa forma, entendendo que o *sigilo, autenticação e integridade da mensagem* são requisitos desejáveis para uma comunicação segura e que estes requerem conceitos de autenticação e criptografia, compreende-se, diante das afirmações dos autores, que para se chegar a um ambiente mais próximo da segurança ideal, deve-se então, promover a combinação de ambas.

Compreende-se também, que o controle de acesso à rede está intrinsecamente ligado ao processo de autenticação. Nesse sentido, o reforço na segurança sob esse aspecto é relevante à medida que exige soluções que atendam as necessidades de controle de acesso, para concomitantemente, promover o sigilo das informações através da criptografia. De maneira que, ambas, tornam-se interdependentes às realidades de um ambiente de computação que está sempre em evolução.

2.2.1 Autenticação e Criptografia

Mediante o que teoricamente já foi exposto, compreende-se, que *autenticação* é um processo de identificação do que se pode reconhecer como verdadeiro. Em se tratando então

do acesso à redes, esse processo se dá através de protocolos que dispõem de recursos para prover a segurança no controle de acesso. Esses protocolos, segundo a enciclopédia Wikipédia, são chamados de métodos de EAP (*Extensible Authenticator Protocol – Protocolo de Autenticação Extensível*), constitui-se como uma estrutura do autenticador, que fornece algumas funções comuns e uma negociação do mecanismo desejado do autenticador. Em outras palavras, cada protocolo que usa EAP, define uma maneira de encapsular as mensagens de EAP dentro das mensagens desse protocolo, sendo esse encapsulamento chamado de EAPOL (*EAP sobre LAN*). Assim, considera-se que os métodos de EAP podem fornecer um mecanismo seguro de autenticação.

Atualmente, há aproximadamente 40 métodos de EAP diferentes definidos pelo IETF (*Internet Engineering Task Force - Força Tarefa de Engenharia da Internet*), além de outros específicos, definidos por fabricantes. Dentre esses, considera-se como mais modernos, os que operam em redes sem fio sendo alguns aqui mencionados, quais sejam: EAP-TLS, EAP-SIM, EAP-AKA, PEAP e EAP-TTLS. Prossegue-se então, com definições para os métodos referidos conforme a descrição da Wikipédia.

- **EAP-TLS – (*Transport Layer Security – Transporte em Segurança da Camada*)** – é um padrão aberto do IETF definido em RFC 2716 como protocolo original de autenticação para redes sem fio, considerado um dos padrões mais seguros disponíveis e é suportado por todos os fabricantes da ferragem wireless e do software de LAN incluindo Microsoft.
- **EAP-SIM – (*para a identidade do subscritor da G/M*)** – é usado para a autenticação e a distribuição da chave da sessão usando o sistema global para o módulo móvel da identidade do subscritor das comunicações (G/M) (SIM), é definido em RFC 4186.
- **EAP-AKA – (*para o autenticador de UMTS e o acordo da chave*)** – é usado para a autenticação e a distribuição da chave da sessão usando o módulo móvel universal da identidade do subscritor do sistema de telecomunicações (UMTS) UMTS (USIM), é definido em RFC 4187.
- **PEAP (*EAP-Protected – EAP Protegido*)** – é uma proposta comum pelo Cisco Systems, pelo Microsoft e pela segurança de RSA como um padrão aberto. Está extensamente disponível nos produtos, e fornece a segurança muito boa. É similar no projeto a EAP-TTLS, requerendo somente um certificado do usuário-lado PKI

(*infra-estrutura de chave pública*) criar um túnel seguro de TLS para proteger a autenticação do usuário.

- **EAP-TTLS- (*Tunneled Transport Layer Security – Transporte em Segurança da Camada em Túnel*)** é um protocolo que estende ao EAP-TLS, pois, conforme Rufino (2005), o estabelecimento de uma sessão que utilize este método é muito semelhante, no que diz respeito aos quesitos utilizado no EAP-TLS, principalmente do lado do servidor, porém o cliente não necessita possuir um certificado digital para o estabelecimento da conexão e fechamento do túnel, já que a autenticação, será feita informando uma identificação (login) uma senha. Desta maneira, o método EAP-TTLS serve apenas para estabelecer um túnel criptográfico. Após o túnel ser criado requer-se, então, outro método que fará efetivamente a autenticação.
- **Wired Equivalente Privacy (WEP)** - ainda considerando o argumento de Rufino (2005), é um protocolo que oferece possibilidades de cifração de dados, está totalmente disseminado e presente em todos os produtos que estão em conformidade com o padrão wi-fi. Como utiliza algoritmos simétricos, existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas. A segurança do WEP é composta de dois elementos básicos: uma chave estática, que deve ser a mesma em todos os equipamentos da rede, e um componente dinâmico, que, juntos, irão formar a chave usada para cifrar o tráfego.

O estudo 'Decisão sobre uma Estratégia de Rede sem Fio Protegida', publicado pelo Centro de Orientações de Segurança da Microsoft, afirma que o WEP foi incluído nos produtos baseados no 802.11 por algum tempo e incluem uma estratégia para restringir o acesso à rede e criptografar o tráfego da rede com base em uma chave compartilhada. As desvantagem do WEP incluem a falta de gerenciamento da chave dinâmica e as falhas na implementação da criptografia, que, com o tempo, podem expor as chaves a invasores.

- **Wi-fi Protected Access (WPA)** – para vários aspectos de uma solução de segurança mais robusta, Rufino (2005), argumenta que WPA, atua em duas áreas distintas: a primeira, visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área não coberta efetivamente por WEP) utiliza,

para isso, padrões 802.1X e EAP. De outro modo, pode ser utilizado de diferentes maneiras, incluindo-se apenas os recursos de segurança nativos como também, trabalhar de forma integrada a outras tecnologias, tais como o 802.1X e EAP e certificados digitais. A maneira mais simples de utilizar os recursos nativos é por meio de chaves compartilhadas, pois assim se estabelece negociação entre o cliente e o concentrador, que, ao usar uma chave preestabelecida, faz com que a chave da seção seja trocada periodicamente, de forma configurável.

Considerando as assertivas do estudo 'Decisão sobre uma Estratégia de Rede sem Fio Protegida', publicado pelo Centro de Orientações de Segurança da Microsoft. Referindo-se ao WPA, que o mesmo foi produzido pela Wi-Fi Alliance como estratégia para unificar e aperfeiçoar a segurança usada na rede sem fio. O WPA reúne uma série de recursos de segurança amplamente considerados como sendo métodos mais seguros disponíveis atualmente para proteger as WLANs. O WPA suporta a criptografia robusta, o que torna a descoberta das chaves de criptografia bem menos viável.

Assim, esses são métodos de proteção que podem ser utilizados para promover um ambiente seguro em redes, contudo, entende-se, que esses métodos podem e devem ser combinados, pois, isoladamente não proporcionam um nível de segurança adequado e, nesse sentido, devem ser combinados para que possam ter eficácia.

2.3 O PADRÃO 802.1X

Para apresentar o Padrão 802.1X combinado aos mecanismos de autenticação e criptografia, buscou-se a fundamentação teórica no estudo 'Decisão sobre uma Estratégia de Rede sem Fio Protegida', publicado pelo Centro de Orientações de Segurança da Microsoft. Assim sendo, segundo o referido estudo, descreve-se a seguir as conceituações inerentes às técnicas mencionadas.

Sabe-se que o 802.1X é uma estrutura baseada nos padrões IEEE para autenticar o acesso a uma rede, sendo que seu uso não está limitado às redes sem fio e, na verdade, é implementado em equipamentos de LAN cabeada. Utiliza o EAP como meio de fazer o pacote de conversação da autenticação entre diversos componentes da solução e, opcionalmente, gerenciar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso de rede.

As diferentes soluções de segurança para WLAN (*Wireless Local Area Network - Redes Locais sem Fio*) fundamentadas no 802.1X oferecem tipos diferentes de EAP com níveis variáveis de proteção. Estes incluem tanto soluções baseadas em padrões como soluções proprietárias e estas soluções tem níveis variáveis de suporte entre os fornecedores de sistemas operacionais e de hardware de rede. A autenticação e o acesso a rede fundamentados no 802.1X e no EAP compõem somente parte da solução. Outro recurso significativo de uma solução WLAN é a criptografia do tráfego sem fio. Atualmente, a segurança Wi-Fi é oferecida em duas principais variedades, WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*). Ambas incluem métodos para criptografar o tráfego sem fio entre os clientes sem fio e os APs sem fio.

Os produtos Microsoft mais recentes suportam o WPA e também oferecem um método para usar o WEP com a troca de chave dinâmica para proporcionar alta segurança a WLAN com o uso do hardware de rede existente. Ambas as opções, o WPA e o WEP dinâmico, suportam o uso da autenticação com senha ou certificado usando o 802.1x e o EAP. Assim, não havendo ampla disponibilidade de hardware da WLAN compatível com WAP, o melhor método para lidar com a criptografia Wi-Fi é usar a criptografia WEP de alto nível (128bits) e gerar chave dinamicamente acionando o EAP e o 802.1X. Isso corrige a principal deficiência do WEP.

- **802.1X com EAP e Chaves de Criptografia Dinâmica** - o EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensiva*) é um meio de fazer o pacote de convenção da autenticação entre diversos componentes da solução e gerar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso da rede. Nesse sentido, o EAP como um padrão IETF (*Internet Engineering Taskforce*) para efetuar a autenticação, pode ser usado com uma variedade de diferentes métodos de autenticação com base em senhas, certificados de chaves públicas ou outras credenciais.

De acordo com Rufino (2005, p. 136), a autenticação no modelo TLS é realizada mediante troca inicial de certificados digitais entre o cliente e o servidor de autenticação RADIUS, por intermédio do concentrador. No caso mais simples, conforme o autor, a autenticação mútua é o único elemento adicional, ou seja, baseia-se apenas na comprovação de autenticidade (os certificados do cliente e do servidor foram assinados pela mesma AC) dos certificados apresentados. Quando o RADIUS aceita as credenciais, ele informa ao

concentrador que está permitido o acesso à rede ao equipamento (já que neste caso não há autenticação do usuário).

- **802.1X com EAP-TLS** - o EAP-TLS (*Transport Layer Securit*) de certificado para autenticação de clientes sem fio mutuamente e os servidores RADIUS, usando métodos de criptografia de alta segurança e gerando chaves de criptografia, usadas para proteger o tráfego sem fio. Este é um dos métodos mais populares e seguros de EAP para usar com 802.1X. Ele requer certificados de chave pública no cliente e no servidor RADIUS.

A solução descrita com o uso do EAP-TLS com o 802.1X para autenticar clientes e servidores mutuamente e gerar de forma dinâmica as chaves de criptografia WEP com as definições para troca de chaves WEP. Alguns principais benefícios de uma solução baseada nesta opção são:

- Oferece controle de acesso com base no computador e no usuário para a rede - isso evita, por exemplo, que um usuário não autorizado se faça login em um computador não autorizado e obtenha acesso à rede;
- Permite uma experiência transparente do usuário na rede – ou seja, não existem logons adicionais para o usuário preencher, e isso não resulta em partes da rede potencialmente inacessíveis;
- Permite que o computador seja autenticado na rede mesmo que nenhum usuário tenha feito login. Isso é necessário para permitir que um computador em modo autônomo baixe a Diretiva de grupo e seja gerenciado e monitorado remotamente;
- Isso não causará gargalos na rede, visto que o tráfego da rede não está todo canalizado em um servidor ou em pequeno número de servidores centrais (como no caso da solução VPN);
- Não é proprietário do fornecedor; baseia-se nos padrões IEEE e IETF;
- Oferece um amplo suporte nas plataformas do cliente e fornecedores de rede (windows xp, windows 2003, windows 2000, windows NT versão 4.0, windows 9x, Pocket PC e hardware de rede com certificado Wi-Fi);

- Usa o esquema de autenticação de chave pública, que permite um nível muito alto de segurança, a autenticação é transparente para o usuário e não é suscetível aos problemas de compartilhamento de senha ou adivinhação de senha;
- Foi projetada para WPA;
- Esta abordagem traz com ela alguns requisitos de infra-estrutura, mas eles não são proibitivos para as maiores empresas.
- Comum a maioria das alternativas descritas posteriormente, esta abordagem requer uma infra-estrutura de autenticação de servidores RADIUS e um banco de dados de conta centralizada, como o serviço de diretório Microsoft Active Directory .
- Ao contrario da autenticação com senha, este método requer uma PKI (*infra-estrutura de chave pública*).
- Também existem outros benefícios para a solução no fato de grande parte da infra-estrutura necessária poder ser reutilizada para outros aplicativos como o de acesso remoto, a segurança de rede cabeada e, no caso do componente PKI, criptografia de arquivos logon com cartão inteligente e outros.
- **802.1X com PEAP** – a Microsoft também oferece suporte para usar o 802.1X com outro tipo de autenticação conhecido como PEAP (EAP Protegido). O PEAP foi projetado para portar os tipos de EAP dentro de um canal protegido por TLS e requer um certificado baseado em servidor. O PEAP também gera chaves dinamicamente para criptografar o tráfego sem fio durante o processo de autenticação de senha segura dentro do PEAP. A autenticação por senha do 802.1X é suficiente para as pequenas empresas que atualmente não têm uma infra-estrutura de certificado e não precisam de certificados para outras finalidades.

2.3.1 Funcionamento do Padrão 802.1X

Para mostrar a utilização do padrão IEEE 802.1X definiu-se os elementos envolvidos conforme Silva & Duarte (2003), e, nesse sentido, são as entidades envolvidas:

- Suplicante - a entidade que está solicitando autenticação;
- Autenticador - a entidade que intermedeia a autenticação do suplicante;

- Servidor de Autenticação - a entidade que provê o serviço de autenticação ao autenticador.

No referido estudo, consta, que o serviço de autenticação, determina, mediante as credenciais fornecidas pelo suplicante, as características do acesso obtido. Nesse sentido, a entidade servidor pode ser combinada com o autenticador ou pode ser acessada remotamente, através de rede que o autenticador acesse. O suplicante é representado por um dispositivo sem fio, o autenticador está no AP (*access point – ponto de acesso*) e o servidor de autenticação pode ser um servidor RADIUS localizado na rede cabeada. Toda a transação de autenticação do IEEE 802.1X é feita utilizando-se o EAP sobre LAN, ou seja, encapsulada em mensagens EAP sobre Redes Locais (*EAP over LAN – EAPOL*). Desta forma, quando o suplicante (estação sem fio) tenta a conexão através do AP (autenticador). Assim sendo, o autenticador recebe a solicitação abrindo uma porta para a sessão IEEE 802.1X de autenticação, não permitindo qualquer outro tipo de tráfego. A figura 1 mostra as definições mencionadas.



Figura 1: Elementos do sistema de autenticação

Relativo a negociação, a mesma é visualizada na Figura 2. Nesse sentido, o suplicante somente terá acesso a rede mediante a mensagem EAP-Success. No referido estudo consta ainda que, apesar de vários fabricantes terem incluído suporte ao EAP em seus AP's e placas de rede sem fio, o IEEE ainda não compatibilizou as máquinas de estado do 802.11 e 802.1X. Nesse sentido, há um grupo, o 802.11i, trabalhando para estabelecer um padrão de segurança que tem como principal objetivo tornar a tecnologia confiável o bastante para que seja maciçamente adotada pelo mercado.

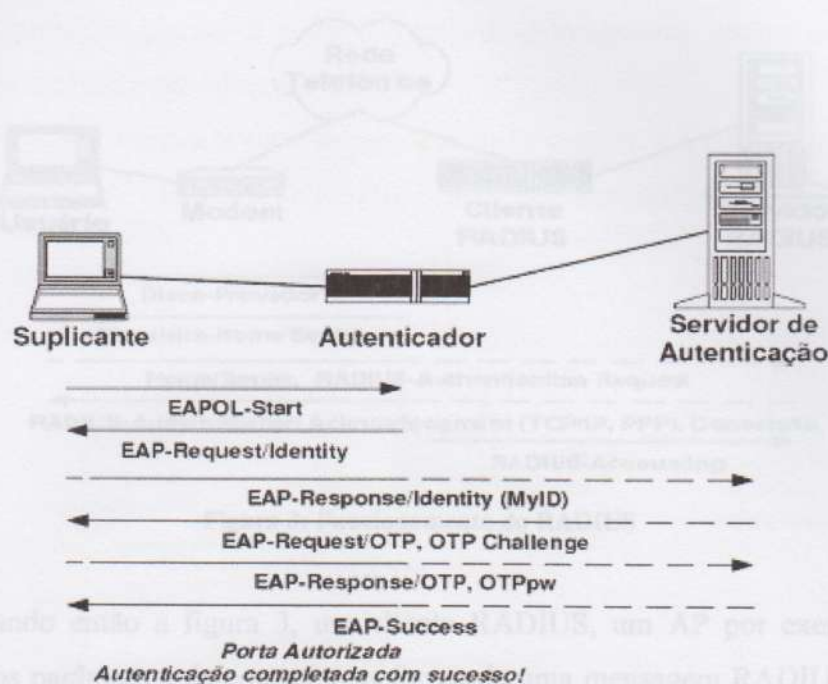


Figura 2: Troca de Mensagens Estação/Switch/Servidor de Autenticação

2.4 O PROTOCOLO RADIUS

Conforme Silva & Duarte (2003), concernente ao RADIUS, trata-se de um protocolo amplamente empregado para disponibilizar acesso a redes com Autenticação, Autorização e Contabilização (*Authentication, Authorization e Accounting - AAA*).

Desenvolvido para uso em serviços de acesso discado, pela sua simplicidade, eficiência e facilidade de implementação hoje é suportado por servidores de VPN, AP's e outros tipos de acesso a redes. As suas características o tornam aplicável a dispositivos embarcados de baixo custo.

Foi descrito pela RFC 2865 e a sua contabilização pela RFC 2866, como também, idealizado para centralizar as atividades de Autenticação, Autorização e Contabilização, visto que o crescente número de sistemas independentes inviabiliza a administração descentralizada.

A Figura 3 mostra o seu funcionamento, à medida que um usuário, através de uma conexão telefônica discada, acessa o Servidor de Acesso Remoto (*Remote Access Server - RAS*) de seu provedor e este requisita-lhe Usuário e Senha. O RAS atua como um cliente do Servidor RADIUS, reencaminhando, Usuário e Senha, agora criptografado com a chave simétrica de que dispõe. O Servidor, após autenticar o usuário, repassa as credenciais relativas às autorizações daquele usuário. O Cliente RADIUS habilita o usuário e passa a transmitir mensagens de contabilização para o Servidor RADIUS.

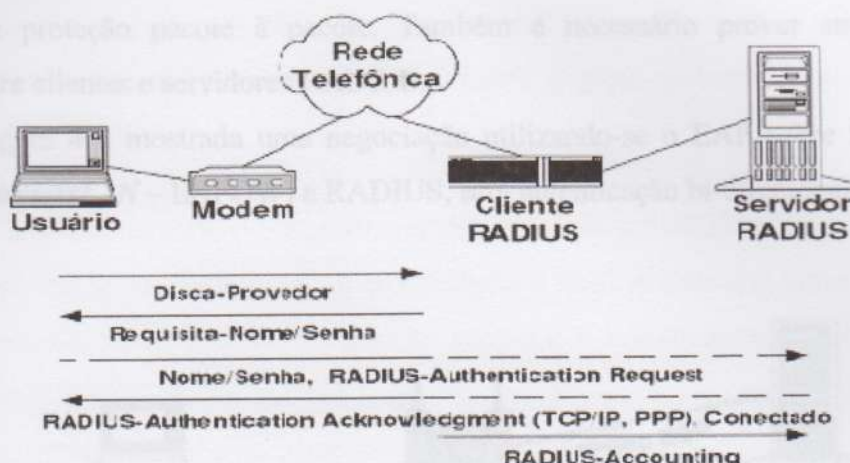


Figura 3: Funcionamento do RADIUS

Explicando então a figura 3, um cliente RADIUS, um AP por exemplo, envia as credenciais e os parâmetros da conexão, na forma de uma mensagem RADIUS, ao servidor. Este servidor autentica e autoriza a requisição ao cliente RADIUS, com o envio de outra mensagem RADIUS. Os clientes também enviam mensagens de contabilização aos servidores RADIUS. A especificação também suporta o uso de procuradores (*proxies*), que nada mais são do que computadores que encaminham mensagens RADIUS entre clientes, servidores e outros procuradores. Um detalhe importante é que as mensagens RADIUS nunca são enviadas entre o cliente do serviço de acesso e o servidor de acesso RADIUS. Outra grande utilidade dos procuradores é o deslocamento (*roaming*), que permite usuários de duas ou mais entidades administrativas serem servidos como se estivessem acessando sua própria rede.

2.4.1 Integração com o 802.1X

Concernente a integração entre o IEEE 802.1X, Silva & Duarte (2003), afirmam que é igualmente tratada em dois documentos distintos, um é a própria norma do IEEE [IEEE 2001], em apêndice não normativo, e outro é a RFC 3580, de caráter informativo. Apesar do IEEE 802.1X não estabelecer um mecanismo padrão para autenticação o RADIUS é considerado, por muitos, um padrão de-facto.

O referido estudo cita que algumas modificações as especificações, tanto de contabilização quanto de autenticação, do RADIUS são tratadas nestes documentos, definindo as alterações necessárias para o seu correto funcionamento. Recomenda que há uma série de considerações relativas à segurança que devem ser feitas, antecedendo a implantação de uma solução IEEE 802.1X/RADIUS. Há um grande número de ameaças relatadas e para solucioná-las é necessário suportar confidencialidade, autenticação na origem dos dados,

integridade e proteção pacote à pacote. Também é necessário prover autenticação bi-direcional entre clientes e servidores RADIUS.

Na Figura 4 é mostrada uma negociação utilizando-se o EAP sobre Rede sem Fio (*EAP over WirelessLAN – EAPOW*) e RADIUS, sem autenticação bi-direcional.

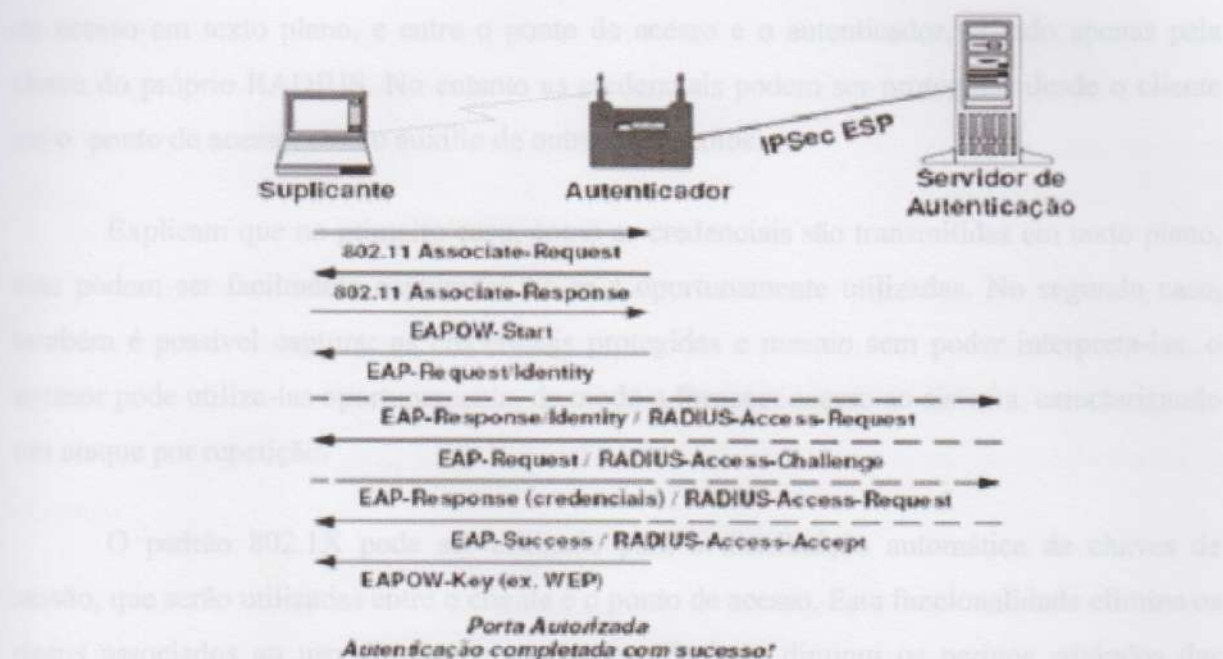


Figura 4: Troca de Mensagens Estação/AP/Servidor de Autenticação

2.5 FRAGILIDADES DO PADRÃO 802.1X

Conforme Silva & Souza (2003), concernente as fragilidades do 802.1X, expõe que o padrão prevê o controle de acesso por porta para toda a família IEEE 802, e também pode ser utilizado para redes locais sem fio.

Nesse sentido, salienta que existe uma grande diferença entre as redes locais sem fio e as demais cabeadas. Nas redes cabeadas explica que a ligação entre o cliente e sua porta de acesso é definida por um cabo fisicamente conectado às duas partes, e no caso das redes locais sem fio, esta ligação é o ar. Desta forma, o padrão falha justamente em não se preocupar com os aspectos de segurança nesta parte da conexão, sendo possível a captura, adulteração e repetição de pacotes de validação.

Como considera um autenticador no processo de autenticação, o ponto de acesso pode tornar-se um repassador de pacotes de autenticação já que toda a base é armazenada no autenticador. Assim, o autenticador pode ser definido no próprio ponto de acesso, porém as

atuais soluções de mercado não têm optado pela implementação dessa funcionalidade nos equipamentos. Pelo contrário tem deixado esta tarefa a cargo de servidores especializados, como servidores RADIUS.,

A validação de usuário e senha através do protocolo RADIUS pode ser utilizada sem mecanismos de cifragem. Neste caso, as credenciais do usuário trafegam entre o ponto de acesso em texto plano, e entre o ponto de acesso e o autenticador, cifrado apenas pela chave do próprio RADIUS. No entanto as credenciais podem ser protegidas desde o cliente até o ponto de acesso, com o auxílio de outros protocolos.

Explicam que no primeiro caso, como as credenciais são transmitidas em texto plano, elas podem ser facilmente capturadas no ar e oportunamente utilizadas. No segundo caso, também é possível capturar as credenciais protegidas e mesmo sem poder interpreta-las, o invasor pode utiliza-las oportunamente, de modo a fornecer acesso ao sistema, caracterizando um ataque por repetição.

O padrão 802.1X pode ser utilizado para a distribuição automática de chaves de sessão, que serão utilizadas entre o cliente e o ponto de acesso. Esta funcionalidade elimina os riscos associados ao uso de chave pré compartilhada, e diminui os perigos advindos das fragilidades do protocolo WEP. Entretanto, neste caso, o mecanismo de troca de chave de sessão deve está associado a processos de reautenticação, com geração e distribuição de novas chaves. Assim, se o invasor consegue credenciais válidas para autenticação, ele poderá receber uma chave de sessão sem maiores dificuldades. Dessa forma, se o processo não estiver protegido por outros protocolos, a chave de sessão poderá ser capturada e utilizada.

Assim, necessário se faz configurar diretivas de acesso remoto, de solicitação de conexão, como também, a diretiva de grupo para computadores cliente. Por fim, torna-se possível configurar a wlan na diretiva de grupo, incluindo configurações para as áreas de configurações gerais, redes preferenciais e propriedades de rede.

3.2 O PROCESSO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO

O processo de autenticação envolve elementos básicos quais sejam: um replicante (dispositivo sem fio que solicita autenticação), um autenticador (ou ponto de acesso habilitado

3 DESENVOLVIMENTO

3.1 CONFIGURAÇÕES DE SOFTWARE PARA WLANS COM 802.1X

No artigo do Centro de Orientações de Segurança da Microsoft (2007), pôde-se verificar que há dois principais componentes da solução baseados em software que devem ser configurados para obter a segurança da wlan no 802.1X, sendo os tais: diretiva de acesso à rede baseada em IAS e diretiva de grupo baseada no active directory para computadores cliente.

A diretiva de acesso à rede baseada em IAS vem a ser a parte essencial da solução de gerenciamento de acesso à rede. As configurações que representam sua política de segurança da wlan são implantadas em cada servidor RADIUS baseado em IAS em modo automatizado. Essa diretiva inclui configurações para diretivas de acesso remoto e diretivas de solicitação de conexão.

Considerando as diretivas de acesso remoto, as mesmas aplicam o acesso às redes por meio de APs sem fio, já as diretivas de solicitação de conexão determinam o tratamento de solicitações RADIUS a partir de vários APs sem fio configurados como clientes RADIUS.

A diretiva de grupo baseada no active directory para computadores cliente, contém todas as configurações que serão implantadas em computadores cliente baseados no Windows XP. Essa diretiva de grupo afeta a interação de clientes com APs sem fio, servidor RADIUS e outras redes sem fio.

Assim, necessário se faz configurar diretivas de acesso remoto, de solicitação de conexão, como também, a diretiva de grupo para computadores cliente. Por fim, torna-se possível configurar a wlan na diretiva de grupo, incluindo configurações para as áreas de configurações gerais, redes preferenciais e propriedades de rede.

3.2 O PROCESSO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO

O processo de autenticação envolve elementos básicos quais sejam: um suplicante (dispositivo sem fio que solicita autenticação), um autenticador (ou ponto de acesso habilitado

para 802.1X) para “mediar” as comunicações antes da atribuição do endereço IP e um servidor RADIUS (provedor do serviço de autenticação) que gerencia o processo.

A operacionalização do processo tem início quando o suplicante tentando acessar a rede alcança o limite de recepção de um autenticador. Este entende que está ocorrendo um pedido de autenticação e envia a solicitação ao servidor RADIUS que solicita as credenciais do suplicante para verificá-las, uma vez que o mesmo é quem especifica o tipo de credenciais necessárias. Essas credenciais podem ser senhas, certificados digitais ou chaves públicas.

O cliente (suplicante) envia suas credenciais ao servidor RADIUS. Se as credenciais forem válidas o servidor enviará uma chave de autenticação criptografada para o autenticador que usa essa chave para transmitir com segurança a sessão de difusão ponto a ponto por estação e chaves de autenticação de difusão seletiva para o cliente sem fio. Contudo, havendo algum problema com as credenciais o servidor poderá instruir o autenticador a restringir o acesso em vários graus conforme a política adotada.

Pertinente se faz mencionar que o software 802.1X deverá estar instalado no dispositivo do usuário final (suplicante), caso contrário, este não poderá “ouvir” a solicitação do autenticador e consequentemente não responderá, o que nesse sentido, o autenticador tratará este usuário como um dispositivo não gerenciado.

Todo o processo é executado através de uma linguagem baseada em padrões EAP (*Extensible Authentication Protocol – Protocolo de Autenticação Extensível*) que é enviada ao autenticador. Convém salientar, que embora o EAP seja um padrão IEEE de autenticação, constata-se também, que existem versões dele, sendo algumas dessas, proprietárias. Nesse sentido, compreende-se que os métodos EAP, torna-se então, um fator a ser considerado, uma vez que, trabalhando como intermediário, o autenticador reempacota as informações EAP para enviar e distribuir ao servidor RADIUS, e dessa forma, todas as boas qualidades do padrão 802.1X vão derivar da utilização do EAP para ampliar a funcionalidade de autenticação, pois, as diferentes versões EAP oferecem diferentes níveis de proteção.

Em se tratando da funcionalidade do processo de autenticação, pode-se afirmar que os protocolos EAP dispõem de recursos para prover a segurança no controle de acesso, como também, no tráfego das mensagens através da criptografia, definindo a forma de encapsulamento das mensagens para propiciar um mecanismo seguro de autenticação. As diferentes versões EAP suportam o uso de autenticação em seus diferentes métodos, seja com

base em senha, certificados de chave públicas ou outras credenciais. Assim, o processo consiste na autenticação do servidor e criação de um canal de criptografia que encapsula mensagens garantindo privacidade aos comunicantes.

Compreende-se então, que o processo de autenticação baseado na solução 802.1X comporta os requisitos que promovem um ambiente seguro à medida que utiliza métodos de proteção que combinados, produzem um efeito eficaz de uma comunicação segura o mais próximo do ideal.

3.3 VULNERABILIDADES DA SOLUÇÃO 802.1X

Verificou-se que existe uma diferença entre as redes locais sem fio e as redes cabeadas. Sendo que nas redes cabeadas a ligação entre o cliente e sua porta de acesso é o cabo fisicamente conectado às duas partes, o que em redes sem fio, esta ligação é o ar. Nesse sentido, é exatamente aí que se configura uma falha do padrão no aspecto segurança, nessa parte da conexão, sendo promovendo a condição para a captura, adulteração e repetição de pacotes de validação.

Tudo isso pode ocorrer através do ponto de acesso (autenticador) que pode tornar-se um repassador de pacotes de autenticação, já que toda a base é armazenada no mesmo. Isso significa dizer que tendo em vista as credenciais serem transmitidas em texto plano, elas podem ser facilmente capturadas no ar e oportunamente utilizadas.

Também é possível capturar as credenciais protegidas por criptografia e, mesmo não podendo interpretá-las, o invasor poderá utilizá-las oportunamente, de modo a fornecer acesso ao sistema, caracterizando um ataque de repetição.

Contudo, verificou-se uma funcionalidade do padrão 802.1X, no sentido de que o mesmo pode ser utilizado para a distribuição automática de chaves de sessão, ou seja, as que serão utilizadas entre o cliente e o ponto de acesso. Essa funcionalidade vem contribuir para eliminar os riscos associados ao uso de chave pré compartilhada, como também, diminuir os perigos advindos das fragilidades do protocolo WEP.

Porém, neste caso, o mecanismo de troca de chave de sessão deverá estar associado a processos de reautenticação, ou seja, com geração e distribuição de novas chaves. Assim, se o invasor consegue credenciais válidas para autenticação, ele poderá receber uma chave de

sessão sem maiores dificuldades. Dessa forma, se o processo não estiver protegido por outros protocolos, a chave de sessão poderá ser capturada e utilizada.

Compreende-se então, que a combinação de protocolos que ofereçam a cifragem dos dados transmitidos devem ser adotados, pois, são recursos que garantem a confiabilidade dos dados, para poder garantir que o tráfego de administração e gerência dos pontos de acesso não seja utilizado para a captura de chaves, credenciais de acesso e nem comprometer a configuração dos pontos de acesso.

Considera-se que os ataques mais comuns em rede sem fio estão relacionados a obtenção de informações sem autorização, acesso indevido a rede e ataques de negação de serviço. Estes possuem diferentes graus de dificuldades dependentes da implantação da rede, sendo, recomendando-se que o uso de aplicativos e protocolos venham a ser combinados para proporcionar um ambiente seguro.

Nesse sentido, concordando-se com o que foi estudado, que é no nível de enlace de dados que deve ser adicionada a segurança, uma vez que os aplicativos e protocolos dos níveis superiores foram desenvolvidos considerando a segurança física disponível nas redes com fio. Assim sendo, recomenda-se, que o nível de enlace das redes sem fio deve, prover características de segurança que compatibilizem estes dois tipos de conexão e possibilitem a execução de aplicativos sem riscos.

Estudo o controle de acesso à rede intrinsecamente ligado ao processo de autenticação, constatou-se que o padrão IEEE 802.1X se configura como uma solução para os problemas de autenticação, e fornece suporte a vários métodos de autenticação existentes. Em relação a sua implementação, a mesma poderá ser feita através de software, hardware ou embarcada em dispositivos específicos que ofereça flexibilidade e interoperabilidade para a integração de componentes e funções.

Considerando os requisitos para uma comunicação segura, pode-se afirmar que o padrão IEEE 802.1X atende aos requisitos básicos de segurança no sentido de autenticidade e integridade dos dados, à medida que, possui recursos que promovem uma negociação segura,

4 CONCLUSÃO

Constata-se que as diversas soluções de segurança para redes sem fio baseadas no 802.1X oferecem tipos diferentes de EAP com níveis variáveis de proteção. Estes abrangem soluções apoiadas em padrões IEEE, como soluções proprietárias e estas variam em seus níveis de suporte entre os fornecedores de sistemas operacionais e de hardware de rede.

O processo de autenticação e acesso a rede baseados no 802.1X e no EAP compõem somente parte da solução, tendo como outro recurso a criptografia do tráfego sem fio, que atualmente é oferecida através de WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*). Ambos incluem métodos para criptografar o tráfego sem fio, entre os clientes sem fio e os APs sem fio.

Considera-se que os ataques mais comuns em rede sem fio estão relacionados a obtenção de informações sem autorização, acesso indevido a rede e ataques de negação de serviço. Estes possuem diferentes graus de dificuldades dependentes da implantação da rede, assim, recomenda-se que o uso de aplicativos e protocolos venham a ser combinados para promoverem um ambiente seguro.

Nesse sentido, concorda-se com o que foi estudado, que é no nível de enlace de dados que deve ser adicionada a segurança, uma vez que os aplicativos e protocolos dos níveis superiores foram desenvolvidos considerando a segurança física disponível nas redes com fios. Assim sendo, recomenda-se, que o nível de enlace das redes sem fio deve, prover características de segurança que compatibilizem estes dois tipos de conexão e possibilitem a execução de aplicativos sem riscos.

Estando o controle de acesso à rede intrinsecamente ligado ao processo de autenticação, constatou-se que o padrão IEEE 802.1X se configura como uma solução para os problemas de autenticação, e fornece suporte a vários métodos de autenticação existente. Em relação a sua implementação, a mesma poderá ser feita através de software, hardware ou embarcadas em dispositivos específicos que oferece flexibilidade e interoperabilidade para a integração de componentes e funções.

Considerando os requisitos para uma comunicação segura, pode-se afirmar que o padrão IEEE 802.1X atende aos requisitos básicos de segurança no sentido de privacidade e integridade dos dados, à medida que, possui recursos que promovem uma autenticação mútua,

através de um ponto de acesso sem fio (PA) e um servidor RADIUS, que através de um processo de autorização usando criptografia de alta segurança, determina quem está autorizado ao acesso à rede. Todo esse processo se dá através dos protocolos EAP que dão provimento de segurança promovendo um ambiente seguro em redes, contudo, entende-se, que esses métodos podem e devem ser combinados, pois, isoladamente não proporcionam um nível de segurança adequado e, nesse sentido, tão somente combinados podem assegurar as melhores práticas para a administração dos pontos de acesso.

Contudo, há de se considerar também, que para as realidades de um ambiente de computação que está sempre em evolução, qualquer que seja o nível de segurança escolhido em rede sem fio, não estará livre de apresentar riscos e vulnerabilidades. Uma vez que, à medida da complexidade da solução adotada, no sentido dos métodos combinados, cada elemento envolvido no processo seja servidor de autenticação, serviços de diretório, banco de dados, enfim, cada um dos tais estará como um elemento de risco em potencial.

Assim, para se obter uma rede sem fio consideravelmente segura, ou seja, um ambiente o mais próximo seguro do ideal, necessário se faz configurar recursos de autenticação e criptografia forte. Convindo salientar, que esses elementos não fazem parte da configuração básica, e a combinação deles requer tempo e trabalho para configuração e manutenção, de todos os equipamentos inerentes a rede.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Sara; OLIVEIRA, Ana Katarina P. de. **Manual para apresentação de trabalhos acadêmicos, projetos de pesquisa, relatórios finais e artigos**. 2. ed. rev. e ampl. ____ Natal: FARN, 2003.

CENTRO DE ORIENTAÇÕES DE SEGURANÇA. **Arquitetura da solução LAN para redes sem fios**. Disponível em: <http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod169.mspx> Acesso em: 13.mar.07

_____. **Decisão sobre uma estratégia de rede sem fio protegida**. Disponível em: <http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx> Acesso em: 14.mar.07

PINHEIRO, José Maurício Santos. **Aplicações para redes wireless**. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_para_redeswireless.php Acesso em: 13.abr.07.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fios**. Novatec Editora: São Paulo, 2005. 2 ed.

SILVA, Luiz Antonio F. da; DUARTE, Otto Carlos M. B. **Radius em rede sem fio**. Disponível em: http://www.gtaufri.br/cpe825/tutoriais/lafs/radius_sem_fio.pdf Acesso em : 23.abr.07.

SILVA, Gilson Marques; SOUZA, João Nunes. **Uma análise dos mecanismos de segurança de redes locais sem fio e uma proposta de melhoria**. Disponível em <http://www.ppgia.pucpr.br/~maziero/pesquisa/ceseg/wseg03/06.pdf> Acesso em: 23.abr.07.

TUTORIAL WIRELESS. **O que são redes wireless** Disponível em <http://www.babooforum.com.br/idealbb/view.asp?topicID=269602> Acesso em: 23.abr.07

WIKIPEDIA. **Protocolo extensible do authentication**. Disponível em http://64.233.179.104/translate_c?hl=pt-BR&sl=en&u=http://en.wikipedia.org/wiki/Enten... Acesso em 16.05.07.