

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN**

Wagner Andrade Cavalcanti

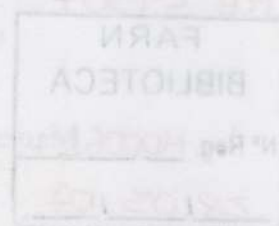
**ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM
FIO COM MICROSOFT WINDOWS**

**ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM
FIO COM MICROSOFT WINDOWS**

Sistema de
Informação da Faculdade Natalsense
para o Desenvolvimento do Rio
Grande do Norte - como requisito
obrigatório para a obtenção do título
de Bacharel em História e de
Informação.

Orientador:

Alcides Pereira de Brito



**NATAL/RN
2006**

FARN

FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
LIGA DE ENSINO DO RIO GRANDE DO NORTE

Wagner Andrade Cavalcanti

ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM
FIO COM MICROSOFT WINDOWS

RB 29307

FARN
BIBLIOTECA
Nº Reg. M000617
28/05/07

004.7
C365e
2006
Ex:01

NATAL/RN
2006

**ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM
FIO COM MICROSOFT WINDOWS**

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em
de _____ de _____, pela banca examinadora composta pelas
seguintes membros.

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

Orientador:

Aluizio Ferreira da Rocha Neto, M

**NATAL/RN
2006**

ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO COM MICROSOFT WINDOWS

Catálogo na Publicação – Biblioteca da FARN

Setor de Processos Técnicos

Cavalcanti, Wagner Andrade

Estudo do protocolo de autenticação 802.1x em redes sem fio com Microsoft Windows/ Wagner Andrade Cavalcanti. – Natal: FARN, 2006.
52f.

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

Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes Wireless – Monografia. 2. Segurança em Redes – Monografia. 3. Protocolo IEEE 802.1x – Monografia I. Título.

RN/FARN/BC

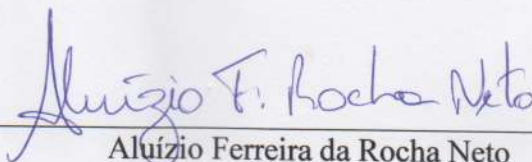
CDU 004.7

ESTUDO DO PROTOCOLO DE AUTENTICAÇÃO 802.1X EM REDES SEM FIO COM MICROSOFT WINDOWS

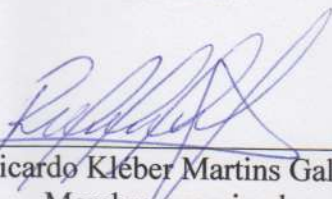
Eu dedico este trabalho a Deus, pois Ele é tudo para mim. Deus Fiel, sempre presente, jamais me abandonou.
Aos meus pais, meu ponto de referência, sempre me apoiando e amando. Por os
ano:
A minha namorada, pela amor, paciência, carinho, apoio, compreensão e
companheirismo dedicado em todos os momentos.

WAGNER ANDRADE CAVALCANTI

Monografia apresentada ao curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em _____ de _____ de _____, pela banca examinadora composta pelos seguintes membros.



Aluizio Ferreira da Rocha Neto
Orientador



Ricardo Kleber Martins Galvão
Membro examinador



Bartira Paraguaçu F. Dantas Rocha
Membro examinador

DEDICATÓRIA

Eu dedico este trabalho a Deus, pois Ele é tudo para mim. Deus Fiel, sempre presente, jamais me abandonou.

Aos meus pais, meu ponto de referência, sempre me apoiando e amando. Eu os amo.

A minha namorada, pelo amor, paciência, carinho, apoio, compreensão e companheirismo dedicado em todos os momentos.

AGRADECIMENTOS

Ao meu orientador Professor Aluizio Ferreira da Rocha Neto, pelo auxílio, compreensão e paciência empregados a mim.

Ao meus amigos que me apoiaram nesta minha monografia.

*"Assim que, se alguém está em Cristo, nova criatura é:
as coisas velhas já passaram, eis que tudo se fez novo".*

A Bíblia Sagrada, em II Cor. 5:17

RESUMO

Esta Monografia apresenta um estudo da implantação de segurança de rede wireless baseada no protocolo 802.1x utilizando o sistema operacional Microsoft Windows. O intuito deste protocolo é prover uma maior segurança dos usuários de redes sem fio através da autenticação e criptografia. É abordada sua padronização, seu funcionamento, os esquemas de autenticação usados com o protocolo 802.1x, instalação e configuração da Microsoft IAS (Serviço de Autenticação de Internet), bem como a autenticação do protocolo 802.1x com o servidor RADIUS.

Palavras-chaves: Redes, Segurança em Redes, IAS, Wireless, IEEE 802.1x, WEP, RADIUS, WPA, Criptografia.

*“Assim que, se alguém está em Cristo, nova criatura é;
as coisas velhas já passaram; eis que tudo se fez novo”.*

A Bíblia Sagrada, em II Cor. 5:17

RESUMO

Esta Monografia apresenta um estudo da implantação de segurança de rede *wireless* baseada no protocolo 802.1x utilizando o sistema operacional Microsoft Windows. O intuito deste protocolo é prover uma maior segurança dos usuários de redes sem fio através da autenticação e criptografia. É abordada sua padronização, seu funcionamento, os esquemas de autenticações usados com o protocolo 802.1x, instalação e configuração do Microsoft IAS (Serviço de Autenticação de Internet), bem como a autenticação do protocolo 802.1x com o servidor RADIUS.

Palavras-chaves: Redes, Segurança em Redes, IAS, Wireless, IEEE 802.1x, WEP, RADIUS, WPA, Criptografia.

ABSTRACT

This Monograph presents a study of the implantation of net security wireless based in the protocol 802.1x using the operational system Microsoft Windows. The intention of this protocol is to provide a bigger security with the users of nets without wire through the authentication and criptografia. Its standardization, its functioning, the used projects of authentications with the protocol is boarded 802.1x, installation and configuration of the Microsoft YOU WENT (Service of Authentication of Internet), as well as the authentication of the protocol 802.1x with server RADIUS.

Word-keys: Networks, Safety in Networks, Wireless, IEEE 802.1x, IAS WEP, WPA, RADIUS, Cryptography.

2.4	ORGANIZAÇÃO DO TRABALHO	15
3.1	REDES DE COMPUTADORES	16
3.2	REDES LOCAIS SEM FIO	17
3.2.1	Visão Geral do Protocolo IEEE 802.11	18
3.3	SEGURANÇA EM REDES DE COMPUTADORES	19
3.3.1	CRİPTOGRAFIA	20
3.4	SEGURANÇA EM REDES LOCAL SEM FIO	20
3.4.1	Prevenção de Spyware em redes Wi-Fi	22
3.5	ORGANIZAÇÃO 802.1X	23
3.5.1	Terminologia do 802.1x	24
3.5.2	Autenticação de Rede	24
3.5.3	Portas Controladas e Não Controladas	25
3.6	USANDO O 802.1X PARA AUTENTICAÇÃO SEM FIO	26
3.6.1	Soluções para questões WEP com 802.1X	28
4	DESENVOLVIMENTO DA SOLUÇÃO	30
4.1	SERVİÇO DE AUTENTICAÇÃO DE INTERNET DO WINDOWS SERVER	30
4.1.1	Instalação do IAS no Windows Server 2003	31
4.1.2	Configurações Iniciais sobre o IAS	34
4.2	CONFIGURAÇÃO DO IAS	35
4.2.1	Configuração Inicial de Parte do IAS	35
4.3	PROCESSO DE AUTENTICAÇÃO USANDO EAP	37
4.3.1	EAP-MD5	38
4.3.2	EAP-TLS	38
4.3.3	EAP-PEAP	40
4.3.4	EAP-PTLS	44
5	CONCLUSÃO	45
6	REFERÊNCIAS	46
7	ANEXOS	48

1	INTRODUÇÃO.....	13
2	OBJETIVOS.....	14
2.1	OBJETIVO GERAL	14
2.2	OBJETIVOS ESPECÍFICOS.....	14
2.3	JUSTIFICATIVA.....	14
2.4	ORGANIZAÇÃO DO TRABALHO.....	15
3	REFERENCIAL TEÓRICO	16
3.1	REDES DE COMPUTADORES.....	16
3.2	REDES LOCAIS SEM FIO.....	17
3.2.1	<i>Visão Geral do Padrão IEEE 802.11</i>	18
3.3	SEGURANÇA EM REDES DE COMPUTADORES	19
3.3.1	<i>CRIPTOGRAFIA</i>	20
3.4	SEGURANÇA EM REDES LOCAL SEM FIO	20
3.4.1	<i>Prevenção de Segurança em redes Wi-Fi</i>	22
3.5	O PADRÃO 802.1X.....	23
3.5.1	<i>Terminologia do 802.1x</i>	24
3.5.2	<i>Autenticador ou Suplicante</i>	24
3.5.3	<i>Portas Controladas e Não Controladas</i>	25
3.6	USANDO O 802.1X PARA AUTENTICAÇÃO SEM-FIO.....	26
3.6.1	<i>Solucionando questões WEP com 802.1X</i>	28
4	DESENVOLVIMENTO DA SOLUÇÃO.....	30
4.1	SERVIÇO DE AUTENTICAÇÃO DE INTERNET DO WINDOWS SERVER	30
4.1.1	<i>Instalação do IAS no Windows Server 2003</i>	31
4.1.2	<i>Observações importantes sobre o IAS</i>	34
4.2	CONFIGURAÇÃO DO IAS	35
4.2.1	<i>Configurando informações de Porta do IAS</i>	35
4.3	PROCESSO DE AUTENTICAÇÃO USANDO EAP	37
4.3.1	<i>EAP-MD5</i>	38
4.3.2	<i>EAP-TLS</i>	38
4.3.3	<i>EAP-PEAP</i>	40
4.3.4	<i>EAP-TTLS</i>	44
5	CONCLUSÃO.....	45
	REFERÊNCIAS	46
	APENDICE.....	48

Figura 1: Pequena de Portas Controladas e Não Controladas no 802.1x	25
Figura 2: Sequência de troca de mensagens entre os sistemas do 802.1x	27
Figura 3: Solução baseada na autenticação EAP-TLS	39
Figura 4: Processo de acesso 802.1X EAP-TLS	40

1 INTRODUÇÃO **LISTA DE FIGURAS**

Figura 1: Esquema de Portas Controladas e Não Controladas no 802.1x	25
Figura 2: Seqüência de troca de mensagens entre os atores do 802.1x	27
Figura 3: Solução baseada na autenticação EAP-TLS.....	39
Figura 4: Processo de acesso 802.1X EAP-TLS.....	40

A palavra *wireless*, proveniente do inglês: *wire* (fio, cabo); *less* (sem); ou seja: sem fios. *Wireless* então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos.

O controle remoto de televisão ou aparelho de som, os telefones celulares e uma infinidade de aparelhos trabalham com conexões *wireless*. Exemplificando, durante uma conversa entre duas pessoas, tem-se uma conexão *wireless*, partindo do princípio de que a voz não utiliza cabos para chegar até o receptor da mensagem.

Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), Bluetooth e Wi-Max.

A comunicação *wireless* está presente a um bom tempo no cotidiano das pessoas. Falando da conexão sem fio mais comum – os controles remotos para televisores, som, DVD, entre outros, utilizam conexão por raios infravermelhos (InfaRed). Essa conexão atua em um alcance máximo de 5m aproximadamente, e com ângulo de 45 graus a partir da fonte.

Dentro do conceito de WLAN (Wireless Local Area Network) tem-se o Wi-Fi. O Wi-Fi nada mais é do que um nome comercial para um padrão de rede *wireless* chamado de 802.11b, utilizado em aplicações de rede local.

O padrão 802.11b define a frequência de trabalho, velocidade, alcance e outras características. Este tipo de conexão também trabalha com rádio frequência em uma faixa de 2.4Ghz. Esta frequência é comumente utilizada em alguns telefones sem fio e alguns microondas.

Embora esse tipo de rede seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus usuários:

- Estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como notebooks, PDAs, celulares de trabalho, etc);

1 INTRODUÇÃO

As tecnologias sem fio trouxeram uma série de novos termos, ainda não assimilados pelo usuário menos experiente. A confusão entre tecnologias, termos, padrões e variações pode ser facilmente desfeita com uma breve explicação do desenvolvimento destas tecnologias.

A palavra *wireless*, provém do inglês: *wire* (fio, cabo); *less* (sem); ou seja: sem fios. *Wireless* então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos.

O controle remoto de televisão ou aparelho de som, os telefones celulares e uma infinidade de aparelhos trabalham com conexões *wireless*. Exemplificando, durante uma conversa entre duas pessoas, tem-se uma conexão *wireless*, partindo do princípio de que a voz não utiliza cabos para chegar até o receptor da mensagem.

Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), Bluetooth e Wi-Max.

A comunicação *wireless* está presente a um bom tempo no cotidiano das pessoas. Falando da conexão sem fio mais comum – os controles remotos para televisores, som, DVD, entre outros, utilizam conexão por raios infravermelhos (InfraRed). Essa conexão atua em um alcance máximo de 5m aproximadamente, e com ângulo de 45 graus a partir da fonte.

Dentro do conceito de WLAN (Wireless Local Area Network) tem-se o Wi-Fi. O Wi-Fi nada mais é do que um nome comercial para um padrão de rede *wireless* chamado de 802.11b, utilizado em aplicações de rede local.

O padrão 802.11b define a frequência de trabalho, velocidade, alcance e outras características. Este tipo de conexão também trabalha com rádio frequências em uma faixa de 2.4Ghz. Esta frequência é comumente utilizada em alguns telefones sem fio e fornos microondas.

Embora esse tipo de rede seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus usuários:

- Estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como *notebooks*, PDAs, estações de trabalho, etc);

- Por serem bastante simples de instalar, muitas pessoas estão utilizando redes desse tipo em casa, sem nenhum cuidado adicional, e até mesmo em empresas, sem o conhecimento dos administradores de rede.

Esta Monografia tem como propósito implementar uma segurança de rede wireless baseada no protocolo sem fio 802.1x utilizando o sistema operacional Microsoft Windows na faculdade FARN, para que os usuários da mesma instituição tenha um acesso restrito e assim tenha mais segurança nos dados através de um login e senha que forem cadastrados no sistema.

2 OBJETIVOS

2.1 Objetivo geral

O projeto tem como objetivo principal implementar uma segurança na rede sem fio da faculdade que tenha um gerenciamento mais consistente e seguro para a rede de computadores da FARN, utilizando o protocolo 802.1x (E um padrão de projeto para controle de acesso de rede baseado em porta). Ele é usado para fornecer acesso de rede autenticado para redes Ethernet e o sistema operacional utilizado é o Microsoft Windows.

2.2 Objetivos específicos

Para alcançar o objetivo geral, desenvolveremos as seguintes etapas:

- Estudar as tecnologias de Redes sem Fio, em especial, a Wi-Fi
- Estudar uma visão geral do Padrão IEEE 802.11
- Estudar o protocolo 802.1x
- Abordar a questão da segurança na tecnologia em Wi-Fi
- Abordar a Criptografia e Prevenções de Segurança em redes Wi-Fi
- Estudar o processo de autenticação usando o EAP e alguns tipos de autenticações com EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP.

2.3 JUSTIFICATIVA

Uma rede sem fio de longo alcance destinada a uma grande comunidade que sofre de problemas de segurança. Estes problemas normalmente se referem ao controle de acesso à rede e de acesso ao tráfego.

O problema no controle de acesso diz respeito ao fato de que qualquer pessoa que possua um dispositivo com a tecnologia Wi-Fi poderá ter acesso físico à rede *wireless* se ela estiver no alcance da mesma.

O problema de acesso ao tráfego se refere ao fato de que como em uma rede sem fio o meio físico, que é o ar, é acessível a qualquer um, alguém mal intencionado poderá capturar e analisar todo o tráfego de um usuário da rede *wireless* no intuito de obter acesso a informações confidenciais.

Portanto, o que motiva o desenvolvimento deste trabalho é a implementação de mecanismos de segurança em redes *wireless*, de forma que o administrador de tal rede possa identificar o usuário desta rede e impedir que informações sigilosas que trafegam em tal rede sejam capturadas.

2.4 ORGANIZAÇÃO DO TRABALHO

No Capítulo 2 será apresentada uma visão geral sobre as redes de computadores, redes sem fio, questões relacionadas à segurança, autenticação dos usuários e problemas relacionados.

No Capítulo 3 são abordadas as várias soluções de autenticação de usuários em uma rede sem fio, bem como a instalação do serviço de autenticação da Internet (IAS) utilizando o sistema operacional Microsoft Windows Server 2003, a configuração e a autenticação com o servidor RADIUS. Também será apresentado o processo de autenticação utilizando o protocolo EAP e alguns tipos de autenticação com MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, como também o processo de autenticação do PEAP.

O Capítulo 4 apresentará as conclusões sobre este trabalho.

3 REFERENCIAL TEÓRICO

3.1 REDES DE COMPUTADORES

Basicamente uma rede consiste em dois computadores interligados com o objetivo de compartilhar dado. Isso já pode ser considerado uma rede. (Fred, Melo Enciclopédia Virtual de Redes de Computadores, 2005).

Este é apenas um exemplo simples, é claro que uma rede não é apenas dois computadores interligados a fim de compartilhar dados e sim dois ou mais interligados. Alias todas as redes, não importa o quanto sejam sofisticadas, derivam desse sistema simples. Se a idéia de dois computadores conectados por um cabo pode não parecer extraordinária, no passado representou uma grande conquista nas comunicações.

Segundo (Fred Melo do Site da Enciclopédia Virtual de Redes de Computadores) define o seguinte:

Uma rede de trabalho é um sistema que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações. Os componentes básicos de uma rede de trabalho (ou rede de informações) são um emissor (origem da informação), o meio através da qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si. Um exemplo comum seria uma pessoa falando no telefone com outra pessoa: O emissor seria quem está falando, o canal seria a linha telefônica, o receptor a pessoa que está ouvindo e a mensagem seria a própria mensagem que está sendo comunicada. Ao longo dos anos as ferramentas para a comunicação de dados foram evoluindo gradativamente, de modo a tornar a troca de informações rápida, fácil e mais eficiente.

Uma rede de computadores baseia-se nos princípios de uma rede de informações, implementando técnicas de hardware e software de modo a torná-la efetivamente mais dinâmica, para atender às necessidades que o mundo moderno impõe. Redes de computadores incluem todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras. Esse dispositivo que se comunica entre si são chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede. Dois computadores, ou nós, seria o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, teoricamente todos os computadores do mundo poderiam estar interligados. (Enciclopédia Virtual de Redes de Computadores, 2005).

Quanto à natureza podemos ter dois tipos de redes de computadores: cliente-servidor (*client-server*) e ponto-a-ponto (*peer-to-peer*). Na rede cliente-servidor uma máquina, ou um pequeno grupo de máquinas, centraliza os serviços da rede oferecidos a demais estações, tais como aplicativos e filas de impressão. As máquinas que requerem esses serviços são chamadas de clientes, e as máquinas que os fornecem são chamadas de servidores. Na rede ponto-a-ponto não existem servidores, todas as estações compartilham seus recursos mutuamente. A grande desvantagem que as redes ponto-a-ponto oferecem com relação às redes cliente-servidor é a dificuldade de gerenciar os seus serviços, já que não existe um sistema operacional que centralize a administração da rede. Também não é possível estendê-las excessivamente, já que um número elevado de nós sobrecarregaria o fluxo de dados, tornando-a lenta e, por conseguinte ineficaz. Aos poucos as empresas estão substituindo suas redes ponto-a-ponto por redes cliente-servidor, e o número de redes ponto-a-ponto está diminuindo. (Melo, Fred - Enciclopédia Virtual de Redes de Computadores, 2005).

O principal motivo para a implementação de redes de computadores nas organizações, sejam elas simples escritórios ou empresas de âmbito internacional, resume-se em uma única palavra: dinheiro! Os custos reduzidos com a automatização dos processos mediante a utilização de redes são realmente muito significativos. Por exemplo, se uma empresa pudesse optar entre adquirir cem impressoras independentes ou apenas dez compartilhadas, sem dúvida alguma a segunda opção seria mais interessante. Também é preferível adquirir o direito de compartilhar um aplicativo (chamados de pacotes para vários usuários) entre um número predeterminado de usuários, do que adquirir várias cópias unitárias. (Melo, Fred Enciclopédia Virtual de Redes de Computadores, (2005).

3.2 REDES LOCAIS SEM FIO

Basicamente, existem dois tipos de redes locais sem fio: as redes independentes, ou *ad-hoc*, e as redes com infra-estrutura. Sobre isto, (Fred Melo do Site da Enciclopédia Virtual de Redes de Computadores) define o seguinte:

As redes independentes, também chamadas de *ad-hoc*, são as redes sem fio mais básicas e simples. São redes sem topologia determinada, em que não existe qualquer elemento central que estruture a comunicação. Neste caso, as estações se comunicam diretamente entre si. A grande vantagem dessas redes é a facilidade de instalação, que se resume à configuração das interfaces de rede sem fio em cada estação

móvel Como nenhum outro elemento é necessário, os custos também são reduzidos, e nem mesmo um projeto precisa ser elaborado.

No entanto, como desvantagens têm-se o fato de uma cobertura pequena e restrita e inconstância na qualidade da comunicação. Há também falhas devido a barreiras físicas que podem interferir na comunicação entre estações, já que elas se comunicam diretamente. Além de deficiências de controle, há também deficiências de segurança, pois a maioria dos mecanismos de segurança são implementados no elemento que coordena a rede e que, neste caso, não existe.

3.2.1 Visão Geral do Padrão IEEE 802.11

As redes locais sem fio são uma alternativa às atuais redes cabeadas, com a grande vantagem de prover flexibilidade e mobilidade. Elas permitem que diversas estações ou servidores se comuniquem sem a necessidade de cabos. A comunicação ocorre através de ondas eletromagnéticas. Essas redes podem existir de forma isolada, apenas com o intuito de prover conectividade a um grupo de sistemas, mas também podem existir como uma extensão de uma rede convencional cabeada. Ou seja, parte do ambiente de rede pode ser implementado no formato convencional através de conexões cabeadas e parte dela, a que requer mobilidade, pode ser implementada por meio de conexões sem fio. Logo, uma rede local sem fio pode ser definida como um meio flexível de comunicação de dados, implementado como uma extensão ou uma alternativa de uma rede local cabeada.

Essas redes têm se tornado cada vez mais uma opção para ambientes corporativos, já que podem ser rapidamente implementadas em locais que não possuam infra-estrutura de cabeamento. Além de permitir a mobilidade, que é um requisito importante no mundo atual.

Em 1999, o IEEE (*Institute of Electrical and Electronics Engineers*) publicou o padrão IEEE 802.11, que é o responsável pela especificação das redes locais sem fio.

Ele descreve o ambiente e o protocolo em todos seus aspectos, incluindo desde a parte física até os mecanismos de segurança do protocolo. (Site da Microsoft Brasil, 28 de Junho de 2004).

O IEEE 802.11 é um padrão de rede de área local (LAN) sem-fio compartilhado. Ele usa o protocolo de acesso múltiplo sensível à operadora (CSMA) e o controle de

acesso médio (MAC) com previsão de colisão (CA). Esse padrão permite tanto transmissões de espectro de disseminação por seqüência direta (DS) quanto por salto de frequência (FH) na camada física. A taxa máxima de transmissão de dados oferecida por esse padrão era de 2 megabits por segundo. Uma versão de velocidade maior, com uma definição de camada física abaixo da especificação de 802.11b, permite uma taxa de transmissão de dados de até 11 megabits por segundo usando a transmissão de espectro de disseminação por DS.

O padrão IEEE 802.11 é dividido em alguns subgrupos:

- No 802.11a, a velocidade pode chegar a 54Mbps/s, no entanto opera em 5GHz, necessitando de autorização para uso de frequência;
- No 802.11b, a velocidade pode chegar a 11Mbps/s operando em 2.4GHz. É a versão atualmente mais utilizada e comum;
- No 802.11g, a velocidade pode chegar a 22Mbps/s, com a vantagem de operar em 2.4GHz;
- O 802.11h é a versão européia do 802.11a, com poucas diferenças e algumas otimizações;
- O 802.11i foca as questões de segurança;
- O 802.11c foca a melhoria de interoperabilidade entre dispositivos;
- O 802.11d foca a melhoria de *roaming*;
- O 802.11e foca a melhoria de qualidade de serviço;
- O 802.11f foca a regularização de *handoff*.

3.3 SEGURANÇA EM REDES DE COMPUTADORES

A segurança da rede local de qualquer LAN está relacionada à necessidade de proteção contra acessos não autorizados, manipulação dos dados armazenados na rede, assim como a sua integridade, e utilização não autorizada de computadores ou de seus respectivos dispositivos periféricos. Essa necessidade de proteção deve ser definida a partir das possíveis ameaças e riscos que a rede sofre, além dos objetivos traçados pela instituição, sendo tudo isso formalizado nos termos de uma política de segurança. Dessa forma, procura-se evitar que pessoas não-autorizadas tenham acesso a informações particulares de qualquer usuário da rede.

3.3.1 CRIPTOGRAFIA

Enquanto o 802.11 teve um crescimento rápido no ambiente de LAN sem-fio, diversas questões de segurança surgiram em relação a redes sem-fio em geral.

Segundo (Tom Fout e Warren Barkey 2003),

O padrão LAN sem-fio 802.11 define serviços de autenticação e criptografia baseados no algoritmo **WEP** (*Wired Equivalent Privacy*). O algoritmo WEP define o uso de uma chave secreta de 40 bits para autenticação e criptografia. Muitas implementações 802.11 também permitem chaves secretas de 104 bits. Entretanto, o padrão não define um protocolo de gerenciamento chave e presume que chaves secretas e compartilhadas são fornecidas para a estação (STA) sem-fio 802.11 através de um canal seguro independente de 802.11.

A falta de um protocolo de gerenciamento chave WEP é a limitação principal para fornecer segurança 802.11; especialmente numa rede de infra-estrutura sem-fio (uma rede sem-fio usando pontos de acesso sem-fio [APs] para fazer interface com a rede com fios) com diversas estações. Alguns exemplos desse tipo de rede incluem campi corporativos e locais públicos tais como aeroportos e *shopping centers*. Quando chaves compartilhadas configuradas manualmente são usadas, as chaves tendem a permanecer no lugar por longos períodos de tempo, dando mais tempo aos *hackers* para usarem diversos ataques para obter as chaves e decodificar a transmissão. A falta de serviços de autenticação e criptografia também afeta a operação numa rede *ad hoc* sem-fio (rede sem-fio ponto a ponto) onde os usuários podem desejar envolver-se em comunicações colaborativas ponto a ponto: por exemplo, em áreas como salas de reunião.

Portanto, a importância reforçada da autenticação e da criptografia em um ambiente sem-fio prova a necessidade de controle do acesso e mecanismos de segurança que incluem um protocolo de gerenciamento chave especificado no 802.11.

3.4 SEGURANÇA EM REDES LOCAL SEM FIO

Como as informações neste tipo de rede trafegam pelo ar, podem ser capturadas por qualquer pessoa que tenha um equipamento compatível. Com o barateamento dos equipamentos e lançamento de placas multipadrão, a compatibilidade deixou de ser um problema.

Portanto, a primeira coisa que o usuário deve ter em mente é que qualquer tráfego não criptografado pode ser facilmente capturado. E aí entra o primeiro problema: muitas pessoas simplesmente não habilitam ou reivindicam aos respectivos administradores a implementação de métodos criptográficos. Mesmo o WEP, que é mais simples de ser quebrado (com programas apropriados), é melhor que não usar nenhuma proteção ao conteúdo do tráfego.

Em ambientes públicos, como aeroportos e centros de compras, é muito comum à existência de serviços de conexão à Internet via redes sem fio, conceito conhecido pelo nome de hot spot. Um dos problemas de segurança mais comuns, neste caso, está ligado à autenticação do usuário, normalmente feita por uma página Web usando o protocolo HTTP e não HTTPS, portanto sem criptografia, passível de captura e utilização posterior não autorizada.

Outro problema diz respeito à inexistência de mecanismos de criptografia no tráfego. Mesmo que no momento da autenticação seja usado o protocolo HTTPS ou similar, se não houver um método para cifrar os dados durante o uso do serviço, o usuário poderá ter sua privacidade comprometida, ainda mais se acessar informações sensíveis via correio eletrônico através de *webmail* ou POP3, por exemplo.

Um usuário assinante de um serviço Wi-Fi, em geral liga o computador, informa suas credenciais (normalmente usuário e senha), estabelece conexão com um concentrador e está apto a navegar. Porém, qual a garantia que este usuário tem de estar conectado por um concentrador legítimo? Com a sofisticação e barateamento dos equipamentos, forjar um concentrador passou a ser uma tarefa factível, até mesmo com equipamentos simples, como PDAs ou notebooks. Um concentrador falso pode ser montado para simplesmente coletar usuários e senhas válidos para uso posterior ou, nos casos mais sofisticados, redirecionar o tráfego para o concentrador real, mas tendo acesso ao conteúdo das informações trafegadas.

Possibilidades de ataques podem existir nos protocolos de rede, nos concentradores e também, claro, nos clientes. Um ataque direto a um cliente conectado possibilita obter dados sobre configurações de rede, incluindo senhas previamente compartilhadas pelos padrões WEP ou WPA. Obtendo domínio sobre o equipamento do usuário legítimo, o atacante pode ainda usar uma conexão estabelecida para fazer uso da rede, ou seja, o usuário acessa a Internet ou rede local, e o atacante também.

3.4.1 Prevenção de Segurança em redes Wi-Fi

Os ataques podem ocorrer em vários níveis, então os métodos preventivos devem se dar em todos eles. O usuário deve cobrar do administrador ou provedor que as soluções adotadas sejam as mais seguras possíveis, porém um modelo eficiente e seguro em um ambiente certamente não será em outro.

Segundo (Nelson Murilo, Site Terra Informática),

Em redes pequenas pode ser razoável usar senhas WEP ou WPA previamente compartilhadas, mas isso não é factível em redes pagas em locais públicos (hotspots), onde não existe condições de contatar todos os usuários do serviço para uma eventual troca da senhas. Neste caso, a autenticação usando HTTPS, por exemplo, pode garantir uma segurança adicional, e ainda maior se o usuário confirmar o certificado digital da empresa provedora do serviço, evitando acessar concentradores falsos.

Sinais suspeitos de conexão com concentradores clonados são:

- Após autenticação, a navegação não funciona;
- Navegação intermitente;
- Sinal do concentrador variando, por vezes sumindo e reaparecendo.

Os novos padrões, notadamente o 802.11i (O padrão 802.11i foi criado como a evolução do protocolo WEP. O WEP (Wired Equivalent Protocol) objetivava trazer o mesmo nível de segurança das redes com fio para as sem fio. Mas, devido à simplicidade de sua elaboração, para permitir a rápida disseminação dos sistemas 802.11, foi decodificado, permitindo aos invasores de redes acesso aos ambientes particulares). Possibilitam métodos de autenticação bastante robustos, com os quais o administrador pode montar ambientes que, por exemplo, usem uma base centralizada de usuários para qualquer necessidade de autenticação, quer seja uma aplicação, acesso a recursos da rede (cabada, sem fio ou ambas), uso de VPNs (Redes Privadas Virtuais), etc.

Esse tipo de solução pode ser interessante para empresas com muitos funcionários, pois reduz bastante as chamadas para troca de senhas, permite um maior controle dos usuários ativos e facilita a criação e manutenção das aplicações e sistemas

da empresa, pois à parte de autenticação é a mesma para todos. Esse método também pode ser usado sem maiores problemas por serviços pagos de acesso à Internet, pois o usuário teria de fornecer as mesmas informações a que ele já está acostumado: usuário e senha.

Entretanto, esses padrões necessitam de equipamentos mais recentes e, em princípio, o fornecedor do serviço não poderia exigir que seus assinantes estivessem atualizados em termos de placas e equipamentos (alguns *notebooks* e PDAs têm placas sem fio integradas, por exemplo). E a despeito da possibilidade de a empresa prestadora do serviço fazer convênios com fabricantes de equipamentos, oferecendo linhas de crédito ou descontos para aquisição de dispositivos compatíveis com o serviço, esta idéia (convênio) pode ser melhor aproveitada por empresas, que têm maior poder de, digamos, convencimento sobre seus funcionários.

É importante saber que acessos públicos (pagos ou não) são, em princípio, um risco, por isso não se deve usar equipamentos de terceiros para acessar informações pessoais ou empresariais sensíveis. E isso vale para equipamentos de infra-estrutura também (link, roteadores, concentradores, servidores etc.). O uso de criptografia é essencial para aumentar a segurança das informações trafegadas, e isso pode ser conseguido através de VPNs, HTTPS, SPOP3 (acesso POP3 seguro) ou protocolos convencionais acrescidos da camada SSL, por exemplo. Verifique com o suporte da sua empresa ou provedor a existência desses mecanismos e como configurá-los.

E, por fim, para evitar ataques aos computadores, *notebooks* e PDAs, devem ser seguidos os mesmos procedimentos conhecidos para redes cabeadas, como atualizar o sistema operacional, aplicativos, antivírus, firewall pessoal, anti-spyware e anti-spam. Da mesma maneira que um carro sem manutenção, um computador desatualizado é dor-de-cabeça na certa.

3.5 O PADRÃO 802.1X

Outro padrão, relacionado à segurança em redes, descreve mecanismos de autenticação por porta. Originalmente desenvolvido para as redes convencionais, o padrão IEEE 802.1X é bastante utilizado para as implementações de redes sem fio. Esse padrão descreve mecanismos adicionais de segurança, que visam tornar essas redes locais sem fio mais seguras.

Segundo (Tom Fout e Warren Barkey 2003),

O 802.1X é um padrão de projeto para controle de acesso de rede baseado em porta. Ele é usado para fornecer acesso de rede autenticado para redes Ethernet. O controle de acesso de rede baseado em porta usa as características físicas da infra-estrutura da LAN comutada para fornecer um meio de autenticação de dispositivos anexados a uma porta da LAN e para impedir o acesso àquela porta em casos onde o processo de autenticação falha.

Normalmente são utilizados nos projetos, servidores Radius para a autenticação dos usuários.

3.5.1 Terminologia do 802.1x

A seguir algumas definições de terminologias que serão utilizadas ao longo deste projeto.

- **Servidor de Autenticação** – Este é o cliente responsável pelo processo de recebimento e resposta de solicitações, para autenticação de acesso à rede. Estes clientes normalmente são Servidores Radius.
- **Autenticador** – Switch, Roteador ou Access Point que disponibiliza o acesso aos usuários da rede. Estes dispositivos são responsáveis pela autenticação do acesso à rede.
- **Suplicante** – 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 Autenticadores.
- **EAP** – *Extensible Authentication Protocol*. EAP é um protocolo genérico que permite que os pontos de acesso à rede suportem múltiplos métodos de autenticação, entre eles esta: *smart cards*.
- **EAPOL** – *EAP over LAN* como definido pelo padrão IEEE 802.1x.

3.5.2 Autenticador ou Suplicante

Uma porta de LAN pode desempenhar um entre dois papéis em uma interação de controle de acesso à rede: autenticador ou suplicante.

Um autenticador é uma porta que “força” a autenticação antes de permitir o acesso aos serviços disponíveis através daquela porta. O suplicante é uma porta que “solicita” o acesso aos serviços disponíveis através da porta do autenticador.

Um servidor de autenticação também executa uma função de autenticação; ele verifica a credencial do suplicante em nome do autenticador. O servidor de autenticação

então responde ao autenticador indicando se o suplicante está autorizado a acessar os serviços do autenticador ou não. O servidor de autenticação pode ser uma entidade separada, ou suas funções podem ser co-localizadas no autenticador.

3.5.3 Portas Controladas e Não Controladas

O controle de acesso baseado em porta do autenticador define dois pontos de acesso lógico para a LAN através de uma porta LAN física única conforme exibido na Figura 1.

O primeiro Acces point lógico denominado “Porta Não Controlada” permite uma troca não controlada entre o autenticador e outros sistemas na LAN — independente do estado de autorização do sistema. O segundo Acces point lógico denominado “Porta Controlada” permite uma troca entre um sistema na LAN e os serviços do autenticador — somente se o sistema estiver autorizado.

Um uso da porta não controlada seria fornecer um caminho para as trocas entre o autenticador e o suplicante.

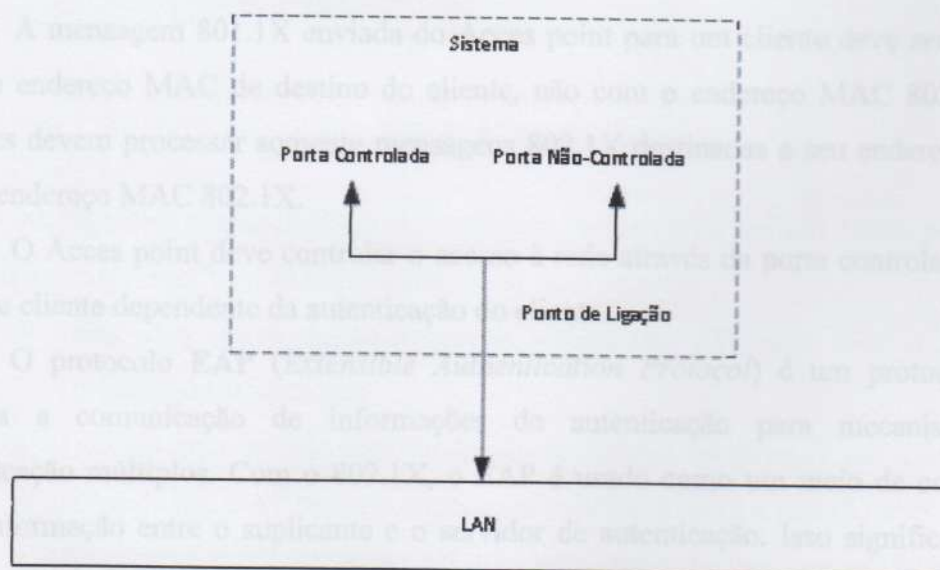


Figura 1: Esquema de Portas Controladas e Não Controladas no 802.1x
Fonte: Site da Microsoft Brasil

O Estado de Autorização da porta controlada determina se a transmissão pode fluir do suplicante para a LAN através dessa porta. O estado de autorização provavelmente iniciará como Não Autorizado e será alterado para o estado Autorizado com a autenticação do suplicante.

3.6 USANDO O 802.1X PARA AUTENTICAÇÃO SEM-FIO

O 802.1X pode ser aplicado à autenticação sem-fio, usando um servidor RADIUS para autenticar as credenciais de clientes.

É necessário uma extensão para o protocolo 802.1X básico para permitir que um Acces point sem-fio identifique com segurança a transmissão de um cliente em particular. Isso é feito através da passagem de uma chave de autenticação para o cliente e para o Acces point sem-fio, como parte do procedimento de autenticação. Somente um cliente autenticado conhece a chave de autenticação, e a chave de autenticação criptografa todos os pacotes enviados por um cliente.

O 802.1X é um padrão IEEE para controle de acesso de rede para LANs. O padrão estabelece o controle de acesso à rede para redes Ethernet e Token Ring. Ele não define como usar o 802.1X para 802.11. Com três alterações, o 802.1X pode ser usado para controle de acesso para redes 802.11:

O 802.11 definiu que mensagens “associadas” e “dissociadas” são equivalentes a “conectar” e “desconectar” na porta Ethernet. Isso controla quando a autenticação ocorre.

A mensagem 802.1X enviada do Acces point para um cliente deve ser enviada com o endereço MAC de destino do cliente, não com o endereço MAC 802.1X. Os clientes devem processar somente mensagens 802.1X destinadas a seu endereço MAC ou ao endereço MAC 802.1X.

O Acces point deve controlar o acesso à rede através da porta controlada numa base de cliente dependente da autenticação do cliente.

O protocolo **EAP** (*Extensible Authentication Protocol*) é um protocolo que suporta a comunicação de informações de autenticação para mecanismos de autenticação múltiplos. Com o 802.1X, o EAP é usado como um meio de comunicar essa informação entre o suplicante e o servidor de autenticação. Isso significa que as mensagens do EAP precisam ser encapsuladas diretamente em um meio LAN. O EAP numa LAN (EAPOL) foi estabelecido com esse objetivo. O autenticador é responsável por retransmitir essas mensagens entre o suplicante e o servidor de autenticação. O servidor de autenticação pode ser um servidor **RADIUS** (Serviço do Usuário de Discagem de Autenticação Remota).

A sequência de troca de mensagens quando um cliente tenta entrar na rede que possui um esquema de autenticação 802.1x é a seguinte. A Figura 2 exibe tal troca de mensagens.

1. Cliente envia pedido de autenticação ao AP (Access Point).
2. AP responde pedindo a identificação do Cliente.
3. Cliente envia sua identificação que é redirecionada pelo AP (Access Point) ao servidor de autenticação
4. Servidor de autenticação verifica a identidade do Cliente e envia uma mensagem de aceitação/negação ao AP (Access Point).
5. Se a identificação for aceita o AP (Access Point) libera o tráfego do Cliente.

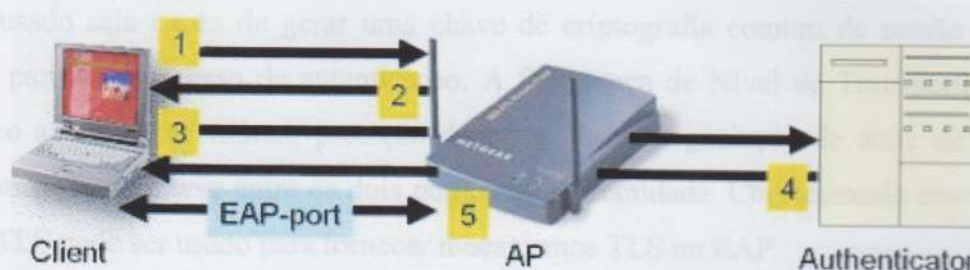


Figura 2: Sequência de troca de mensagens entre os atores do 802.1x

Fonte: Site da Microsoft Brasil

As seguintes etapas ilustram a abordagem básica usada por um Access point (AP) sem-fio e um servidor RADIUS para autenticar uma estação.

- Sem uma chave de autenticação válida, um AP inibe todo o fluxo de transmissão através dele.
- Quando uma estação sem-fio (suplicante) entra na faixa de um autenticador AP sem-fio, o AP sem-fio emite uma solicitação para a estação sem-fio.
- Ao receber a solicitação do AP, a estação responde com sua identidade.
- O AP então encaminha a identidade da estação para o servidor RADIUS (autenticação) para iniciar os serviços de autenticação.
- O servidor RADIUS então solicita as credenciais da estação, especificando o tipo de credenciais necessárias para confirmar a identidade da estação.
- A estação envia suas credenciais para o servidor RADIUS.

- Ao validar as credenciais da estação, o servidor RADIUS transmite a chave de sessão unicast por estação para o AP, que é criptografada de forma que somente o AP possa acessá-la.
- Lembre-se que as solicitações que passam entre a estação e o servidor RADIUS passam pela porta “não controlada” no AP, pois a estação não pode alcançar diretamente o servidor RADIUS. O AP não permite a comunicação através da porta “controlada” porque a estação STA ainda não foi autenticada.
- O AP usa a chave de sessão *unicast* por estação recebida do servidor RADIUS para transmitir de forma segura a criptografia *multicast/global* para a estação.

A chave de criptografia global deve ser criptografada. Isso exige que o método EAP usado seja capaz de gerar uma chave de criptografia comum de sessão unicast como parte do processo de autenticação. A Segurança de Nível de Transporte (TLS) fornece autenticação mútua; proteção da integridade, negociação de suíte de cifra e determinação de chave entre os dois pontos de extremidade. Considerando esse fato, o EAP-TLS pode ser usado para fornecer mecanismos TLS no EAP.

3.6.1 Solucionando questões WEP com 802.1X

Os ataques no WEP discutidos anteriormente podem ser interrompidos das seguintes maneiras:

1. Fornecendo chaves por estação ou por sessão para limitar o número de pacotes que usam a mesma chave.
2. Certificando-se de que as chaves são trocadas com frequência – atribuindo novas chaves a cada 5-10 minutos ou pacotes de 4 milhões. Isso também limita a reutilização de chaves, a principal causa dos ataques citados.

Com o 802.1X implementado e implantado, isso pode ser realizado automaticamente. Após a autenticação, o protocolo 802.1X deve ser configurado para solicitar que a estação faça novas autenticações periodicamente, em intervalos de tempo específicos. O 802.1X fornece, portanto, chaves por estação e por sessão e faz com que essas chaves sejam trocadas frequentemente – eliminando problemas de reutilização. Além disso, o 802.1X permite a identificação e autenticação do usuário e autenticação

centralizada, suporte de autorização e de contas. Isso também permite o uso futuro de mecanismos de autenticação estendidos.

Neste capítulo apresentamos detalhes da implementação da solução de autenticação dos usuários na rede sem fio da FAKN, bem como a instalação do serviço de autenticação da Internet (IAS) utilizando o sistema operacional Microsoft Windows Server 2003, a configuração e a autenticação com o servidor RADIUS.

4.1 SERVIÇO DE AUTENTICAÇÃO DE INTERNET DO WINDOWS SERVER

O Serviço de Autenticação da Internet (IAS) do Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition e do Windows Server 2003, Datacenter Edition é a implementação da Microsoft de um servidor e de um proxy RADIUS (*Remote Authentication Dial-In User Service*). Como um servidor RADIUS, o IAS cuida da autenticação, autorização e estatísticas de eventos centralizadas para vários tipos de acesso à rede, incluindo conexões sem fio, switch de autenticação, acesso remoto através de conexões dial-up e rede virtual privada (VPN) e roteadores roteador a roteador. Como um proxy RADIUS, o IAS encaminha mensagens de autenticação e sobre estatísticas para outros servidores RADIUS. O IAS oferece suporte aos padrões da IETF (*Internet Engineering Task Force*) para RADIUS definidos nos RFCs 2464 e 2865.

O IAS permite utilizar um conjunto heterogêneo de equipamentos para acesso sem fio, por switch, remoto ou por VPN. É possível usar o IAS com o serviço de Tratamento e Acesso Remoto, que está disponível no Microsoft Windows 2003, Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition e no Windows Server 2003, Datacenter Edition.

Quando um servidor IAS é membro de um domínio do Active Directory, ele usa o serviço de diretório como banco de dados de contas de usuários e faz parte de uma política de início de sessão universal. O mesmo conjunto de credenciais é usado para acessar o acesso à rede (acesso a uma rede via autenticação e autorização) e para fazer login no domínio do Active Directory.

Os provedores de serviços de Internet (ISPs) e as organizações que misturam acesso à rede com o desafio maior de gerenciar todos os tipos de acesso à rede por um único grupo de administração, independentemente do tipo de equipamento usado para acesso à rede. O padrão RADIUS oferece suporte a essa funcionalidade em ambientes homogêneos e heterogêneos. O RADIUS é um protocolo cliente/servidor que permite

4 DESENVOLVIMENTO DA SOLUÇÃO

Neste capítulo apresenta-se detalhes da implantação da solução de autenticação dos usuários na rede sem fio da FARN, bem como a instalação do serviço de autenticação da Internet (IAS) utilizando o sistema operacional Microsoft Windows Server 2003, a configuração e a autenticação com o servidor RADIUS.

4.1 SERVIÇO DE AUTENTICAÇÃO DE INTERNET DO WINDOWS SERVER

O Serviço de Autenticação da Internet (IAS) do Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition e do Windows Server 2003, Datacenter Edition é a implementação da Microsoft de um servidor e de um *proxy* RADIUS (*Remote Authentication Dial-In User Service*). Como um servidor RADIUS, o IAS cuida da autenticação, autorização e estatísticas de conexões centralizadas para vários tipos de acesso à rede, incluindo conexões sem fio, switch de autenticação, acesso remoto através de conexões *dial-up* e rede virtual privada (VPN) e conexões roteador a roteador. Como um *proxy* RADIUS, o IAS encaminha mensagens de autenticação e sobre estatísticas para outros servidores RADIUS. O IAS oferece suporte aos padrões da IETF (*Internet Engineering Task Force*) para RADIUS descritos nas RFCs 2865 e 2866.

O IAS permite utilizar um conjunto heterogêneo de equipamentos para acesso sem fio, por switch, remoto ou por VPN. É possível usar o IAS com o serviço de Roteamento e Acesso Remoto, que está disponível no Microsoft Windows 2000, Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition e no Windows Server 2003, Datacenter Edition.

Quando um servidor IAS é membro de um domínio do Active Directory, ele usa o serviço de diretório como banco de dados de contas de usuários e faz parte de uma solução de início de sessão universal. O mesmo conjunto de credenciais é usado para controlar o acesso à rede (acesso a uma rede via autenticação e autorização) e para fazer login em um domínio do Active Directory.

Os provedores de serviços de Internet (ISPs) e as organizações que mantêm acesso à rede têm o desafio maior de gerenciar todos os tipos de acesso à rede em um único ponto de administração, independentemente do tipo de equipamento usado para acessar a rede. O padrão RADIUS oferece suporte a essa funcionalidade em ambientes homogêneos e heterogêneos. O RADIUS é um protocolo cliente/servidor que permite

ao equipamento usado para acessar a rede (utilizado como cliente RADIUS) enviar solicitações de estatísticas e autenticação a um servidor RADIUS.

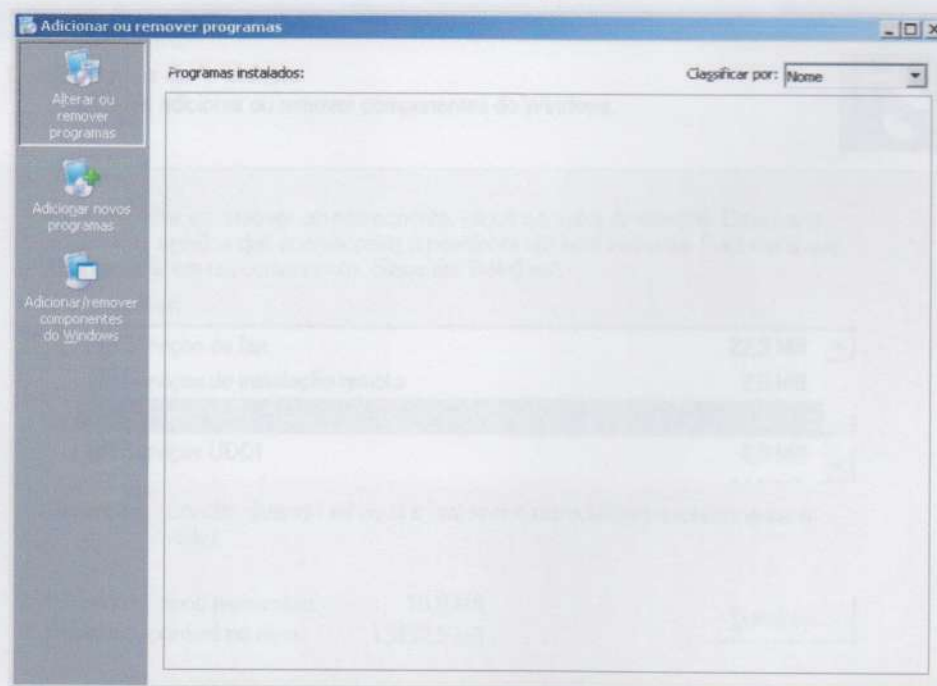
Um servidor RADIUS tem acesso a informações de contas de usuários e pode verificar as credenciais de autenticação de acesso à rede. Se as credenciais do usuário forem autênticas e a tentativa de conexão for autorizada, o servidor RADIUS autorizará o acesso do usuário com base nas condições especificadas e registrará a conexão de acesso à rede no log de estatísticas. O uso do RADIUS permite que os dados de autenticação, autorização e estatísticas do usuário que acessa a rede sejam coletados e armazenados em um local central e não em cada servidor de acesso.

Com o IAS, as organizações também podem terceirizar a infra-estrutura de acesso remoto para um provedor de serviços, ao mesmo tempo em que detêm o controle dos processos de autenticação, autorização e estatísticas do usuário. Na seção 3.1.1 será abordado a como proceder na instalação do IAS no Windows Server 2003.

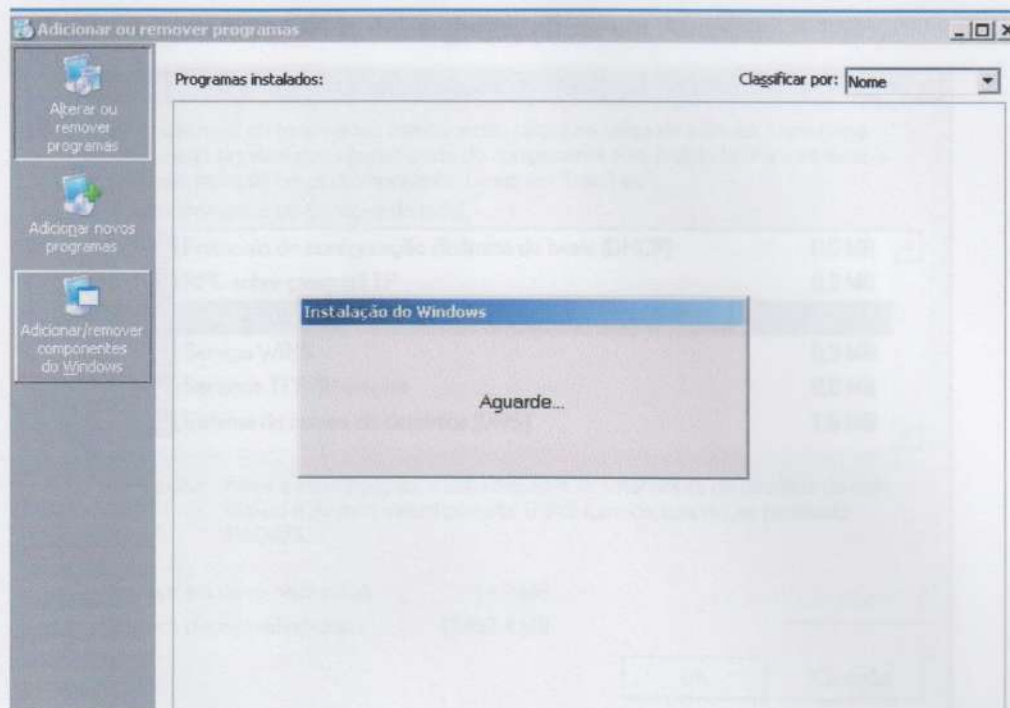
4.1.1 Instalação do IAS no Windows Server 2003

Os procedimentos para instalar o IAS no Windows Server 2003 são os seguintes:

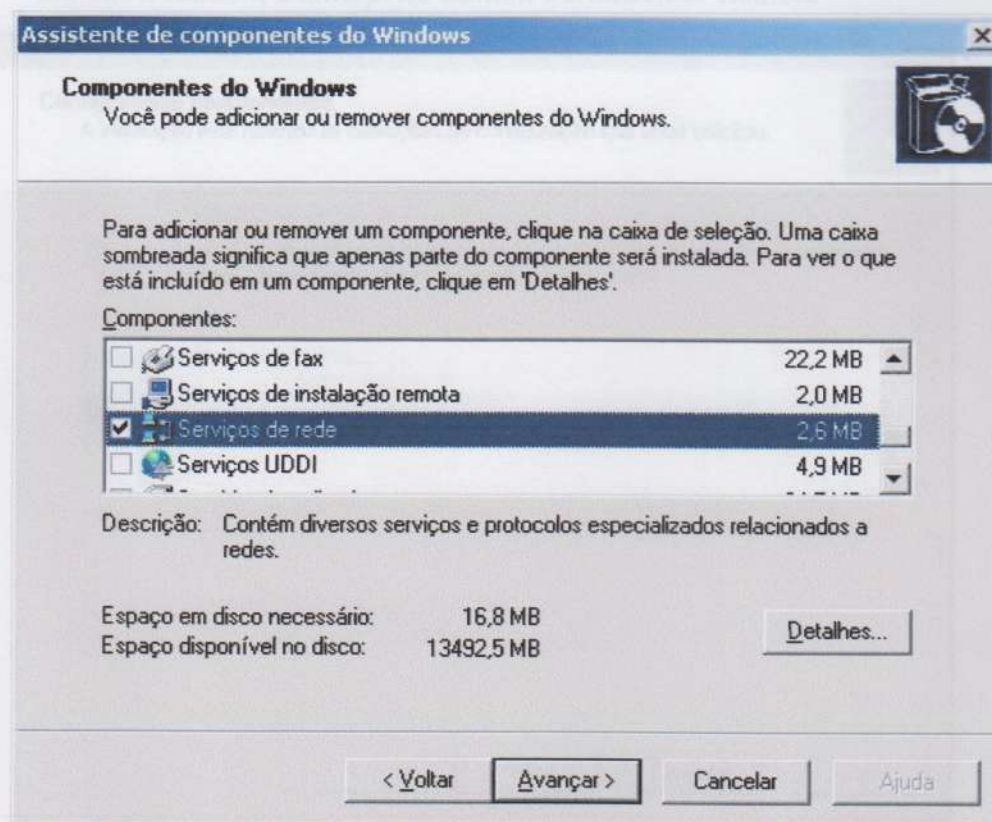
1. Abrir a opção Adicionar ou Remover Programas no Painel de Controle.



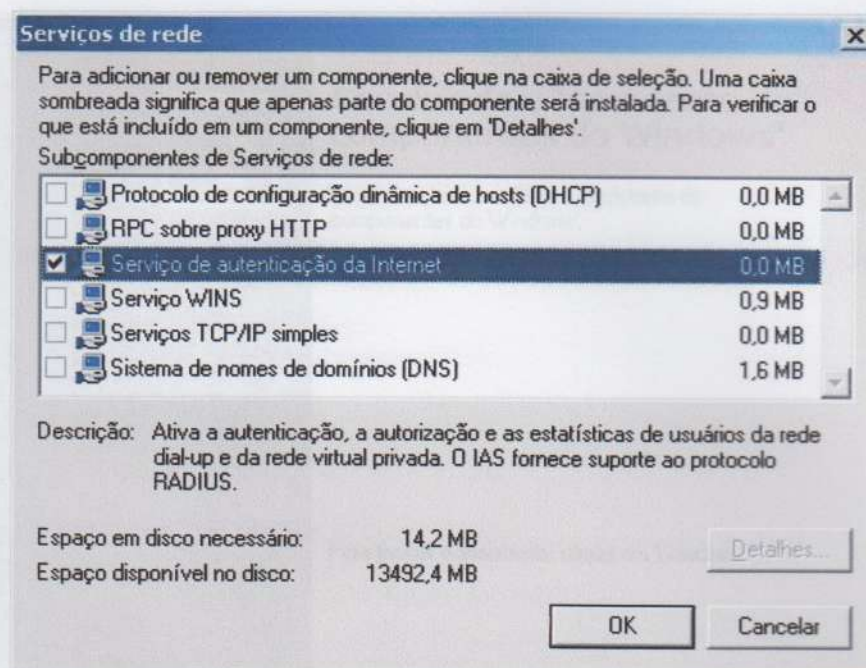
2. Clicar em Adicionar ou Remover Componentes do Windows.



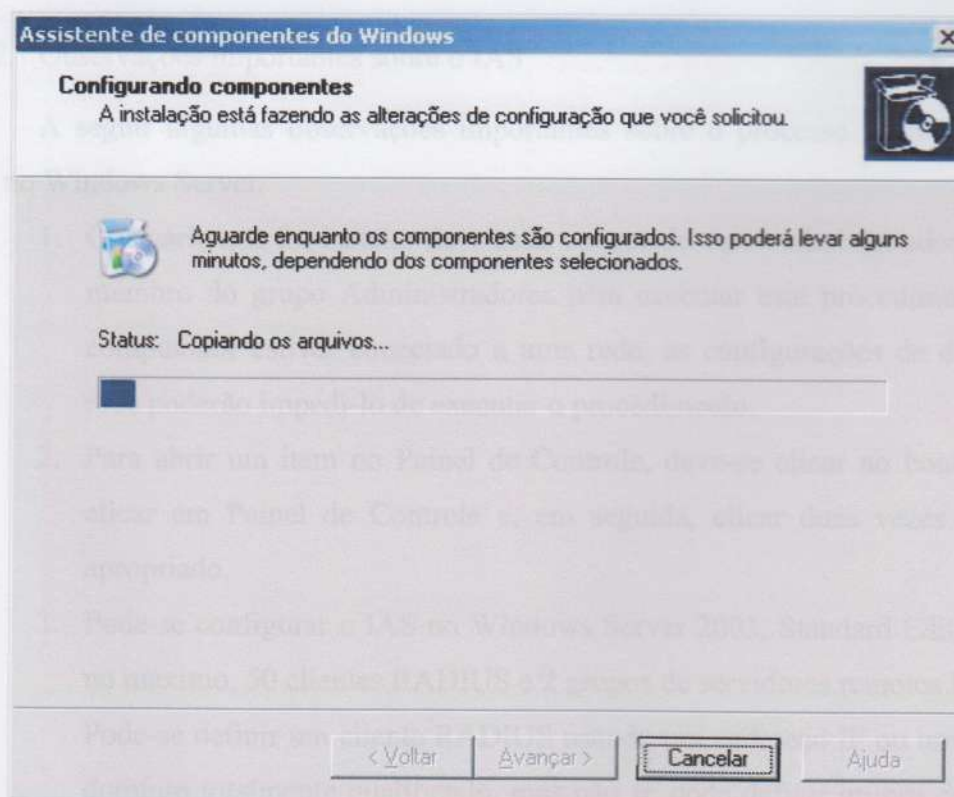
3. Na caixa de diálogo Assistente de Componentes do Windows, clicar em Serviços de Rede e, em seguida, clicar em Detalhes.



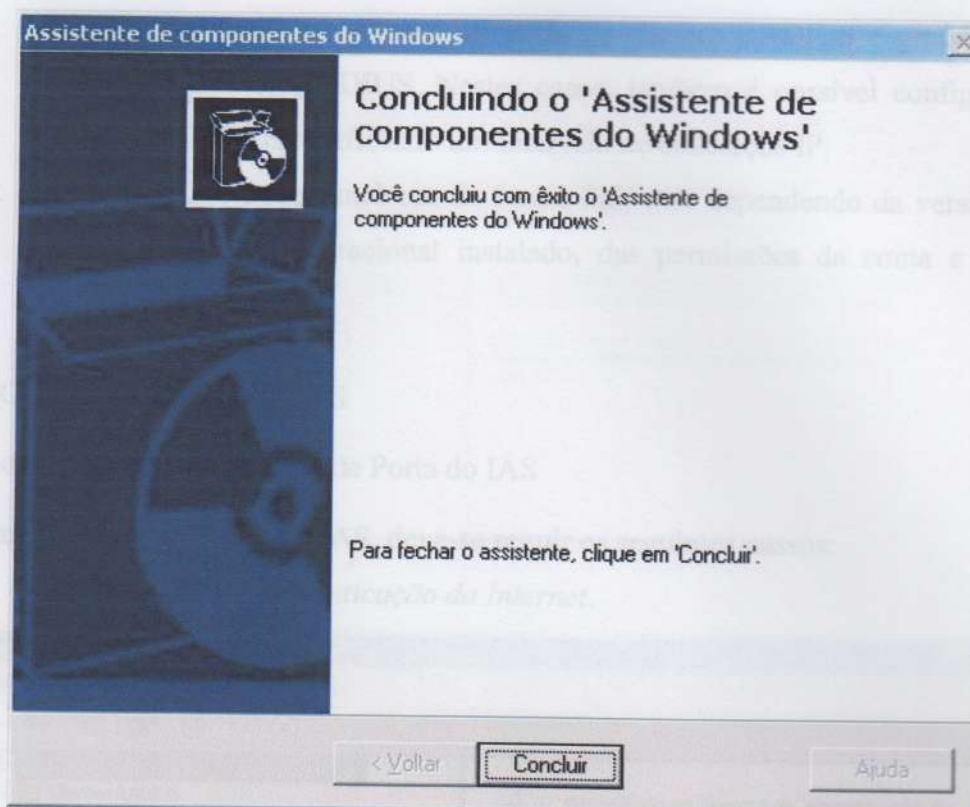
4. Na caixa de diálogo Serviços de Rede, selecionar Serviço de Autenticação da Internet, clicar em OK e, em seguida, clicar em Avançar.



5. Se solicitado, inserir o CD de instalação do Windows Server 2003 seja ela a *Standard Edition*, a *Enterprise Edition* a *Datacenter Edition*.



6. Após a instalação do IAS, clicar em Concluir e, em seguida, clicar em Fechar.



4.1.2 Observações importantes sobre o IAS

A seguir algumas observações importantes sobre o processo de instalação do IAS no Windows Server.

1. O usuário que for instalar deve estar conectado como administrador ou como membro do grupo Administradores para executar este procedimento. Se o computador estiver conectado a uma rede, as configurações de diretiva de rede poderão impedi-lo de executar o procedimento.
2. Para abrir um item no Painel de Controle, deve-se clicar no botão Iniciar, clicar em Painel de Controle e, em seguida, clicar duas vezes no ícone apropriado.
3. Pode-se configurar o IAS no Windows Server 2003, Standard Edition, com, no máximo, 50 clientes RADIUS e 2 grupos de servidores remotos RADIUS. Pode-se definir um cliente RADIUS usando um endereço IP ou um nome de domínio totalmente qualificado, mas não se pode definir grupos de clientes RADIUS especificando um intervalo de endereços IP. Se o nome de domínio totalmente qualificado de um cliente RADIUS resolve vários endereços IP, o

servidor IAS usa o primeiro endereço IP retornado na consulta DNS. Com o IAS no Windows Server 2003, *Enterprise Edition*, ou *Datacenter Edition*, pode-se configurar um número ilimitado de clientes RADIUS e grupos de servidores remotos RADIUS. Nestes casos, também é possível configurar clientes RADIUS especificando um intervalo de endereços IP.

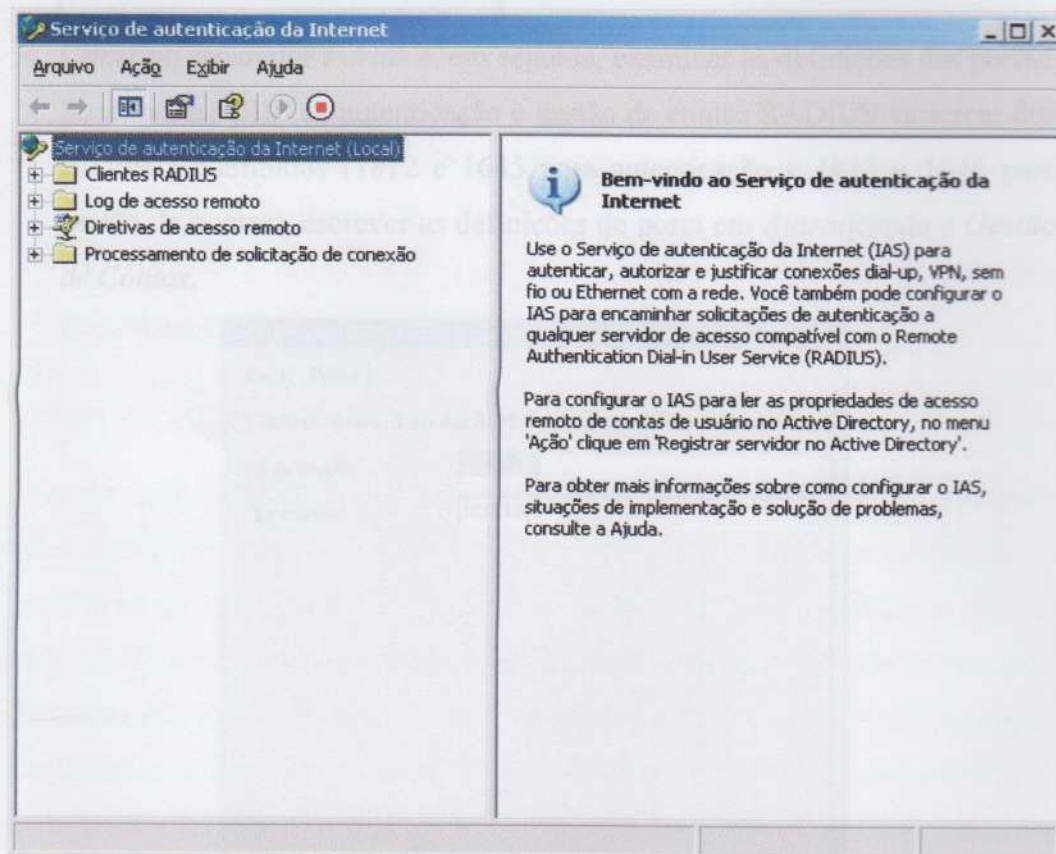
4. O servidor IAS pode funcionar de forma diferente dependendo da versão e edição do sistema operacional instalado, das permissões da conta e das configurações de menu.

4.2 CONFIGURAÇÃO DO IAS

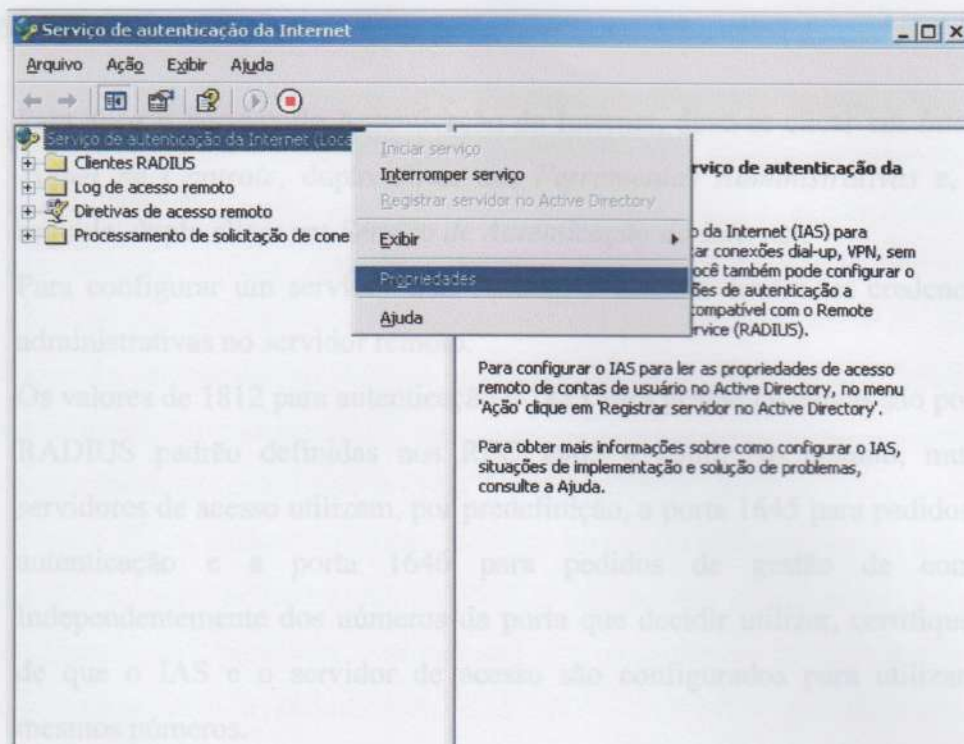
4.2.1 Configurando informações de Porta do IAS

Para configurar a porta do IAS, deve-se seguir os seguintes passos:

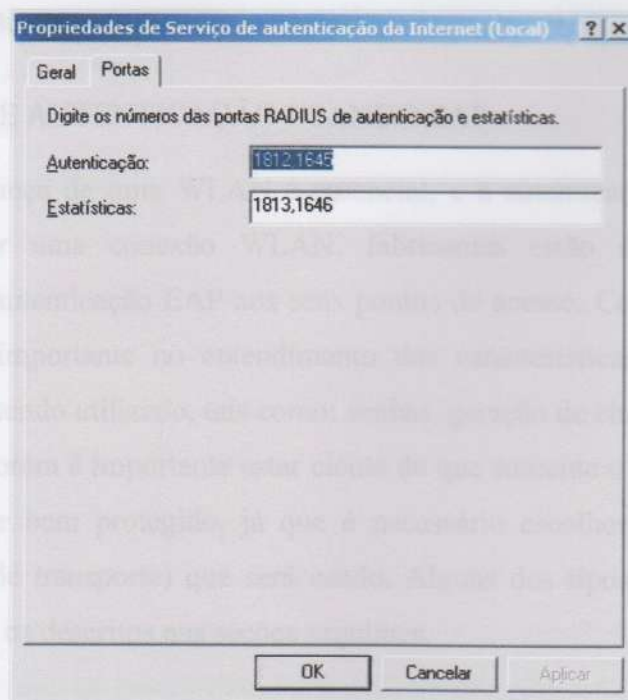
1. Abrir o *Serviço de Autenticação da Internet*.



2. Clicar com o botão direito do mouse em *Serviço de Autenticação da Internet* e, em seguida, clicar em *Propriedades*.



3. Clicar no separador *Portas* e, em seguida, examinar as definições das portas. Se as portas UDP de autenticação e gestão de contas RADIUS variarem dos valores predefinidos (1812 e 1645 para autenticação e 1813 e 1646 para gestão de contas), escrever as definições de porta em *Autenticação e Gestão de Contas*.



Para utilizar várias definições de porta para autenticação ou pedidos de gestão de contas, separe os números das portas com vírgulas.

Observações:

1. Para abrir o Serviço de Autenticação da Internet, deve-se clicar em *Iniciar*, *Painel de Controle*, duplo clicar em *Ferramentas Administrativas* e, em seguida, duplo clicar em *Serviço de Autenticação da Internet*.
2. Para configurar um servidor IAS remoto, o usuário deverá ter credenciais administrativas no servidor remoto.
3. Os valores de 1812 para autenticação e 1813 para gestão de contas são portas RADIUS padrão definidas nos RFC 2865 e 2866. No entanto, muitos servidores de acesso utilizam, por predefinição, a porta 1645 para pedidos de autenticação e a porta 1646 para pedidos de gestão de contas. Independentemente dos números da porta que decidir utilizar, certifique-se de que o IAS e o servidor de acesso são configurados para utilizar os mesmos números.
4. Pode-se especificar um endereço IP para o qual as mensagens RADIUS têm de ser enviadas com a seguinte sintaxe: *EndereçoIP: PortaUDP*. Por exemplo, se tiver várias placas de rede e apenas pretender receber as mensagens de autenticação RADIUS enviadas para o endereço IP de 10.0.0.99 e a porta UDP 1812, deverá escrever 10.0.0.99: 1812 em Autenticação.

4.3 PROCESSO DE AUTENTICAÇÃO USANDO EAP

Como a segurança de uma WLAN é essencial, e a autenticação EAP fornece meios para assegurar uma conexão WLAN, fabricantes estão desenvolvendo e adicionando tipos de autenticação EAP aos seus pontos de acesso. Conhecer o tipo de autenticação EAP é importante no entendimento das características do método de autenticação que está sendo utilizado, tais como: senhas, geração de chave, autenticação mútua e protocolos. Porém é importante estar ciente de que somente o uso do EAP não é suficiente para estar bem protegido, já que é necessário escolher o tipo de EAP (protegem a camada de transporte) que será usado. Alguns dos tipos de autenticação EAP mais comuns são os descritos nas seções seguintes.

4.3.1 EAP-MD5

O EAP-MD5 (*Message Digest 5*) é um tipo de EAP que utiliza o mesmo protocolo de autenticação *Challenge Handshake* (CHAP, *Challenge Handshake Protocol*) que o CHAP baseado em PPP, mas as contestações e as respostas são enviadas como mensagens EAP. EAP-MD5 fornece uma forma simples de centralizar as informações de autenticação de clientes da rede em um servidor RADIUS. Neste esquema, o servidor não requer certificados ou outra informação de segurança instalado nas máquinas clientes. No momento do login, o servidor RADIUS verifica o nome do usuário e a senha fornecida pelo usuário. Uma vez que o usuário tenha se autenticado, o servidor informa o AP da autenticação bem sucedida e a partir daí dados podem trafegar entre o cliente e a rede, normalmente. EAP-MD5 só fornece autenticação. Mas, é possível configurar o AP para usar qualquer um dos mecanismos de criptografia do 802.11 em conjunto com a autenticação EAP-MD5. EAP-MD5 um esquema de autenticação conhecido como *one-way* (somente em um sentido): ele autentica o cliente para o servidor, mas não autentica o servidor para o cliente. Além deste problema, ele não é mais suportado pelo Windows XP para conexões sem fio.

4.3.2 EAP-TLS

O EAP-*Transport Level Security* (EAP-TLS) é um tipo de EAP utilizado em ambientes de segurança com base em certificados. O padrão 802.1X para controle de acesso à rede combinado a um método de autenticação protegido. Nesta seção será abordado o Conceito da solução baseada na autenticação EAP-TLS do 802.1X que é exibido na figura do diagrama abaixo.

Na Figura 3 é retratado quatro componentes principais:

- **O cliente sem fio:** Este é um computador ou dispositivo que executa um aplicativo que requer acesso aos recursos da rede. O cliente possui a capacidade de criptografar seu tráfego de rede e de armazenar e intercambiar com segurança as credenciais (como chaves ou senhas).
- **O AP sem fio:** Implementa as funções de controle de acesso para permitir ou negar o acesso à rede e fornece a capacidade de criptografar o tráfego sem fio. Ele também possui os meios para intercambiar com segurança as chaves de criptografia com o cliente para proteger o tráfego da rede. Por fim, ele pode

pesquisar um serviço de autenticação e autorização para as decisões de autorização.

- **O processo NAAS (Network Authentication and Authorization Service).** Ele armazena e verifica as credenciais de usuários válidos e toma as decisões de autorização com base em uma diretiva de acesso. Ele também pode coletar informações sobre contas e auditoria sobre o acesso do cliente à rede. Ele é usado aqui somente por conveniência.
- **A rede interna.** Esta é uma área protegida dos serviços de rede à qual o aplicativo de cliente sem fio precisa obter acesso.

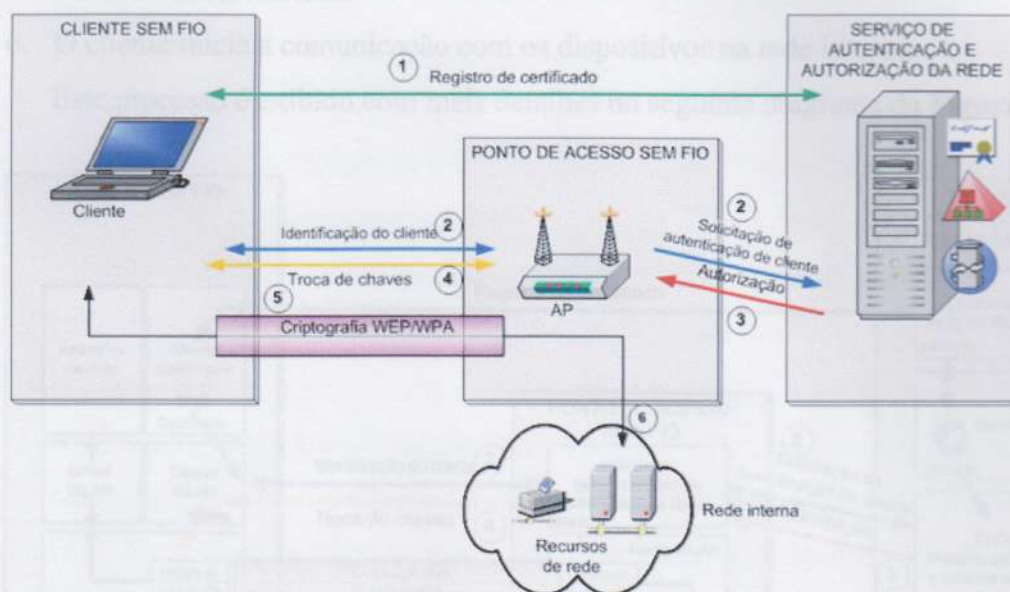


Figura 3: Solução baseada na autenticação EAP-TLS
Fonte: Site da Microsoft Brasil

Abaixo está descrito com mais detalhes as etapas do Processo de acesso 802.1x EAP-TLS:

1. O cliente sem fio deve em algum ponto estabelecer as credenciais com uma autoridade central antes do acesso à rede sem fio ser estabelecido. (Este pode ser por meio de um método fora de padrão - por exemplo, por intermédio da troca de disquete - ou pode ocorrer em uma rede cabeada ou outra rede protegida.).
2. Quando o cliente requer o acesso à rede, ele passa suas credenciais (ou mais precisamente, a evidência de que ele detém as credenciais) para o AP sem fio; O AP sem fio as passa em seguida para o NAAS para solicitar autorização.

3. O NAAS verifica as credenciais, consulta sua diretiva de acesso e também concede ou nega autorização ao cliente.
4. Se o cliente foi autorizado, o acesso será concedido e o cliente fará o intercâmbio das chaves de criptografia com segurança com o AP sem fio. (As chaves são na verdade geradas pelo NAAS e transmitidas ao AP sem fio por um canal seguro.) Se o cliente não foi autorizado pelo NAAS, o acesso é negado e nenhuma comunicação posterior ocorre.
5. Com o uso de chaves de criptografia, o cliente e o AP sem fio estabelecem uma conexão segura com o link sem fio e a conectividade é estabelecida entre o cliente e a rede interna.
6. O cliente inicia a comunicação com os dispositivos na rede interna.

Este processo é exibido com mais detalhes no seguinte diagrama da **Figura 4**.

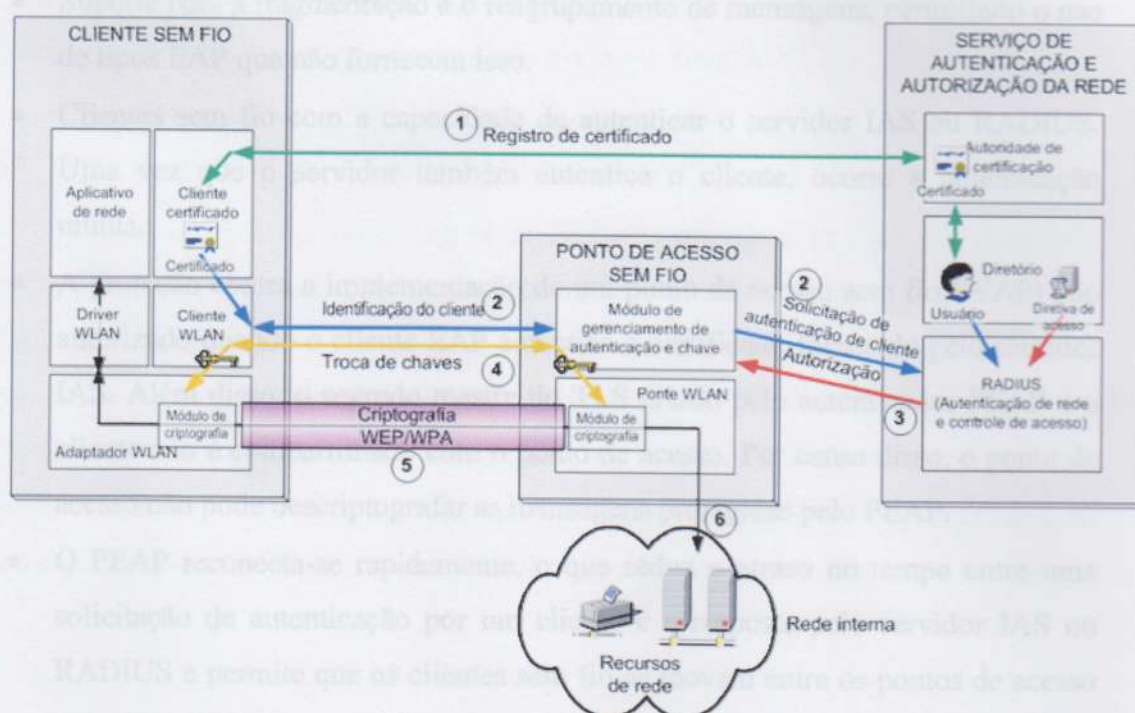


Figura 4: Processo de acesso 802.1X EAP-TLS

Fonte: Site da Microsoft Brasil

4.3.3 EAP-PEAP

O Protocolo de Autenticação Extensível Protegido (PEAP) é um novo membro da família dos protocolos EAP. O PEAP usa o *Transport Level Security* (TLS) para criar um canal criptografado entre um cliente PEAP de autenticação, como um

computador sem fio, e um autenticador PEAP, como um servidor RADIUS. O PEAP não especifica um método de autenticação, mas fornece segurança adicional para outros protocolos de autenticação EAP, como EAP-MSCHAPv2, que podem operar pelo canal criptografado TLS fornecido pelo PEAP. O PEAP é usado como um método de autenticação para computadores clientes sem fio 802.11, mas não há suporte para rede virtual privada (VPN) ou outros clientes de acesso remoto.

Para aprimorar os protocolos EAP e a segurança de rede, o PEAP fornece:

- Proteção para a negociação do método EAP que ocorre entre o cliente e o servidor por um canal TLS. Isso ajuda a impedir que um invasor insira pacotes entre o cliente e o servidor de acesso à rede (NAS) para forçar a negociação de um método EAP menos seguro. O canal TLS criptografado também ajuda a impedir os ataques de negação de serviço contra o servidor IAS.
- Suporte para a fragmentação e o reagrupamento de mensagens, permitindo o uso de tipos EAP que não fornecem isso.
- Clientes sem fio com a capacidade de autenticar o servidor IAS ou RADIUS. Uma vez que o servidor também autentica o cliente, ocorre a autenticação mútua.
- A proteção contra a implementação de um ponto de acesso sem fio (WAP) não autorizado quando o cliente EAP autentica o certificado fornecido pelo servidor IAS. Além disso, o segredo mestre do TLS criado pelo autenticador PEAP e o cliente não é compartilhado com o ponto de acesso. Por causa disso, o ponto de acesso não pode descriptografar as mensagens protegidas pelo PEAP.
- O PEAP reconecta-se rapidamente, o que reduz o atraso no tempo entre uma solicitação de autenticação por um cliente e a resposta pelo servidor IAS ou RADIUS e permite que os clientes sem fio se movam entre os pontos de acesso sem as solicitações repetitivas para autenticação. Isso reduz as exigências de recursos para cliente e servidor.

4.3.3.1 Processo de autenticação do PEAP

Existem dois estágios no processo de autenticação PEAP entre o autenticador e o cliente PEAP. O primeiro estágio configura um canal seguro entre o cliente PEAP e o servidor de autenticação. O segundo estágio fornece a autenticação EAP entre o autenticador e o cliente EAP.

O cliente sem fio associa-se a um ponto de acesso sem fio. Uma associação com base em IEEE 802.11 fornece uma Autenticação de Chave Compartilhada ou um Sistema Aberto antes que uma associação segura seja criada entre o ponto de acesso e o cliente. Depois que uma associação com base em IEEE 802.11 é estabelecida com êxito entre o cliente e o ponto de acesso, a sessão TLS é negociada com o ponto de acesso. Depois que a autenticação entre o cliente sem fio e o servidor é concluída com êxito (por exemplo, um servidor IAS), a sessão TLS é negociada entre eles. A chave derivada durante esta negociação é usada para criptografar toda a comunicação subsequente.

A comunicação EAP completa, incluindo a negociação EAP, ocorre pelo canal TLS. O servidor IAS autentica o computador cliente e o usuário com o método que é determinado pelo tipo de EAP e selecionado para uso no PEAP (EAP-TLS ou EAP-MS-CHAPv2). O ponto de acesso só encaminha mensagens entre o cliente sem fio e o servidor RADIUS—o ponto de acesso (ou a pessoa que o monitora) não pode descriptografar essas mensagens porque não é o ponto final do TLS.

4.3.3.2 Implementações sem fio do 802.11 usando PEAP

É possível escolher entre dois tipos de EAP para uso com o PEAP: EAP-MS-CHAPv2 ou EAP-TLS. O EAP-MS-CHAPv2 usa credenciais (nome do usuário e senha) para autenticação do usuário e um armazenamento de certificados do computador servidor para autenticação do servidor. O EAP-TLS usa certificados instalados no armazenamento de certificados do computador cliente ou um cartão inteligente para autenticação do computador cliente e usuário e um certificado no armazenamento de certificados do computador servidor para autenticação do servidor.

4.3.3.2.1 PEAP com EAP-MS-CHAPv2

O PEAP com EAP-MS-CHAPv2 (PEAP-EAP-MS-CHAPv2) é mais fácil de ser implementado do que o EAP-TLS uma vez que a autenticação do usuário é realizada com credenciais com base na senha (nome do usuário e senha) em vez de certificados ou cartões inteligentes—exige-se apenas que o servidor IAS ou RADIUS tenha um certificado. Além disso, o certificado do servidor pode ser emitido por uma autoridade de certificação (CA) pública na qual o computador cliente confie (ou seja, o certificado CA público já existe na pasta Autoridade de Certificação Raiz Confiável no armazenamento de certificados do computador cliente). Nesse caso, o certificado do

servidor não é obtido por download e adicionado ao armazenamento de certificados raiz confiáveis do cliente e o usuário não é solicitado a tomar uma decisão sobre se deve confiar no servidor.

O PEAP-EAP-MS-CHAPv2 fornece segurança melhorada pelo MS-CHAPv2 usando autenticação mútua, impedindo que um servidor não autorizado negocie o método de autenticação menos seguro e fornecendo a geração de chaves com TLS. O PEAP-EAP-MS-CHAPv2 exige os certificados de confiança de clientes fornecidos pelo servidor.

Para obter as exigências do certificado do computador cliente e servidor, consulte Autenticação de acesso à rede e certificados. Para obter um exemplo de diretiva de acesso sem fio usando o PEAP-EAP-MS-CHAPv2, consulte Acesso sem fio com autenticação de senha protegida.

4.3.3.2.2 PEAP com EAP-TLS

Os certificados de chave pública fornecem um método de autenticação mais forte do que aquele que usa credenciais com base em senha. O PEAP com EAP-TLS (PEAP-EAP-TLS) usa certificados para autenticação de servidores e certificados ou cartões inteligentes ou para autenticação de usuários e de computadores cliente. Para usar PEAP-EAP-TLS, você deve implantar uma infra-estrutura de chave pública (PKI).

4.3.3.3 Reconexão rápida do PEAP

A reconexão rápida do PEAP permite que os clientes sem fio se movam entre os pontos de acesso sem fio na mesma rede sem serem autenticados novamente cada vez que você se associar a um novo ponto de acesso.

Os pontos de acesso sem fio são configurados como clientes RADIUS para servidores RADIUS. Se um cliente sem fio for movido entre os pontos de acesso configurados como clientes para o mesmo servidor RADIUS, o cliente não terá que ser autenticado a cada nova associação. Quando um cliente se move para um ponto de acesso configurado como um cliente RADIUS para um servidor RADIUS diferente, embora o cliente seja autenticado novamente, este processo ocorrerá de maneira mais eficiente.

A reconexão rápida do PEAP reduz o tempo de resposta para autenticação entre o cliente e o autenticador, uma vez que a solicitação de autenticação é encaminhada do

novo servidor para o servidor original. Uma vez que o autenticador e o cliente PEAP usam as propriedades de conexão por TLS armazenadas em *cache* anteriormente (a coleta a partir da qual o manipulador TLS é nomeado), o autenticador pode determinar rapidamente se a conexão do cliente deve ser reconectada.

Se o autenticador PEAP original não está disponível, deve ocorrer a autenticação completa entre o cliente e o novo autenticador. O manipulador TLS do novo autenticador PEAP é armazenado em *cache* pelo cliente. O cliente pode armazenar em *cache* os manipuladores TLS para diversos autenticadores PEAP. Para cartões inteligentes ou autenticação PEAP-EAP-MSCHAPv2, o usuário é solicitado a fornecer o PIN ou as credenciais, respectivamente.

4.3.4 EAP-TTLS

É um tipo de autenticação que usa o EAP (*Extensible Authentication Protocol*) e o TTLS (*Tunneled Transport Layer Security*). O EAP-TTLS usa uma combinação de certificados e um outro método, como senhas. Ele é mais seguro do que a autenticação MD5, que usa senhas, e menos seguro que a autenticação EAP-TLS, que usa exclusivamente certificados. A autenticação EAP-TTLS suporta gerenciamento dinâmico de chaves WEP. No caso EAP/TTLS será necessário o usuário instalar um software cliente em seu computador que tem por função fornecer suporte à autenticação via login e senha para acesso à rede *wireless* da instituição. Caso o usuário não tenha direito a uma conta na rede da instituição ou deseje efetuar o acesso mediante autenticação por certificado digital pessoal (EAP/TLS), a instalação deste software é necessária.

5 CONCLUSÃO

Nesta Monografia foi apresentado o conceito sobre redes de computadores, redes locais sem fio (*wireless*), uma visão geral sobre o padrão IEEE 802.11, segurança em redes locais sem fio, prevenção de segurança em redes Wi-Fi, e por fim um estudo sobre o protocolo de autenticação 802.1x. Foram apresentadas os esquemas de autenticação EAP-MD5, EAP-TLS, EAP-TTLS e PEAP.

Durante as minhas pesquisas foi constatado que entre os métodos de autenticação estudados, o mais seguro para ser utilizado em uma rede sem fio é o método de autenticação EAP-TLS, por ele possuir mais segurança que os demais métodos e não necessitar de algum software para a sua configuração.

Esta monografia tinha como propósito implementar o protocolo de autenticação 802.1x, mas devido ao problema de emissão dos certificados e também nos problemas de comunicação da AP com o servidor Radius não foi possível realização dos testes.

Este trabalho servirá de base para projetos futuros relacionados a este tema e que poderão ser implementados qualquer um dos métodos de autenticação estudados.

REFERÊNCIAS

Grupo Meta - **Artigo Escolhendo uma estratégia para a segurança da LAN sem fio** Disponível em

http://www.microsoft.com/brasil/security/guidance/lans/peap_int.mspix, Acessado em 19/04/2006.

Guia do usuário de rede sem fio Access Point 8000

<http://support.3com.com/registration/frontpg.pl> Acessado em 27/10/2006

Melo, Fred. - **Enciclopédia Virtual de Redes de Computadores**, Disponível em: <http://www.webpuc.hpg.ig.com.br/oquesao.html>, Acessado em 21/04/2006.

Microsoft Technet - <http://www.microsoft.com/technet/>, Acessado em 25/08/2006.

Murilo, Nelson - **Segurança em redes Wi-Fi** Disponível em: <http://informatica.terra.com.br/wifi/interna/0,,OI452200-EI4254,00.html>. Acessado em 18/04/2006

Neto - **Clube do hardware** Disponível em: <http://forum.clubedohardware.com.br/index.php?showtopic=216806> Acessado em 21/04/2006.

Rigonatti, Thiago - **Webinsider**, Disponível em <http://webinsider.uol.com.br/vernoticia.php/id/2233> acessado em 21/04/2006.

Schlemer, Elgio - **Segurança em Redes**, Disponível em www.inf.ufrgs.br/~elgios/trabs-html/redes/seg_rede.html, Acessado em 22/04/2006.
www.ime.unicamp.br/wireless/IMECC_Wireless_Windows.pdf, Acessado em 01/11/2006.

Tom Fout e Warren Barkley - **Site da Microfot Brasil** Disponível em: <http://www.microsoft.com/brasil/windowsxp/pro/techinfo/administracao/wirelesssecurity/default.mspix>, Acessado em 20/04/2006.

Glossário

AP: (Access Point) - É o nó que coordena a comunicação entre as STAAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

BLUETOOTH: Bluetooth é um padrão para comunicação sem-fio, de curto alcance e baixo custo. Através dele permite-se a comunicação sem fio entre aparelhos eletrônicos que podem ser telefones celulares, PDA's, computadores, scanners, impressoras, equipamentos de escritório, enfim, qualquer aparelho que possua um chip Bluetooth.

BSS: (Basic Service Set) - Corresponde a uma célula de comunicação na rede sem fio.

CSMA: (Carrier Sense Multiple Access/CSSA), do inglês *Carrier Sense Multiple Access with Collision Detection*, é um protocolo de telecomunicação que organiza a forma como as computadores compartilham o canal.

APÊNDICE

EAP-TLS: (EAP-Segureza Transport) É um tipo de EAP usado em ambientes de segurança baseados em certificado. Ele fornece o método de autenticação e determinação de chave mais seguro.

EAP: (protocolo de autenticação extensível), um mecanismo de autenticação arbitrária utilizada para concessão de acesso remoto.

EAP-MD5: O Message Digest 5 Challenge (MD5-Challenge) é um tipo de EAP obrigatório que utiliza o mesmo protocolo de autenticação Challenge Handshake (CHAP, *challenge handshake protocol*) que o CHAP baseado em PPP, mas as solicitações e as respostas são enviadas como mensagens EAP.

EAPOL: É um método de encapsular mensagens EAP para poderem ser enviadas através de protocolos Ethernet ou rede local sem fio.

EAP-TTLS: Um tipo de autenticação (que usa o EAP (Extensible Authentication Protocol) e o TLS (Transport Layer Security). O EAP-TTLS usa uma combinação de certificados e um outro método, como senhas. Ele é mais seguro do que a autenticação MD5, que usa senhas, e menos seguro que a autenticação EAP-TLS, que usa exclusivamente certificados.

GLOSSÁRIO

AP: (Access Point) - É o nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

BLUETOOTH: Bluetooth é um padrão para comunicação sem-fio, de curto alcance e baixo custo. Através dele permite-se a comunicação sem fio entre aparelhos eletrônicos que podem ser telefones celulares, Palmtops, computadores, scanners, impressoras, equipamentos de escritório, enfim, qualquer aparelho que possua um chip Bluetooth.

BSS: (Basic Service Set) - Corresponde a uma célula de comunicação da rede sem fio.

CSMA: Em ciência da computação, **CSMA/CD**, do inglês *Carrier Sense Multiple Access with Collision Detection*, é um protocolo de telecomunicação que organiza a forma como os computadores compartilham o canal.

EAP-TLS: (EAP-Segurança de Camada de Transporte) É um tipo de EAP usado em ambientes de segurança baseados em certificado. Ele fornece o método de autenticação e determinação de chave mais seguro.

EAP: (protocolo de autenticação extensível), um mecanismo de autenticação arbitrária autentica uma conexão de acesso remoto.

EAP-MD5: O Message Digest 5 Challenge (MD5-Challenge) é um tipo de EAP obrigatório que utiliza o mesmo protocolo de autenticação Challenge Handshake (CHAP, *challenge handshake protocol*) que o CHAP baseado em PPP, mas as contestações e as respostas são enviadas como mensagens EAP.

EAPOL: É um método de encapsular mensagens EAP para poderem ser enviadas através de segmentos Ethernet ou rede local sem fio.

EAP-TTLS: Um tipo de autenticação que usa o EAP (Extensible Authentication Protocol) e o TTLS (Tunneled Transport Layer Security). O EAP-TTLS usa uma combinação de certificados e um outro método, como senhas. Ele é mais seguro do que a autenticação MD5, que usa senhas, e menos seguro que a autenticação EAP-TLS, que usa exclusivamente certificados.

HOTSPOTS: É o nome dado ao local onde a tecnologia Wi-Fi está disponível. São locais públicos como cafés, restaurantes, hotéis e aeroportos onde você pode se conectar à internet utilizando um notebook, PDA ou um videogame portátil, como um PlayStation Portable (PSP) ou um Nintendo DS.

HTTP: Significa *HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto) e é um protocolo da camada de "Aplicação" do modelo OSI, utilizado para transferência de dados na World Wide Web.

HTTPS: (*HyperText Transfer Protocol Secure*), é uma implementação do protocolo HTTP sobre uma camada SSL ou do TLS, essa camada adicional permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais.

IAS: O Serviço de Autenticação da Internet (IAS) do Microsoft® Windows Server™ 2003, Standard Edition, Windows Server 2003, Enterprise Edition e do Windows Server 2003, Datacenter Edition é a implementação da Microsoft de um servidor e de um proxy RADIUS (Remote Authentication Dial-In User Service).

IEEE: (**Institute of Electrical and Electronics Engineers**): Organização de engenharia que cria as normas de computação e comunicações.

IETF: (sigla em inglês de Internet Engineering Task Force) é uma comunidade internacional ampla e aberta (técnicos, agências, fabricantes, fornecedores, pesquisadores) preocupada com a evolução da arquitetura da Internet e seu perfeito funcionamento.

INFRARED : (infravermelho)

LAN: São redes utilizadas na interconexão de equipamentos processadores com a finalidade de troca de dados.

MAC: Endereço MAC (Media Access Control): Endereço incorporado no dispositivo e aplicado na fábrica. Identifica de forma exclusiva o hardware da rede, por exemplo, uma placa de PC sem fio numa LAN ou numa WAN.

MS-CHAP: A família Windows Server 2003 inclui suporte para o Protocolo de Autenticação Challenge Handshake da Microsoft (MS-CHAP), também conhecido como MS-CHAP versão 1.

PEAP: O Protocolo de Autenticação Extensível Protegido (PEAP) é um novo membro da família dos protocolos Protocolo de Autenticação Extensível (EAP). O PEAP usa o Transport Level Security (TLS) para criar um canal criptografado entre um cliente PEAP de autenticação, como um computador sem fio, e um autenticador PEAP, como um serviço de autenticação da Internet (IAS) ou servidor Remote Authentication Dial-In User Service (RADIUS).

PEAP-MS-CHAP: Autenticação segura baseada em nome de usuário/senha; suporta distribuição de chave automática.

PKI: Infra-estrutura de chave pública (PKI)

RADIUS: (*Remote Authentication Dial-In User Service*): Sistema de autenticação e controle que verifica as credenciais dos usuários e concede acesso aos recursos solicitados.

SPOP3: acesso POP 3 seguro.

SSL e TLS: Secure Sockets Layer (SSL) e seu sucessor Transport Layer Security (TLS) são protocolos criptográficos que provêem comunicação segura na Internet para coisas como e-mail, navegação por páginas, e outros tipos de transferência de dados.

STA: (Wireless LAN Stations) - São os diversos clientes da rede.

UDP: É o protocolo irmão do TCP. A diferença básica entre os dois é que o TCP é um protocolo orientado à conexão, que inclui vários mecanismos para iniciar e encerrar a conexão, negociar tamanhos de pacotes e permitir a retransmissão de pacotes corrompidos. No TCP tudo isso é feito com muito cuidado, para garantir que os dados realmente cheguem inalterados, apesar de todos os problemas que possam existir na conexão.

VPN: Uma Rede Privada Virtual (*Virtual Private Network* - VPN) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto

de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

WI-MAX: O padrão IEEE 802.16, completo em outubro de 2001 e publicado em 8 de abril 2002, especifica uma interface sem fio para redes metropolitanas (WMAN).

IEEE 802.16. Este padrão é similar ao padrão Wi-Fi (IEEE 802.11), que já é bastante difundido, porém agrega conhecimentos e recursos mais recentes, visando uma melhor performance de comunicação.

WPA: O WPA (Wi-Fi Protected Access) é uma melhoria de segurança que aumenta significativamente o nível de proteção de dados e de controle de acesso de uma rede sem fio. O modo WPA usa a autenticação 802.1x e a troca de chaves e só funciona com chaves de criptografia dinâmicas. Para melhorar a criptografia de dados, o WPA utiliza o TKIP (Temporal Key Integrity Protocol).