Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento – ICPD

LEONARDO REIS LATERZA

REDES SEM FIO PADRÃO 802.1X
IMPLEMENTAÇÃO DE UMA REDE SEGURA UTILIZANDO PROTOCOLO DE AUTENTICAÇÃO EAP-TLS.

Brasília
2012

LEONARDO REIS LATERZA

REDES SEM FIO PADRÃO 802.1X IMPLEMENTAÇÃO DE UMA REDE SEGURA UTILIZANDO PROTOCOLO DE AUTENTICAÇÃO **EAP-TLS.**

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Rede de Computadores.
Orientador: Prof. Marco Antonio

Brasília
2012

LEONARDO REIS LATERZA

REDES SEM FIO PADRÃO 802.1X

IMPLEMENTAÇÃO DE UMA REDE SEGURA UTILIZANDO PROTOCOLO DE AUTENTICAÇÃO **EAP-TLS.**

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Rede de Computadores.
Orientador: Prof. Marco Antonio

Brasília 17 de Junho de 2013

Banca examinadora

_____

Prof. Luciano Henrique Duque

_____

Prof.Dr. Gilson Ciaralho

Dedico

Ao meu pai por todo conhecimento de
vida transmitido alem de me
Apoiar e me incentivar em busca
De novos desafios e conhecimento

AGRADECIMENTOS

A Deus por me dar força e inspiração em meus estudos e projetos.

A minha mãe pelo apoio e por sempre me mostrar que não podemos desistir de nossos objetivos.

A minhas irmãs Bianca e Vanessa pelo incentivo durante esse projeto.

Ao professor Javier por todo conhecimento transmitido durante minha graduação e pelo incentivo em que eu fizesse essa Pós – Graduação.

Ao meu Orientador professor Marco Antonio pelo apoio e atenção dado na elaboração deste projeto.

Aos demais professores da Pós Graduação por todo conhecimento transmitido.

Aos colegas de trabalho por todo conhecimento técnico trocado durante o projeto.

“Imagens e palavras chegam via internet
Eu sou mais um viajante, um sonhador
Diante de um maravilhoso mundo novo
A tela de um computador”

Bruno e Marrone – Homem do Meu Tempo

RESUMO

Este trabalho tem como objetivo a criação de um ambiente de rede sem fio seguro utilizando o protocolo EAP- TLS.Com o surgimento de novos equipamentos para acesso a internet como smatphones e tablets, bem como a diminuição do custo dos notebooks, tem tornado a utilização de redes sem fio cada vez mais freqüente em ambientes residenciais, e empresas com objetivo de redução de custos em infraestrutura de cabeamento utilizam redes sem fio em seu ambiente, conseqüentemente o numero de ataques de intrusão também se torna cada vez mais frequentes e maliciosos podendo causar grandes prejuízos aos usuários, a utilização do padrão de autenticação com o protocolo EAP-TLS dificulta estas invasões devido a necessidade de autenticação de usuários através de certificados digitais, alem de utilizar uma conexão segura através do TLS onde os dados que trafegam na rede são criptografados, este trabalho apresenta a implentação de um ambiente de rede sem fio seguro utilizando o padrão EAP-TLS de autenticação e também as ferramentas necessárias para implementação do EAP-TLS em um rede baseada em ambiente Microsoft Windows.Conclui se com este trabalho que, mesmo não existindo um ambiente de rede totalmente seguro, a utilização do EAP-TLS torna mais difícil um intrusão a rede que utiliza este protocolo.

PALAVRAS – CHAVE:

Segurança. Autenticação. redes sem fio . Certificados digitais

ABSTRACT

With the advent of new equipment to access the internet as smatphones and tablets, as well as reducing the cost of laptops has made the use of wireless networks increasingly common in residential environments, and companies with the aim of reducing costs in infrastructure cabling using wireless networks in their environment, hence the number of intrusion attacks also become increasingly frequent and malicious and can cause great harm to users, using the default authentication protocol EAP-TLS difficult because of these invasions need for user authentication using digital certificates, besides using a secure connection via TLS where the data traveling over the network is encrypted, this work presents the implementation of a wireless network environment using the default secure EAP-TLS authentication and the tools necessary to implement EAP-TLS on a network based on Microsoft Windows environment.

KEY - WORDS:

Security. authentication. wireless . digital certificates

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AAA - Authentication, Authorization and Accounting

AC – Autoridade Certificadora

AD – Active Directory

AES - Advanced Encryption Standard

AP – Access Point

DHCP - Dynamic Host Configuration Protocol

EAP - Protocolo de autenticação extensível

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos

LDAP - Lightweight Directory Access Protocol

IP – Internet Protocol

NAS - Network Access Server

PEA - Port Access Entity

PDA - Personal digital assistant

SSL - Secure Sockets Layer

TKIP - Temporal Key Integrity Protocol

TLS - Transport Layer Security

SUMÁRIO

INTRODUÇÃO

MOTIVAÇÃO

A importância da segurança em redes sem fio é conhecida desde a publicação do padrão IEEE 802.11 em novembro de 1997 (IEEE. 1997). O mecanismo denominado Wired Equivalent Privacy (privacidade equivalente ao das redes cabeadas), ou WEP, propõe formas de autenticação dos computadores e também criptografia de dados, porém o nível de proteção do WEP se mostrou insuficiente para muitas redes sem fio.

O grande êxito do padrão 802.11 é o fato de ter se tornado um padrão na indústria que o batizou de Wi-Fi, possibilitando assim a produção de equipamentos em larga escala e com razoável interoperabilidade. Sendo estes dois fatores larga escala e interoperabilidade foram responsáveis pela queda de preço dos equipamentos para redes sem fio tornando assim as redes sem fio financeiramente viáveis tanto para empresas quanto para residências.

O grande benefício das redes sem fio se dá pela possibilidade de acesso sem a necessidade de cabeamento, eliminando assim a necessidade de planejamento de uma infra – estrutura de rede e também elimina o trabalho da passagem de cabos por paredes, tetos e pisos.

Por todas as suas vantagens somadas à mobilidade de acesso, as redes sem fio se popularizaram com muita rapidez, tornando assim comum o tráfego de informações sigilosas por meios destas redes.

O IEEE 802.1X é uma solução para os problemas de autenticação encontrados no IEE 802.11, pois o mesmo suporta diversos métodos de autenticação existentes, podendo o padrão 802.1X ser adotado para autenticação ao nível de porta em redes IEEE 802 cabeadas ou sem fio.

Objetivo

O objetivo deste trabalho é implementar um ambiente de rede sem fio, utilizando protocolo de autenticação EAP – TLS. Tendo como objetivos específicos apresentar as definições do padrão IEEE 802.1X, bem como mostrar as etapas para implementação do ambiente e os softwares utilizados para configuração da rede sem fio utilizando o protocolo EAP-TLS

Metodologia

Para realização deste trabalho, foram feitas pesquisas em livros bem como materiais de fabricantes de produtos voltados a redes sem fio, também foi necessário a montagem de um ambiente de rede sem fio utilizando softwares como: Vitrualbox e Windows Server.

ORGANIZAÇÃO DO TRABALHO

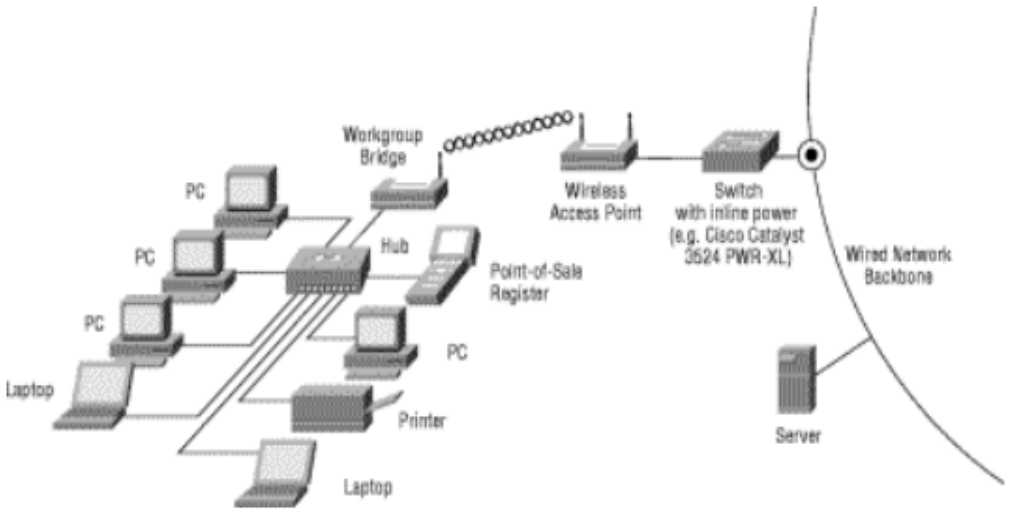
O capitulo 1 traz alguns conceitos úteis para a compreensão deste trabalho bem como conceitos de segurança em redes sem fio; o capitulo 2 analisa o padrão 802.1X, explicando seu funcionamento formas de autenticação; conceitua também o protocolo EAP-TLS e servidor Radius bem como os conceitos de certificado digital; o capitulo 3 mostra os detalhes da implementação de um ambiente de rede sem fio utilizando protocolo de autenticação EAP-TLS e as ferramentas utilizadas na implementação da rede; o capitulo 4 será apresentado os testes realizados no ambiente implementado bem como a validação do mesmo e os resultados obtidos.

1 REFERENCIAL TEÓRICO

1.1 Redes sem fio padrão 802.11

Uma rede sem fio é uma extensão de uma rede local (Local Área Network – LAN), convencional com fio, Uma WLAN realiza a conversão de pacote de dados em ondas de radio ou infravermelho e os envia para outros dispositivos sem fio ou para pontos de acesso que servem como uma conexão para uma rede com fio. [1]

Figura 1 – Conexão de uma rede sem fio com uma convencional com fio



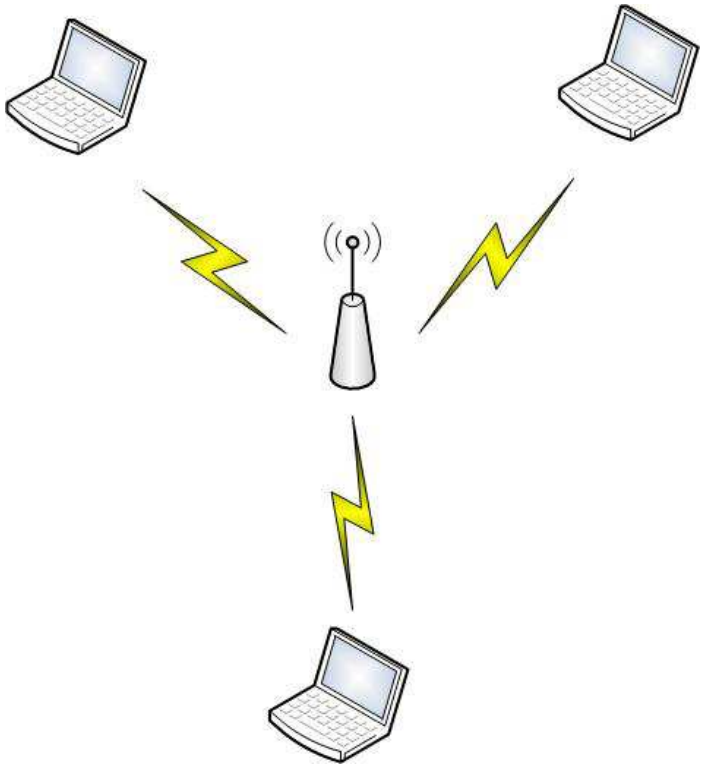
Fonte : Cysco

O padrão IEEE 802.11 tem como premissas: Suporte a vários canais; sobreposição de varias redes em uma mesma área de canal; apresentar se forte em relação à interferências do meio; existência de ferramentas para evitar a presença de nós escondidos; oferecer ao usuário privacidade e um controle de acesso ao meio.[1]

Segundo (IEEE,1997), O padrão 802.11 e definido por dois modos de rede sem fio denominados infra-estrutura e ad-hoc.

- Modo infra – estrutura: A comunicação entre as estações de trabalho é realizada através de um ponto de acesso (AP). Sendo este o modo mais comum de redes sem fio, pois permite que através dos pontos de acesso, estações de trabalho se conecte a redes cabeadas, permitindo assim acesso a servidores e outras estações de trabalho da rede local escopo este utilizado neste trabalho.

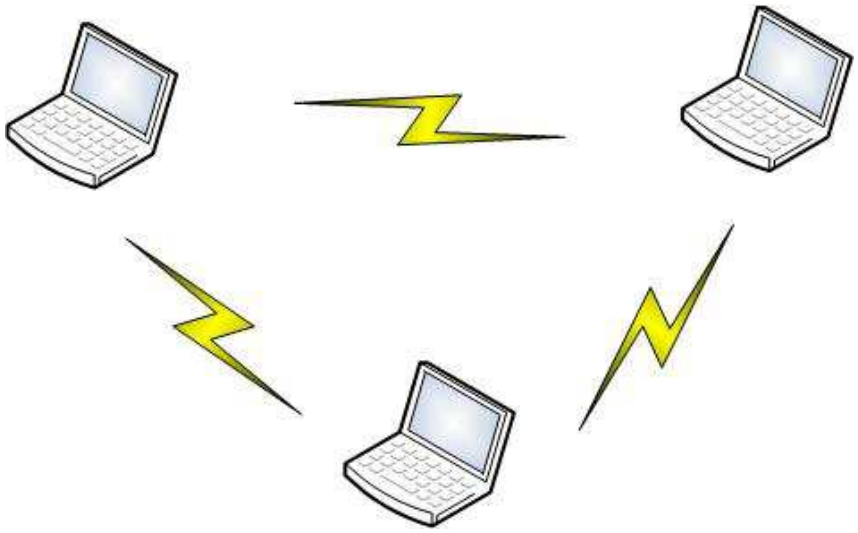
Figura 2 – Rede sem fio no modo infra – estrutura.



Fonte: O próprio autor

- Modo ad – hoc: A comunicação entre estações de trabalho é feito de forma direta. Podendo ser implementada sem um planejamento prévio, pois para criação de uma rede ad – hoc basta que duas estações de trabalho estejam equipadas com placas de rede sem fio.

Figura 3 – Redes sem fio modo ad – hoc



Fonte: O próprio autor

1.2 Seguranças em redes sem fio

Segundo Ohrtmam segurança é um ponto fraco nas redes sem fio, pois o sinal se propaga pelo ar em todas as direções e pode ser captado a distancias de centenas de metros utilizando um laptop com antena amplificada o que torna as redes sem fio vulneráveis a interceptação.[10]

Como descrito no padrão IEEE 802.11 os serviços de segurança fornecidos pelo WEP bem como suas definições são.

a) Confidencialidade: É o principio de que da informação de não se tornar disponível ou revelada a indivíduos, entidades ou processos não autorizados
b) Autenticação: Serviço utilizado para se estabelecer a identidade de uma estação como um membro do conjunto de estações autorizadas a associar com outra estação.
c) Controle de acesso: Prevenção contra o uso não autorizado das informações.

1.3 Ataques

Redes sem fio também estão sujeitas a ataques comuns as redes cabeadas e também a tipos específicos de ataques para redes sem fio que serão descritos a seguir: [2]

1.3.1 Vigilância

Ataque de vigilância busca o reconhecimento do local a ser atacado a procura de redes sem fio. Indícios podem ser antenas, pontos de acesso, cabos de rede e dispositivos PDA ` S(Personal Digital Assistant). A tabela 1.1 lista alguns indícios a serem observados. [2]

Quadro 1 – Indícios de redes sem fio

Coisas para procurar	Potenciais localizações
Antenas	Paredes, tetos, corredores, telhados e janelas
Pontos de Acesso (AP)	Tetos, paredes, suportes e prateleiras
Cabos de rede	Correndo por paredes ou calhas ou teto
Plataformas recém instaladas	Paredes, corredores e suportes
Dispositivos – scanners/PDA's	Funcionários, áreas de recepção ou saídas

Fonte: PEIKARI; FOGIE(2002)

1.3.2 War Driving

É um tipo de ataque que pode ser realizado após a vigilância para uma complementação de informações. O termo *War Driving* originou se da expressão *war-dialing*, que consiste em fazer ligações para diversos telefones a procura de modem. O *War – Driving* se da em mover se de carro ou ônibus a procura de redes sem fio, utilizando ferramentas de mapeamento de rede. [2]

Este tipo de ataque tornou se popular a partir de 2001, como o lançamento de ferramentas de mapeamento de redes sem fio como *NetStubmber*. Sendo que o próprio Windows XP apresenta lista de redes sem fio ao alcance para conexão.

1.3.3 War - Chalking

Uma variação do *War – Driving* conhecida como *War – Chalking*, tem como objetivo detectar a existência de sinal de redes sem fio. Se conectar as referidas redes e então marcar as paredes externas dos edifícios indicando a presença de redes capazes de serem penetradas. Esta informação pode ser utilizada por pessoas com a intenção de conseguir acesso gratuito a internet e por pessoas mal intencionadas que podem “escutar” livremente o trafego da rede. [2]

1.3.4 Hacking Cliente-a-Cliente

Uma intrusão pode ser feita a um notebook conectado a uma rede cabeada, e que esteja com interface de rede sem fio ativa e configurada para o modo ponto a ponto. Com um ataque deste tipo é possível ganhar acesso ao notebook e, com algum esforço, à rede cabeada.[2]

É um ataque especialmente perigoso, pois grande parte de usuários não tem conhecimentos necessários para detectar ou prever o ataque, colocando em assim a segurança da rede em risco.

1.3.5 Negação de Serviço (DOS)

Os ataques de negação de serviço têm como objetivo impedir que as estações de trabalho tenham acesso a serviços da rede. Levando em consideração que redes sem fio operam através de transmissão de radio, é possível gerar ondas em freqüências iguais às usadas pela rede sem fio interferindo assim na transmissão de dados. [2]

1.4 Redes sem fio padrão 802.1X

O padrão 802.11X tem como objetivo prover o controle de acesso nas portas disponíveis a conexão como *bridges,hubs e AP `S* , de modo a evitar que conexões clandestinas tenham acesso a rede.

O padrão IEEE 802.1x foi desenvolvido visando solucionar problemas de autenticação que existem no padrão IEEE 802.11, visto que o padrão 802.1x suporta diversos métodos de autenticação. O padrão 802.1x assegura uma compatibilidade entre o TKIP(Protocolo de Integridade Temporal) desenvolvido como solução para o problema da chave WEP, como o padrão criptográfico avançado (AES – *Advanced Encryption Standard*).[3]

Segundo (BLUNK, 1998) uma das maneiras de utilização do padrão 802.1X, e a implementação do protocolo EAP (Extensible Authentication Protocol), este podendo ser configurado de maneira a exigir do cliente uma prévia autenticação entre o cliente e a rede, não havendo esta autenticação as comunicações não serão permitidas. [6]

No padrão IEEE 802.1X a autenticação do usuário é realizada utilizando um servidor RADIUS e uma base de dados de usuários para sua validação.[3]

A autenticação no modelo 802.1X consiste em três partes: O requerente (cliente), Autenticador (Ponto de acesso) e o servidor de autenticação (RADIUS).

1.5 Certificados digitais

O certificado digital é um conjunto de métodos e processos que visa prover maior segurança em transações e comunicações eletrônicas evitando assim possíveis roubos de informações, sendo que sua utilização proporciona: *[4]*

- **Privacidade**: Garantia que as informações tocadas em transações eletrônicas não serão acessadas por intrusos.
- **Integridade**: Garantia que as informações enviadas durante a transação eletrônica não foram modificadas desde que foram assinadas.
- **Autenticidade**: Garante a identidade da origem e do destino da transação.
- **Assinatura Digital**: Assinatura eletrônica se baseia em métodos criptográficos elaborados a partir de um conjunto de regras que permite a um documento a possibilidade de uma confirmação segura de que o mesmo permanece integro bem como a identificação do autor do documento eletrônico.
- **Não Repudio**: É a garantia que somente o detentor do certificado digital poderia ter feito uma transação eletrônica, impedindo assim que os demais integrantes da transação neguem uma transação após esta ter sido realizada.

A utilização de certificado digital evita adulteração de dados em comunicações realizadas via internet. Possibilitando saber a autoria da transação ou de uma mensagem, e ainda manter dados confidenciais protegidos contra leitura de terceiros não autorizados. *(4)*

Uma estrutura de assinatura digital possui alem de um emissor e do receptor, a Autoridade Certificadora (AR) esta responsável pela requisição da emissão de certificados a uma Autoridade Certificadora (AC) que também faz parte da maioria dos esquemas de assinatura digital, podendo uma AR ser um AC ou vise-versa. *[4]*

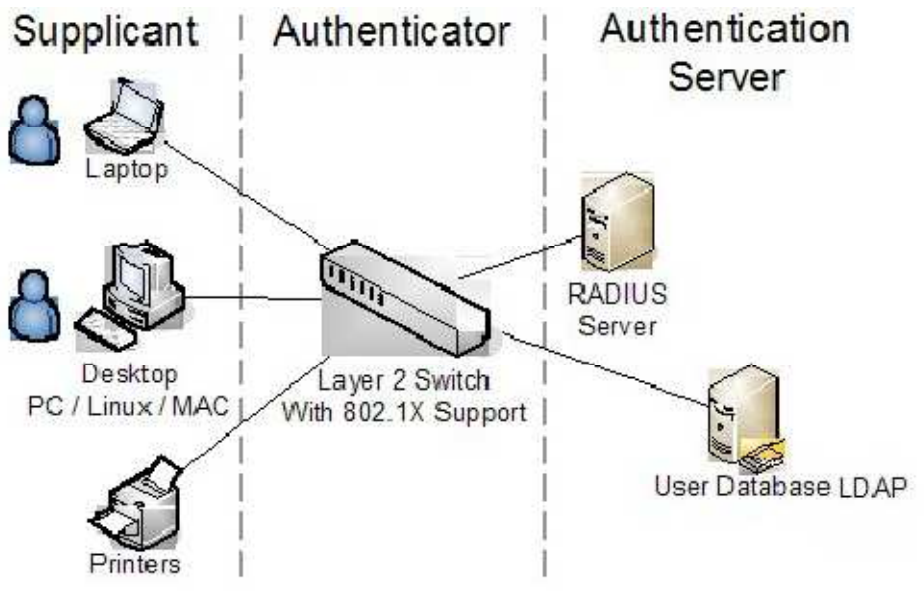
2 ANALISE DO PADRÃO 802.1X

2.1 Autenticação Baseada no padrão 802.1X

Para seja possível implementar uma rede com o padrão IEEE 802.1X é preciso a existência de uma infraestrutura de suporte, clientes que tenham suporte ao padrão IEEE 802.1X, switches, pontos de acesso sem fio, servidor RADIUS e algum tipo de banco de dados de contas, como *LDAP(Lightweight Directory Access Protocol)* ou Active Directory.[6]

O padrão 802.1X tem como ideia prover controle de acesso nas portas dos dispositivos de conexão, de modo a impedir que conexões clandestinas tenham acesso a rede.[6]

Figura 4 – Infraestrutura para operar com 802.1X



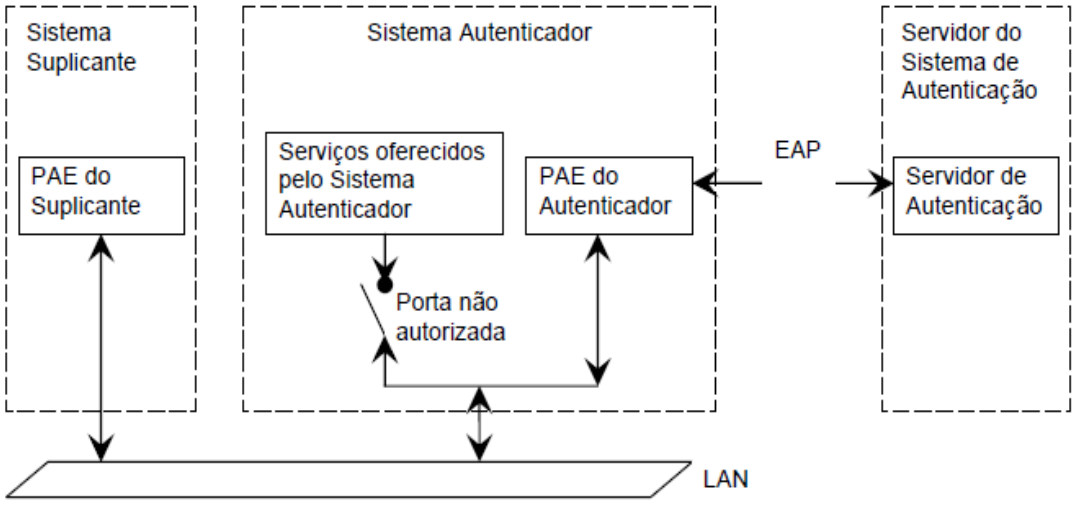
Fonte: Blunk e Vollbrecht(2012)

O padrão 802.1X define três atores durante o processo de autenticação, conforme figura 4:

- Suplicante: É um cliente que deseja ser autenticado na rede, este representado por uma interface de rede sem fio no padrão 802.11, geralmente um notebook.
- Autenticador: É o dispositivo intermediário entre o suplicante e o servidor de autenticação, este constituído pelo AP (Ponto de Acesso).
- Servidor de Autenticação: É um dispositivo responsável pelo controle de acesso, em geral se trata de um servidor Radius.

O controle de acesso é realizado mantendo – se as portas em um de dois estados existentes: autorizado ou não – autorizado. O padrão 802.1X é ilustrado na figura 5. [5]

Figura 5 – Padrão 802.1X



Fonte:Edney e Arbaugh,(2004)

Na figura 5 é possível observar que o sistema Suplicante comunica – se com o sistema autenticador através da LAN. Anterior ao processo de autenticação, toda comunicação

entre os dois sistemas se da através das portas não controladas conectadas às PEA`s (*Port Acess Entity* – Entidade de Acesso a porta). A autenticação será realizada através da PAE do autenticador. Sendo que esta se comunicará com o Servidor de autenticação por meio do protocolo EAP, para obter autenticação do sistema suplicante, o autenticador modificará o estado da porta controlada para autorizado. Assim permitindo que o sistema suplicante obtenha acesso aos serviços oferecidos pelo sistema autenticador, em geral corresponde a ganhar acesso a rede. [5]

Para autenticação no padrão IEEE 802.1X são necessários os seguintes passos:

- O suplicante inicializa uma conexão com suplicante, que habilita somente as portas do 802.1X
- O autenticador realiza a solicitação da identidade do suplicante.
- O suplicante envia a resposta com sua identidade e o autenticador a envia para o servidor de autenticação.
- O servidor de autenticação autentica o servidor e comunica ao autenticador, este habilita a comunicação do suplicante nas demais portas.
- O suplicante realiza a solicitação da identidade do servidor de autenticação.
- O servidor de autenticação informa a sua identidade.
- O Suplicante autentica o servidor de autenticação.

2.2 EAP – TLS

Entre os padrões de autenticação EAP (Extensible Authentication Protocol), considera – se o EAP-TLS um dos mais seguros disponíveis, sendo que o mesmo é suportado por todas as fabricantes de hardware e software pare redes sem fio. [7]

A necessidade de o usuário ter que utilizar um certificado para autenticação na rede que o faz ser tornar um padrão seguro, o que também o torna impopular e pouco implementado. O padrão EAP-TLS é baseado no protocolo SSL(Secure Socket Layer), utilizado para fornecer segurança ao tráfego na web. [7]

Os certificados são utilizados para autenticar o servidor de autenticação para o suplicante no EAP-TLS, e com uma opção de autenticar o suplicante para o servidor de autenticação [7]

O padrão de autenticação EAP-TLS tem como base o SSL em sua versão 3.0, sendo o *handshake* SSL executado através de EAP, porem na internet o *handshake SSL* é conduzido através do protocolo TCP(*Transmission Control Protocol*). [7]

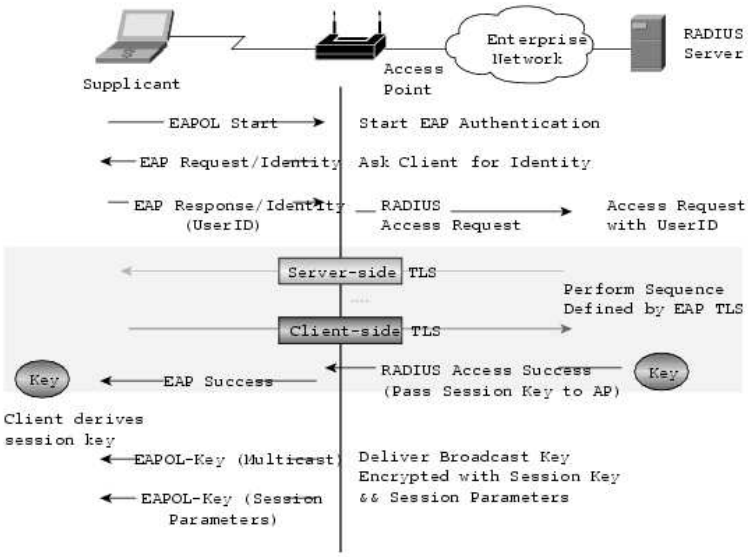
2.2.1 Como trabalha o EAP-TLS

Durante o processo de autenticação do EAP-TLS são envolvidos os seguintes componentes: [8]

- Suplicante (Computador Cliente)
- Autenticador (Ponto de acesso)
- Servidor de Autenticação

O processo de autenticação do padrão EAP-TLS é mostrado na figura 6. Neste processo o servidor Radius fornece o certificado digital para o cliente bem como as requisições de certificados do cliente. O certificado do servidor é validado pelo cliente que responde com uma mensagem de resposta EAP que contem seu certificado e também inicia a negociação para as especificações de criptografia. Após esta etapa ocorre a validação do certificado (8)

Figura 6 – EAP-TLS Visão Geral



Fonte: Cisco 2012

2.3 RADIUS

O protocolo RADIUS tem como objetivo de fornecer acesso a redes que utilizam a arquitetura AAA(*Authentication, Authorization, and Accounting* - autenticação, autorização e contabilização), o protocolo Radius no seu inicio foi criado para ser utilizado em serviços de acesso discado. Nos dias atuais também é implementado e pontos de acesso de redes sem fio e também em outros dispositivos que possibilitam acesso autenticado a redes de computadores.[9].

2.3.1 Arquitetura AAA

O protocolo Radius é desenvolvido com base em um processo denominado AAA, este constituído em autenticação, autorização e *accounting* (acompanhamento / monitoramento do uso de recursos de rede por usuários).As etapas que o Radius sugue são:[9].

- **Autenticação do usuário:** Neste processo ocorre a verificação da validade de login e senha. Sendo que o login pode uma conta de usuário, conta de maquina , certificado digital etc.
- **Autorização de serviços:** O segundo passo é a autorização, neste passo o sistema verifica as permissões que o usuário possui no sistema. Neste passo o servidor AAA fará uma serie de processos e analises para determinar quem é o usuário, bem como saber quais as permissões de acesso que o usuário possui.

- **Contabilização:** É o processo de monitoramento / gerenciamento denominado ***accounting*** sendo este utilizado pelo usuário**.** Nesta etapa é

realizado o acompanhamento pelo sistema de cada passo do usuário na utilização dos serviços da rede.

2.3.2 Funcionamento do RADIUS

O *Radius* tem como base em seu desenvolvimento o modelo cliente / servidor, sendo o cliente o *Network Acess Server – NAS* e o servidor *Radius*. É realizada a troca de mensagens entre o utilizador, o *NAS* e o servidor quando o utilizador solicita se autenticar para utilização de um servidor na rede. [9]

A mensagem do protocolo *Radius* é constituída de um pacote contendo cabeçalho *Radius* com o tipo de mensagem, também podendo conter atributos associados à mensagem. No *Radius* existem atributos para nome de usuário, senha do mesmo, tipo de serviço solicitado pelo usuário bem como para o IP do servidor de acesso.[9]

Os atributos do protocolo Radius são usados na transmissão de informações entre clientes Radius e servidores Radius. Quando um usuário da rede deseja acessar um serviço o mesmo envia os seus dados para o NAS. [9]

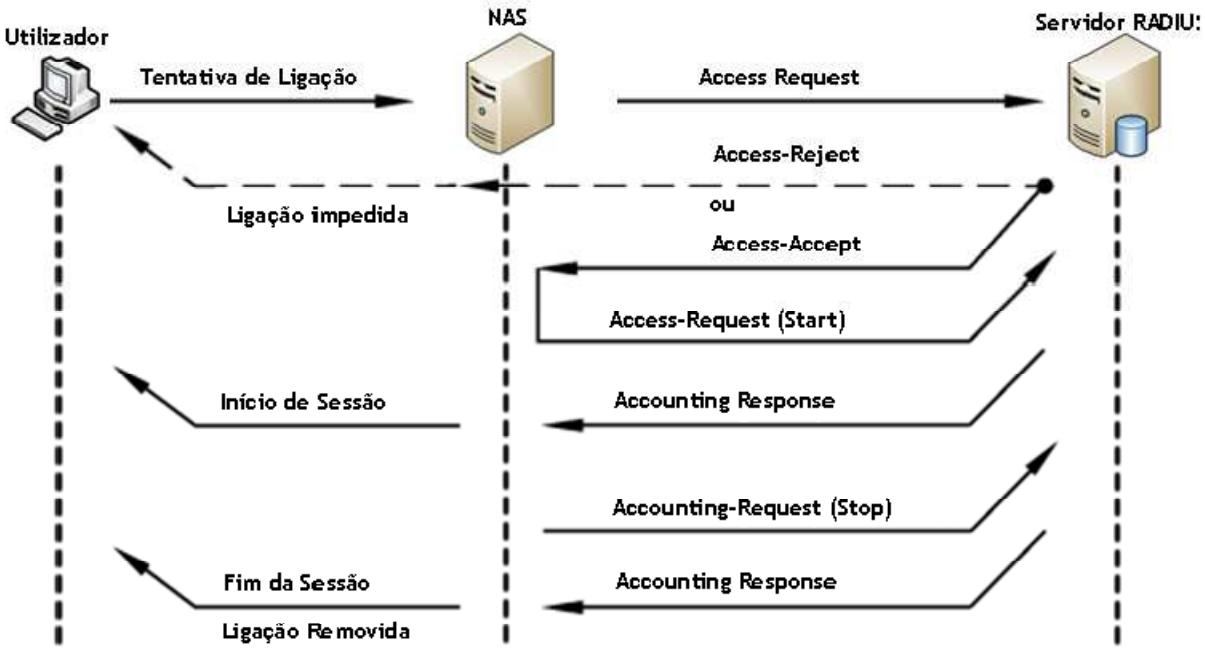
O NAS tem a responsabilidade pelo recebimento de todos dados do usuário, que em grande parte dos casos são o nome de usuário e senha (a senha é cifrada no envio do nas para o servidor evitando assim intrusões) e também envia – los ao servidor *Radius* através do pedido de acesso este designado de *Access – Request*.[9]

Após o recebimento da solicitação de acesso o servidor realiza a tentativa de autenticação do usuário, em seguida é enviada uma resposta para o NAS, resposta essa

contendo um *Access – Reject*, em caso de acesso negado e um *Access - Accept* em caso de acesso aceito ou então *Access – Challenge* no caso de uma pedida de nova confirmação. (9)

Após o processo de autenticação, é realizada a comparação e verificação de alguns dados para que o servidor determine o nível de acesso a ser fornecido ao usuário que foi autenticado. A figura 7 descreve o funcionamento do servidor RADIUS. (9)

Figura 7 – Funcionamento do Radius.



Fonte: Hassell, (2002)

2.4 Certificados digitais padrão x509

O certificado digital e o equivalente a uma carteira de identidade, passaporte ou carteira de motorista. Assim como estes documentos, o objetivo do certificado digital é provar sua identidade. Sendo o X.509 o padrão atual utilizados para certificados digitais. [4]

O certificados digitais utilizam PKI(Infra-estrutura de chaves públicas) com objetivo de fornecer um método tanto de autenticação quanto de passar as chaves públicas.

No geral os certificados digitais contêm três grupos principais de informações:

- A Chave(s) publica(s) do assunto
- Informações sobre o assunto
- Informações sobre o emissor e sua assinatura.

Contanto que haja confiança no emissor do certificado, é necessário apenas verificar se a identidade do servidor ou usuário e a mesma que essa no certificado e se não houve a revogação do certificado. Os certificados digitais são emitidos por uma autoridade certificadora. É função da autoridade certificadora verificar os detalhes da pessoa para quem o certificado será emitido, e então fornecer o certificado após uma completa conferencia. [4]

O padrão X509 encontra se atualmente na versão 3 laçada em 1998, e sua estrutura é definida pela *International Telecomunication Union– Telecomunication (ITU-T).*

A tabela 2 apresenta a estrutura da versão três do padrão X509, com seus respectivos campos e descrição. [4]

Quadro 2 – Descrição dos campos de um certificado no formato X 509

NOME DO CAMPO	DESCRIÇÃO
Versão	Número da versão X.509 do certificado, tendo como valor válido apenas 1, 2 ou 3.
Número de série	Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora.
Algoritmo de assinatura	Identificador do algoritmo usado para a assinatura do certificado pela autoridade certificadora.
Emissor	Nome da autoridade certificadora que produziu e assinou um certificado.
Período de validade	Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora.
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada
Identificador Único de Emissor (opcional)	Campo opcional para permitir o reuso de um emissor com o tempo.
Identificador Único de Assunto (opcional)	Campo opcional para permitir o reuso de um assunto com o tempo.
Extensões (opcional)	Campos complementares com informações adicionais personalizadas.

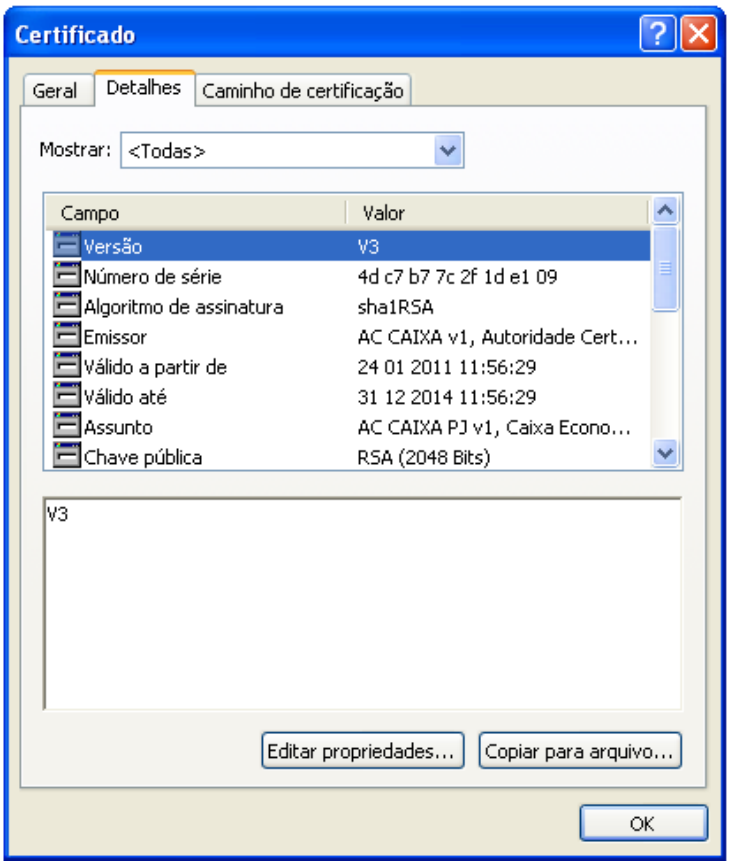
Fonte: Certificação Digital. Conceitos e aplicações(2008)

As extensões originadas da versão 3 permitem um melhor controle, no qual empresas, autoridades certificadoras e outros podem realizar personalizações que se adapte melhor as suas necessidades. Campo este que se divide em três partes: [4]

- Tipo de extensão: Realiza a identificação da semântica e o tipo de informação.
- Indicador critico: Padroniza as aplicações de software.
- Valor de extensão: Contém o valor real do campo.

A figura 8 apresenta um certificado digital padrão x 509 em sua versão 3 fornecido pela AC da Caixa Econômica Federal.(4)

Figura 8 – Certificado digital padrão X509 versão 3.



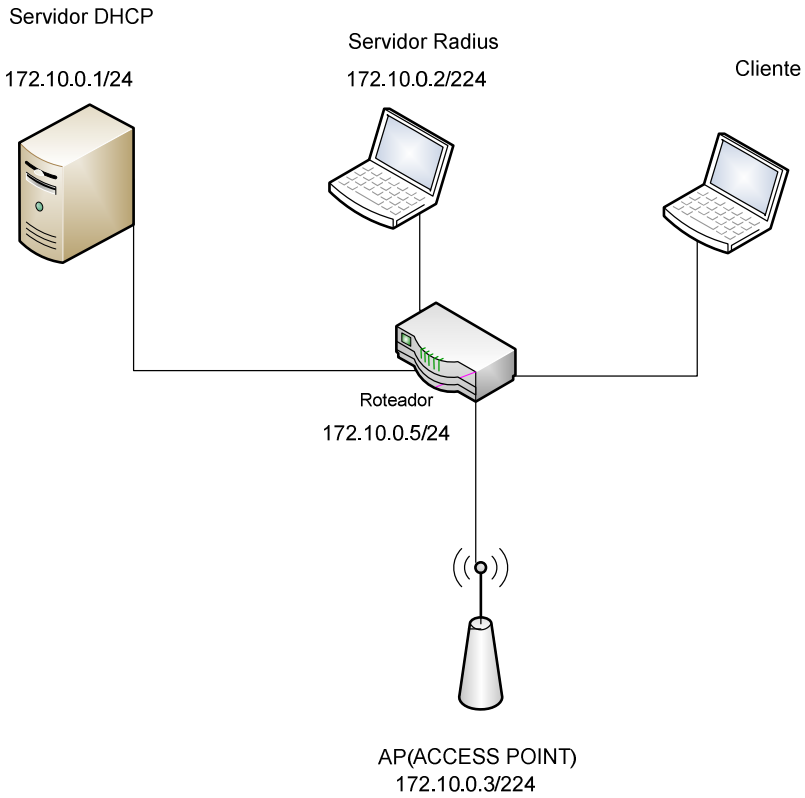
Fonte : Caixa Econômica Federal

3 IMPLEMENTAÇÃO DO EAP – TLS EM UMA REDE SEM FIO

3.1 Proposta de Implementação

Para implementação de uma rede sem fio utilizando o protocolo EAP-TLS, foi desenvolvida uma rede contendo dois servidores sendo um servidor de domínio e DHCP e um servidor RADIUS alem de um computador cliente que fará a autenticação na de rede sem fio tendo como Access Point Cisco 350, conforme figura 9.

Figura 9 – Escopo da rede implementada



Fonte: O próprio autor

Os servidores foram criados em maquinas virtuais utilizando a ferramenta *VirtualBox* e o cliente é um *Netbook*, e suas configurações serão descritas no decorrer deste capitulo.

3.2 Ferramentas utilizadas na implementação

3.2.1 VirtualBox

O *Oracle VirtualBox* é um virtualizador voltado para o uso em desktops e também em servidores, sua escolha para implementação deste projeto foi devido ao software atender as necessidades requeridas para criação de uma rede sem fio com a utilização de autenticação EAP-TLS.

Para este projeto foram montadas duas maquina virtuais sendo um servidor DHCP e a outra o servidor Radius com a seguintes configurações:

- Servidor DHCP
  - Sistema Operacional: Windows Server Enterprise Edition 2003
  - Memória RAM : 512 MB
  - Espaço de disco: 10 GB dinamicamente expansível
  - Placa de rede em modo bridge
- Servidor Radius
  - Sistema Operacional: Windows Server Standart Edition 2003
  - Memória RAM : 512 MB
  - Espaço de disco: 10 GB dinamicamente expansível
  - Placa de rede em modo bridge

3.2.2 Active Directory (AD)

O EAP-TLS tem como pré requisito para seu funcionamento a existência de um banco de dados de contas podendo um LDAP ou AD, para este projeto foi instalado o serviço de banco de dados de contas *Active Directory* no servidor de nome DHCPSRV, a escolha do AD foi feita por sua maior facilidade de configuração de contas de usuário bem como grupos de usuários e também pelo da rede proposta ser baseada em ambiente Microsoft Windows.

3.2.3 Wireshark

O Wireshark é um dos mais populares analisadores de pacote existentes, com ele é possível realizar analise do trafego de rede facilitada por permitir a organização dos protocolos, com esta ferramenta é possível saber tudo que esta se passa na rede através dos pacotes capturados pelo software, sendo ele disponível para Windows e Linux.

3.2.4 Cisco Aironet 350 Series Access Point

O Access Point (AP) Cisco Aironet 350, atende de forma segura e eficaz as necessidades de implementação de uma rede sem fio que utiliza como protocolo de autenticação o EAP-TLS.

Este AP suporta a taxas de dados de até 11Mbs, sendo compatível com o padrão IEE 802.1b podendo ser utilizado em ambientes domésticos e empresas, o Access Point (AP) Cisco Aironet 350 suporta os seguintes recursos de software:

- IEEE 802.1X baseando no protocolo EAP, fornecendo serviço centralizado, autenticação baseada no usuário e mono usuário, sessão única de chaves criptográficas e administração baseada no usuário.
- Seleção de canis automatizada, Cisco Discovery Protocol (CDP), serviço DHCP e também serviços de BOOTP que simplifica a instalação e gestão de WLANS.
- Serviços de balanceamento de carga

Figura 10 – Access point Cisco Aironet 350

Fonte: Cisco

4 TESTES E VALIDAÇÃO DO AMBIENTE

4.1 Configurações básicas do Servidor DHCPSRV

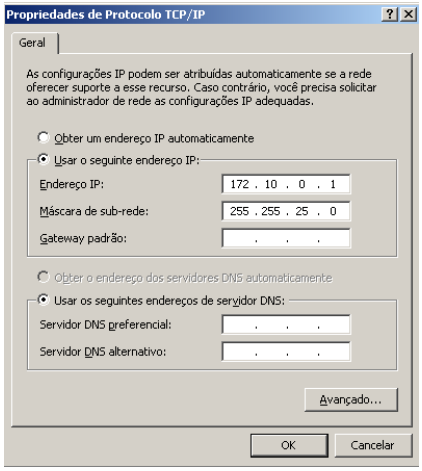
O servidor DHCP é uma maquina virtual rodando o sistema operacional Windows 2003 Server SP1 Enterprise Edition este rodando os seguintes serviços:

- Controlador de domínio para o domínio: posuniceub.com
- DNS Server para o domínio: posuniceub.com
- DHCP Server para o segmento de intranet
- Autoridade Certificadora CA para o domínio: LATERZA
- Servidor WEB

4.1.2 Configurando serviços no servidor DHCPSRV

Inicialmente foi realizada a definição de um IP bem como sua respectiva mascara de sub-rede, escolhido de forma a atender as necessidades do ambiente de testes que será descrito no decorrer deste capitulo. A figura 11 mostra a definição de IP e máscara para o servidor.

Figura 11 Definição de ip no Servidor DHCP

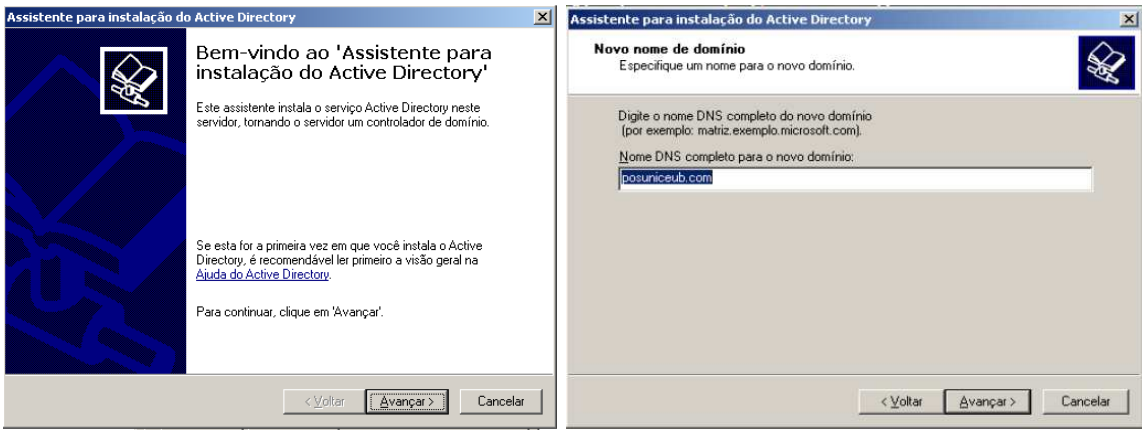


Fonte: O próprio autor

4.1.2 Configuração do Active Directory

Como o requisito para o funcionamento da autenticação no padrão EAP-TLS, de ser instalado um banco de dados de contas, para esta implementação o *Active Dire*ctory foi configurado na maquina virtual denominada DHCPSRV e será dado o nome de LATERZA para o domínio a ser criado nesta configuração do AD.

Figura 12 configuração do Active Directory

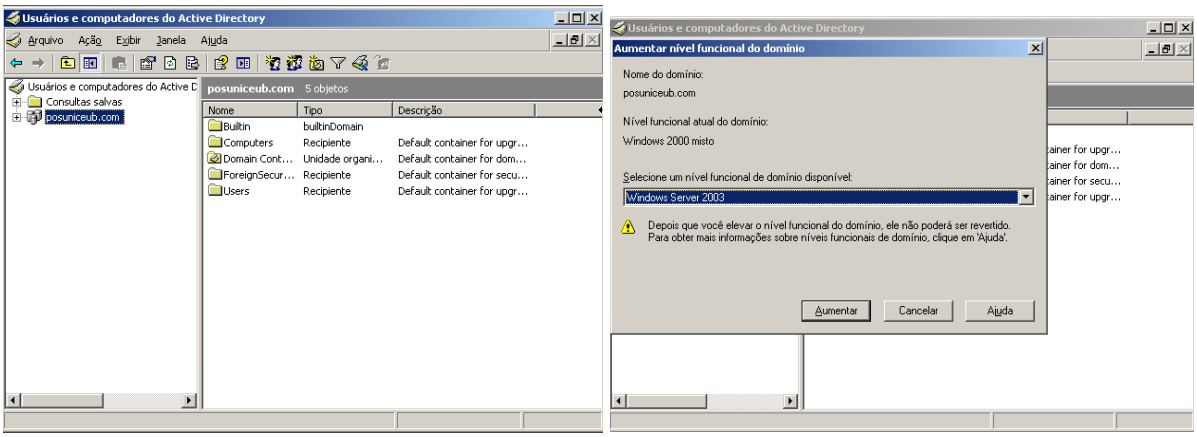


Fonte: O próprio autor

4.1.3 Promovendo ao nível de domínio

Outra etapa importante para o funcionamento do servidor DHCPSRV é promovê-lo a controlador de domínio que para está implementação o domínio terá o nome de laterza.com, esta configuração foi feita acessando o Active Directory conforme mostrado na figura 13.

Figura 13 – Promovendo servidor ao nível de domínio.



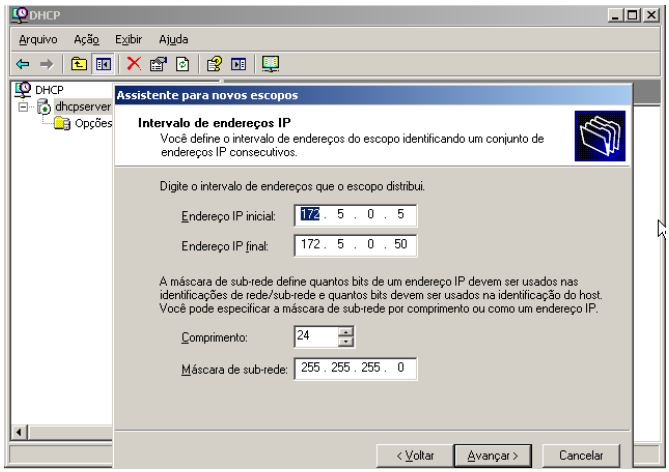
Fonte: O próprio autor

4.1.4 Serviço DHCP

O serviço Dynamic Host Configuration Protocol(DHCP) será configurado com objetivo de prover IPS aos *hosts* clientes que farão parte do domino criado bem como farão autenticação na rede sem fio criada utilizando o EAP-TLS, para esta implementação o DHCP foi configurado da seguinte forma:

- Nome do escopo: LaterzaNet
- Range de ips: inicial: 172.10.0.10 – Final: 172.10.0.60
- Mascara de sub – rede : 255.255.255.0 / 24

Figura 14 – Configuração do DHCP



Fonte: O próprio autor

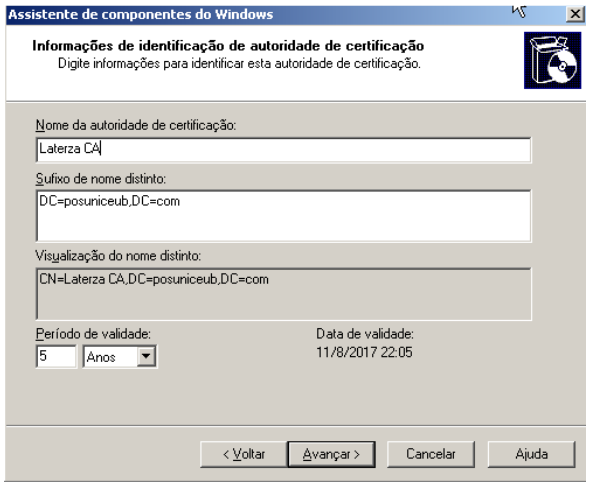
4.1.5 Instalação e configuração do serviço IIS(Internet Information Services)

Com objetivo de criar uma pagina HTML na qual os usuários da rede farão à solicitação do certificado digital e necessário a instalação do serviço IIS que tem por função a criação de paginas HTML dinâmicas usando também a tecnologia ASP, sendo que no sistema operacional Windows Server Enterprise Edition 2003 a versão do IIS utilizada é a 6.0.

4.1.6 Serviço de Certificado

O servidor denominado DHCPSRV também terá habilitado o serviço de certificado sendo assim ele será a AC(autoridade certificadora) responsável por gerar, armazenar alem de poder revogar ou renovar certificados quando assim for necessário, a AC criada recebeu o nome de LATERZA CA.

Figura 15 – Configuração do serviço de certificado



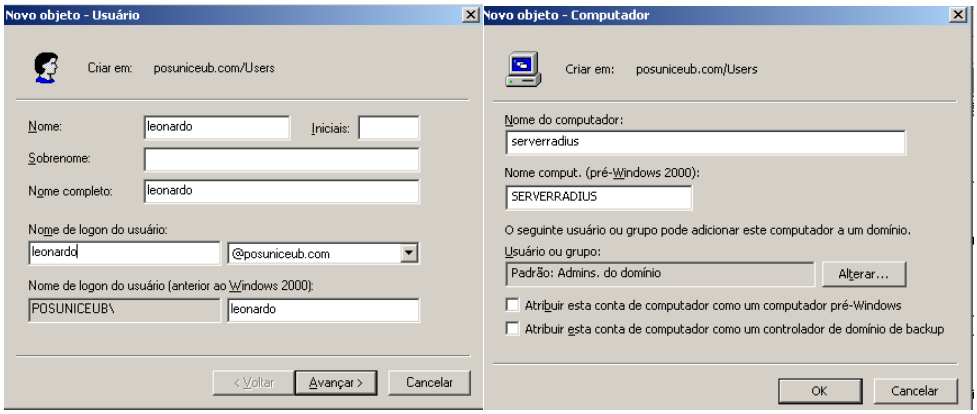
Fonte: O próprio autor

4.1.7 Cadastramento de maquinas da rede no AD

As maquinas que farão parte da rede implementada para autenticação na rede sem fio utilizado o EAP-TLS devem estar cadastradas no AD, para este projeto foi adicionado no banco de dados de contas os seguintes componentes:

- Usuários:
  - Leonardo
  - user01
  - user02
- Computadores
  - cliente01
- Grupos:
  - UsersWireless

Figura 16 – Cadastramento de usuários do AD



Fonte: O próprio autor

4.2 Configuração Básica no servidor Radius

O servidor *Radius* é uma maquina virtual rodando Windows Server 2003 Standard Edition sendo este servidor denominado RADIUS para esta implementação, o serviços de *Radius* poderiam estar instalados no mesmo servidor dos serviços DHCP e AD, porem para melhor organização foram montados em servidores diferentes.

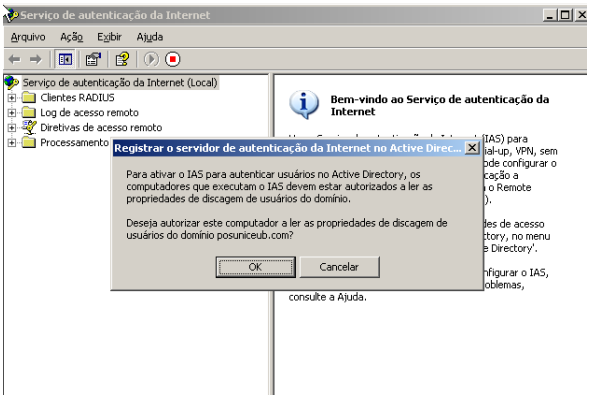
O servidor *Radius* responsável por prover autenticação e autorização para o AP, servidor este configurado com seguinte endereçamento:

- Nome do computador: RADIUS
- IP: 172.10.0.2
- Mascara de sub – rede: 255.255.255.0
- DNS: 172..10.0.1

4.2.1 Instalação do Internet Authentication Service(IAS)

Com objetivo de realizar a autenticação de usuários na rede proposta para este projeto, é necessária a instalação do serviço de autenticação da internet, após a instalação do serviço IAS o mesmo tem que ser registrado no AD conforme apresentado na figura 17.

Figura 17 – Registrando IAS no AD.

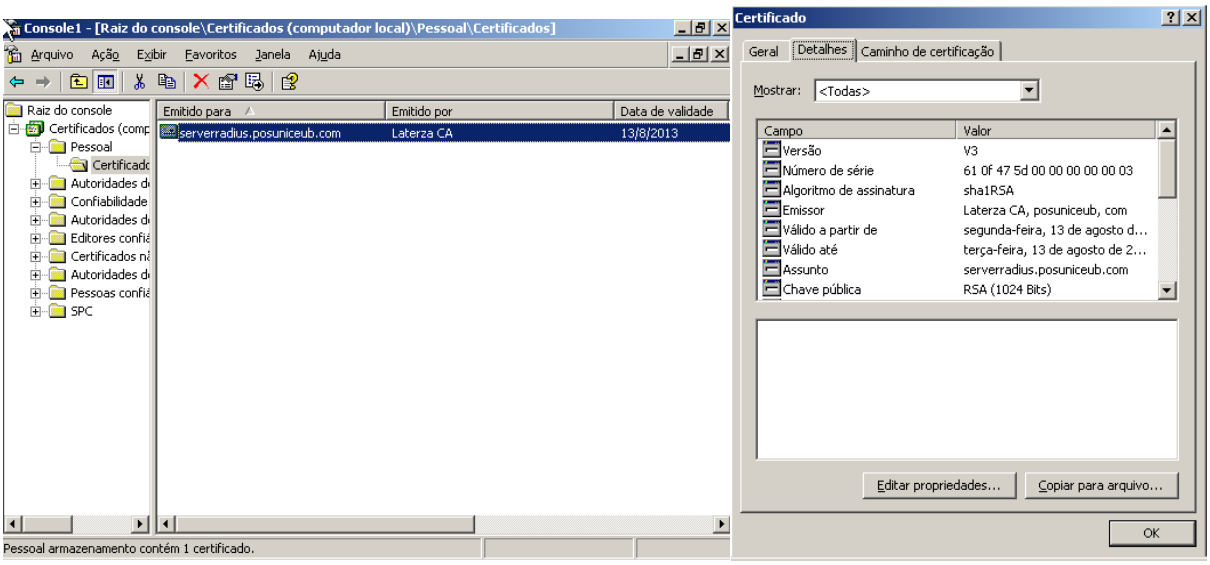


Fonte: O próprio autor

4.2.2 Criação do certificado local

Até esta etapa do projeto o *autoenrollment*(registro automático de certificado) não está ativado, sendo assim necessário a criação de um certificado local para o servidor radius de forma manual, a configuração será feita nas configurações especificas do servidor para o funcionamento do EAP-TLS configurações estas descritas a partir do item 4.3.

Figura 18 – Certificado local do servidor Radius



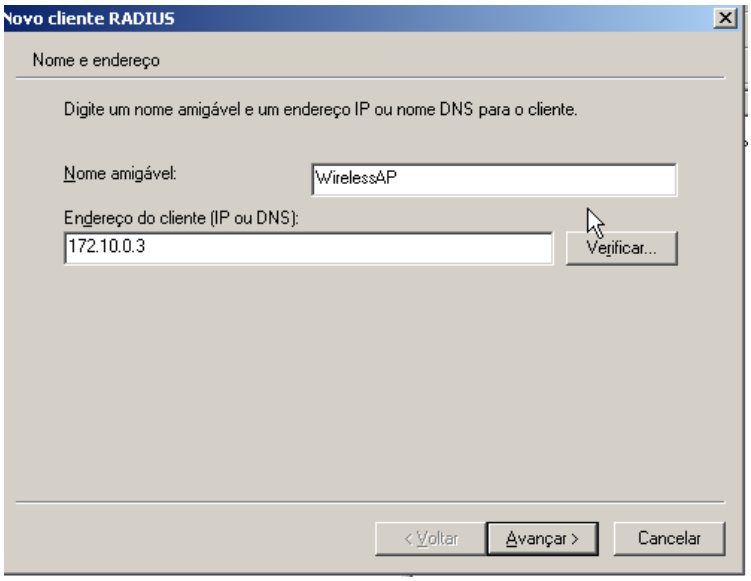
Fonte: O próprio autor

4.2.3 Adicionando do AP como cliente Radius

Como requisito para o funcionamento da implementação de uma rede sem fio utilizando a tecnologia EAP-TLS é necessário que o AP seja adicionado no servidor como cliente Radius, neste projeto o AP recebeu as seguintes configurações:

- Nome Amigável: WirelessAP
- IP ou DNS : 172.10.0.3

Figura 19 – Adicionando cliente Radius



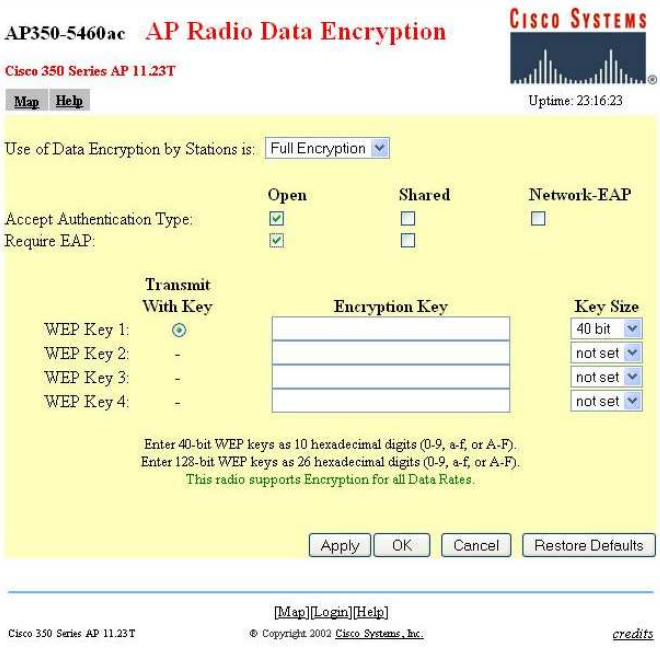
Fonte: O próprio autor

4.3 Configurações do Access Point Cisco Aironet 350 para o EAP-TLS

O Acces Point Cisco Aironet 350 permite três formas de acesso ao seu painel de configurações, através do Browser de internet, cabo serial RS232 e através de linha de comando, neste projeto as configurações foram feitas pelo navegador Internet Explorer, sendo feita as seguintes configurações:

- Formas de autenticação: Devem estar marcado as opções *Requere EAP e Network EAP* conforme figura 20

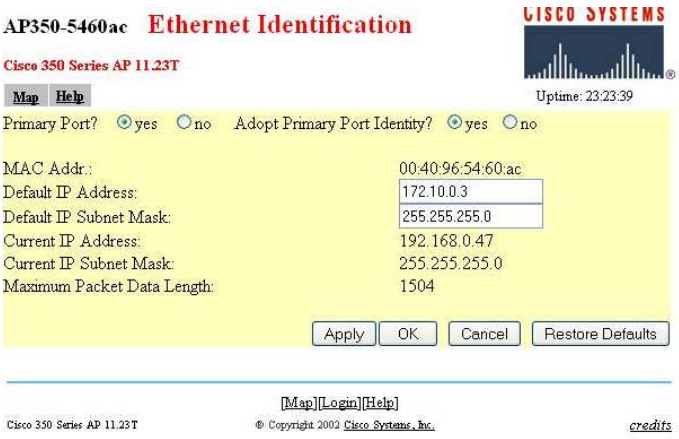
Figura 20 – Configuração de autenticação do AP



Fonte: O próprio autor

- Definição do ip do AP: 172.10.0.3
- Mascara de sub – rede : 255.255.255

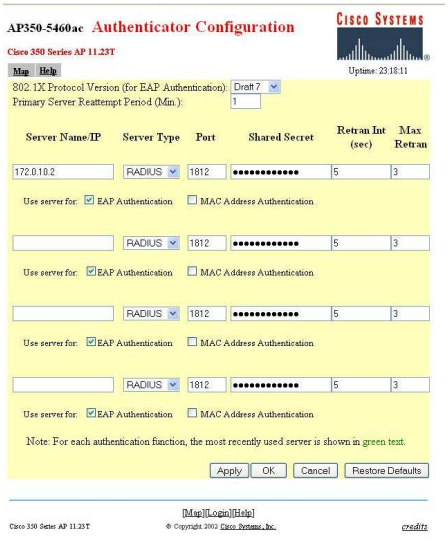
Figura 21 – Definição de IP do AP



Fonte: O próprio autor

- Configuração o IP do servidor Radius no AP

Figura 22 – Configuração do Radius no AP



Fonte: O próprio autor

4.4 Testes e Resultados

4.4.1 Inserindo cliente no domínio

Para realização dos testes de autenticação na rede wireless usando o padrão EAP-TLS, primeiramente o cliente que neste caso se trata de um notebook deve ser conectada a rede através da conexão cabeada para que o cliente se comunique com o servidor de domínio.

Após o processo de inserção do micro no domínio, deve ser dada ao usuário a permissão de Administrador no computador cliente para que o mesmo possa fazer as configurações descritas no decorrer da etapa de testes.

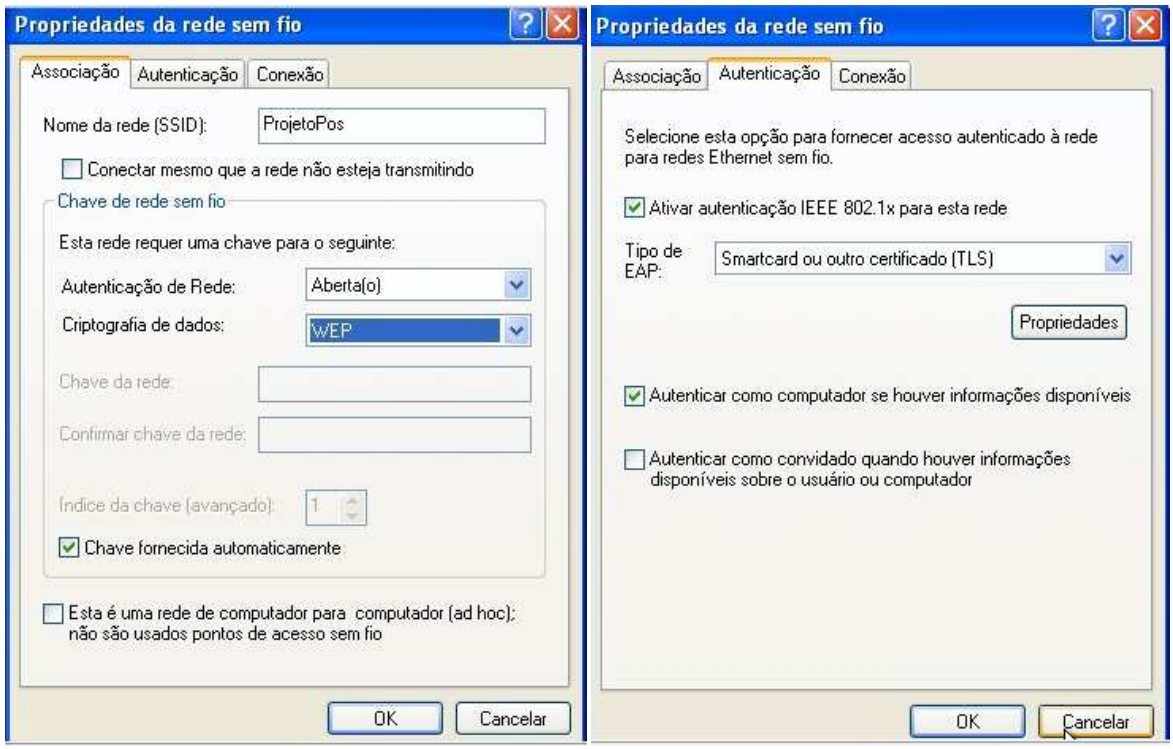
4.4.2 Configuração da conexão

A conexão a rede implementada para este projeto deve ser configurada nas propriedades do dispositivo de conexão de rede sem fio do computador cliente, sendo esta configuração feita através da adição de uma conexão a rede sem fio que para este projeto tem o nome de ProjetoPos

Conforme apresentado na figura 23 deve ser configurada a conexão da seguinte forma:

- Nome da rede (SSID): ProjetoPos
- Autenticação da rede: Aberta
- Criptografia de dados: WEP
- Tipo de EAP: Smart card ou outro certificado (TLS)

Figura 23 – Configuração de conexão de rede



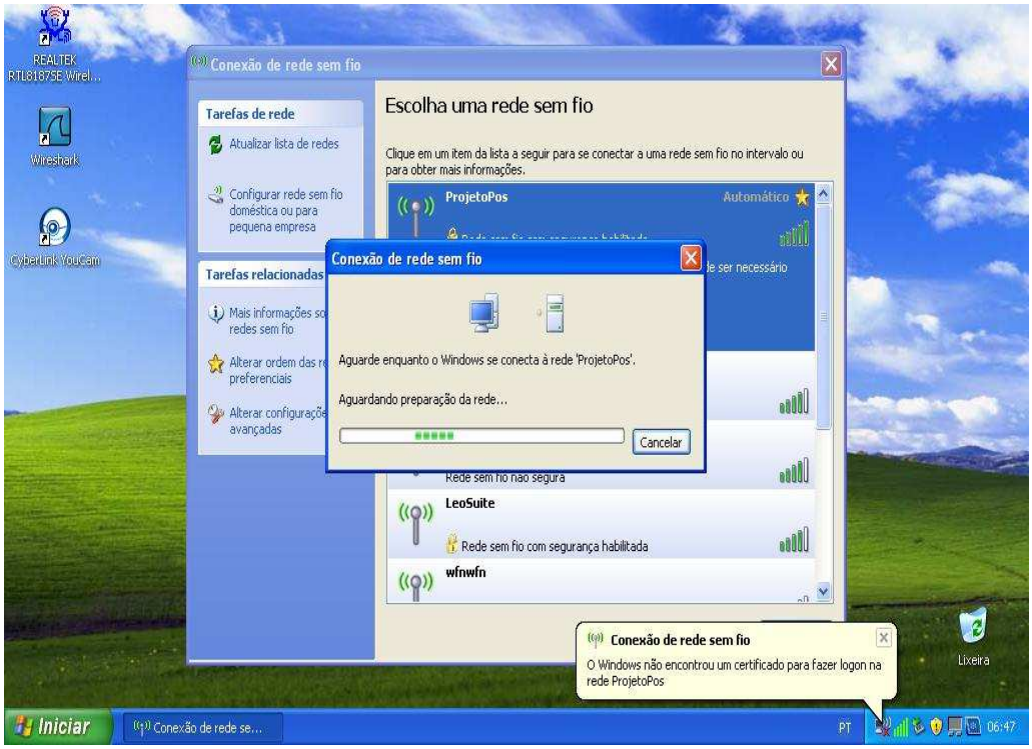
Fonte: O próprio autor

4.4.3 Tentativa de conexão de usuário sem certificado de autenticação

Com objetivo de comprovar que apenas os usuários que possuem certificados em sua maquina fornecidos pela AC(autoridade certificadora) que para este projeto tem o nome de Laterza CA

Quando é feita a tentativa de conexão na rede o servidor Radius busca autenticação do usuário, não encontrando o certificado é apresentada a mensagem de erro "*O Windows não encontrou um certificado para fazer logon na rede ProjetoPos"* conforme visto na figura 24, sendo assim somente após o usuário requerer e instalar o certificado em seu computador será possível que ele se conecte a rede sem fio.

Figura 24 – Tentativa de login na rede sem certificado



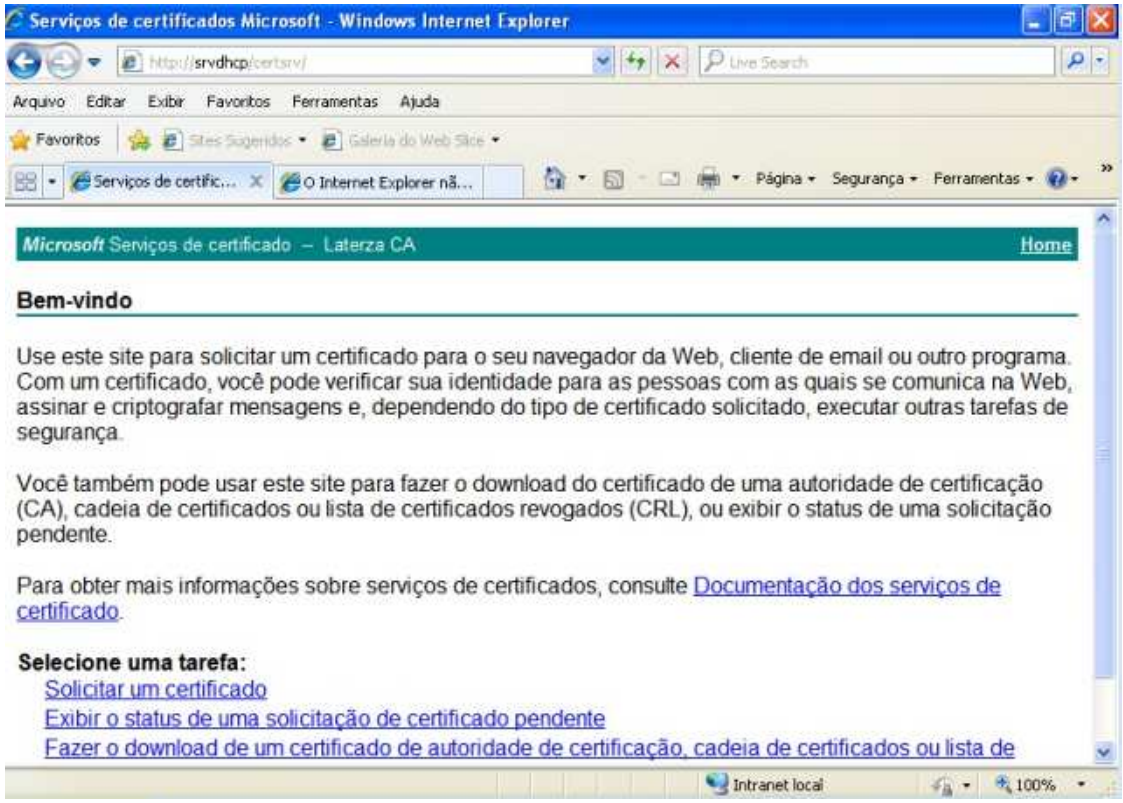
Fonte: O próprio autor

4.4.4 Requisição de Certificado

Para possibilitar a conexão e autenticação do usuário na rede implementada é necessário a requisição certificado a AC, o processo de requisição e feito com o computador cliente logado no domínio e conectado a rede cabeada.

A requisição é realizada acessando via navegador de internet, que para este projeto será utilizado o Internet Explorer, o endereço do serviço de certificado do servidor que tem como endereço para esta implementação *HTTP://srvdhcp/certsrv* conforme apresentado na figura 25 no qual esta mostrando a pagina inicial do servidor de certificado.

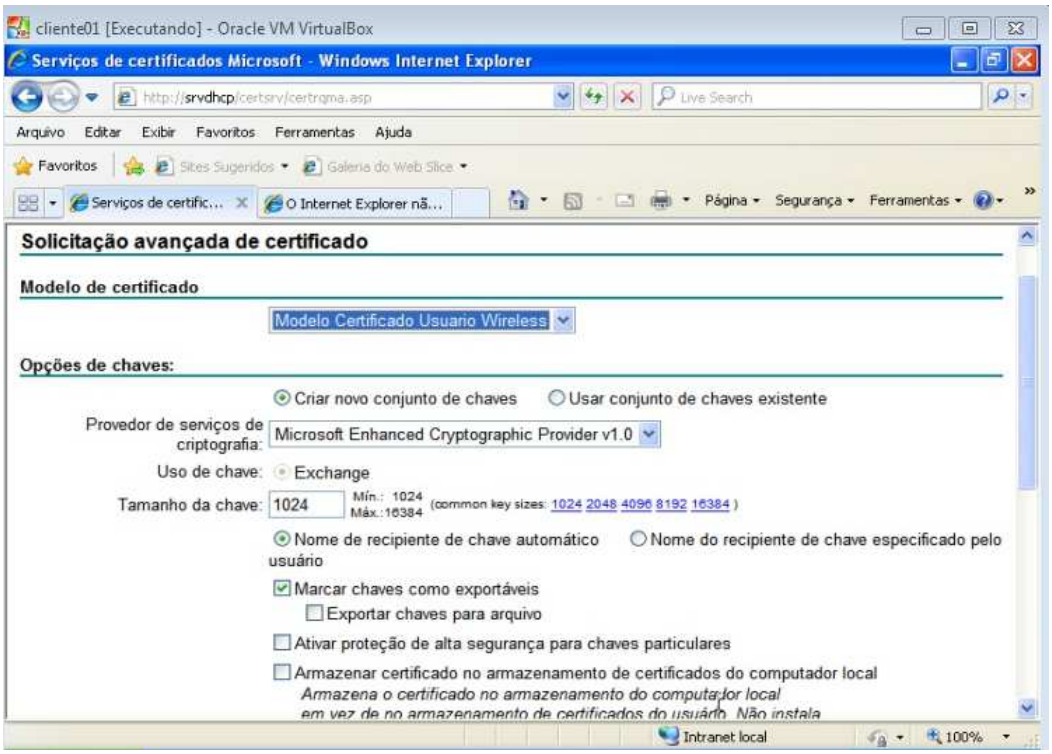
Figura 25 – Pagina inicial do servidor de certificados.



Fonte: O próprio autor

Após clicar na opção de solicitar certificado de usuário deve ser clicar no link mais opções que permite a escolha do tipo de certificado a ser gerado como apresentada na figura 26, deve ser escolhido o modelo de certificado criado para usuários Wireless.

Figura 26 – Seleção de modelo de certificado de usuário



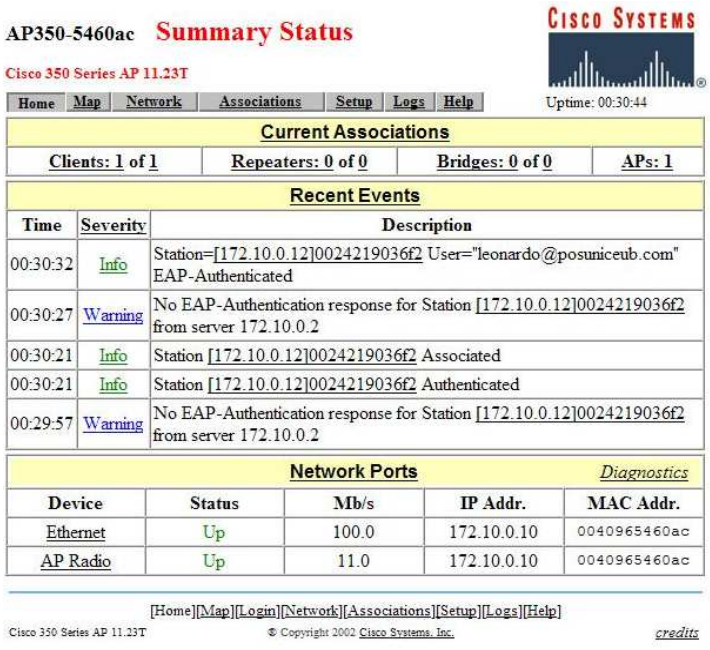
Fonte: O próprio autor

4.5 Resultados

4.5.1 Status de autenticação na pagina de configuração do AP

Após as configurar os requisitos de uma conexão a um rede wireless com autenticação EAP-TLS, sendo estas estar registrado no domino e possuir certificado digital fornecido pela AC do domínio, assim a conexão com a rede wireless PosProjeto foi estabelecida com sucesso, como visto na figura 27 que é a pagina de configuração do AP, no status de eventos do roteador indica que o computador de ip 172.10.0.12 realizou com sucesso a autenticação do usuário Leonardo, comprovando assim o sucesso do implementação proposta para este projeto.

Figura 27 – Pagina de configuração do AP



AP350-5460ac **Summary Status**

Cisco 350 Series AP 11.23T

Home | Map | Network | Associations | Setup | Logs | Help

Uptime: 00:30:44

Current Associations

Clients: 1 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
00:30:32	Info	Station=[172.10.0.12]0024219036f2 User="leonardo@posuniceub.com" EAP-Authenticated
00:30:27	Warning	No EAP-Authentication response for Station [172.10.0.12]0024219036f2 from server 172.10.0.2
00:30:21	Info	Station [172.10.0.12]0024219036f2 Associated
00:30:21	Info	Station [172.10.0.12]0024219036f2 Authenticated
00:29:57	Warning	No EAP-Authentication response for Station [172.10.0.12]0024219036f2 from server 172.10.0.2

Network Ports *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	172.10.0.10	0040965460ac
AP Radio	Up	11.0	172.10.0.10	0040965460ac

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

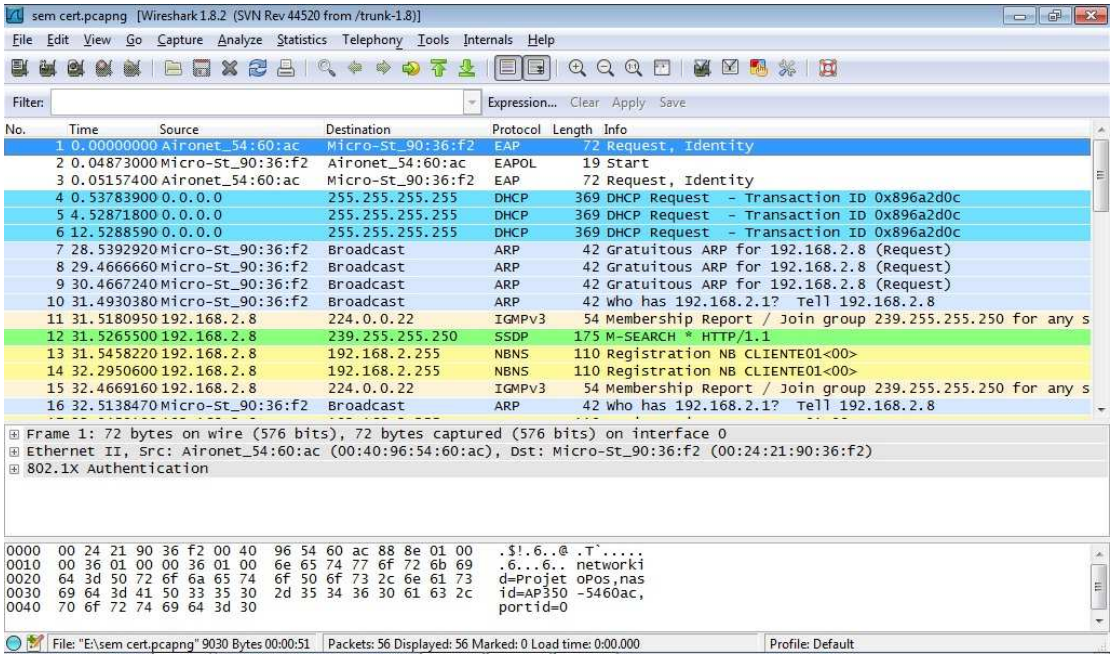
Cisco 350 Series AP 11.23T © Copyright 2002 Cisco Systems, Inc. *credits*

Fonte: O próprio autor

4.5.2 Análise de tráfego da rede com Wireshark

Com objetivo de testar a eficácia do protocolo de autenticação EAP-TLS bem como o perfeito funcionamento da rede implementada, foi realizado uma captura de pacotes no momento de um tentativa de conexão de um usuário que apesar de estar cadastrado no domínio, este não possui seu certificado digital instalado no computador, como pode ser observado na figura 28 o usuário não é autenticado no servidor não tendo assim acesso a rede.

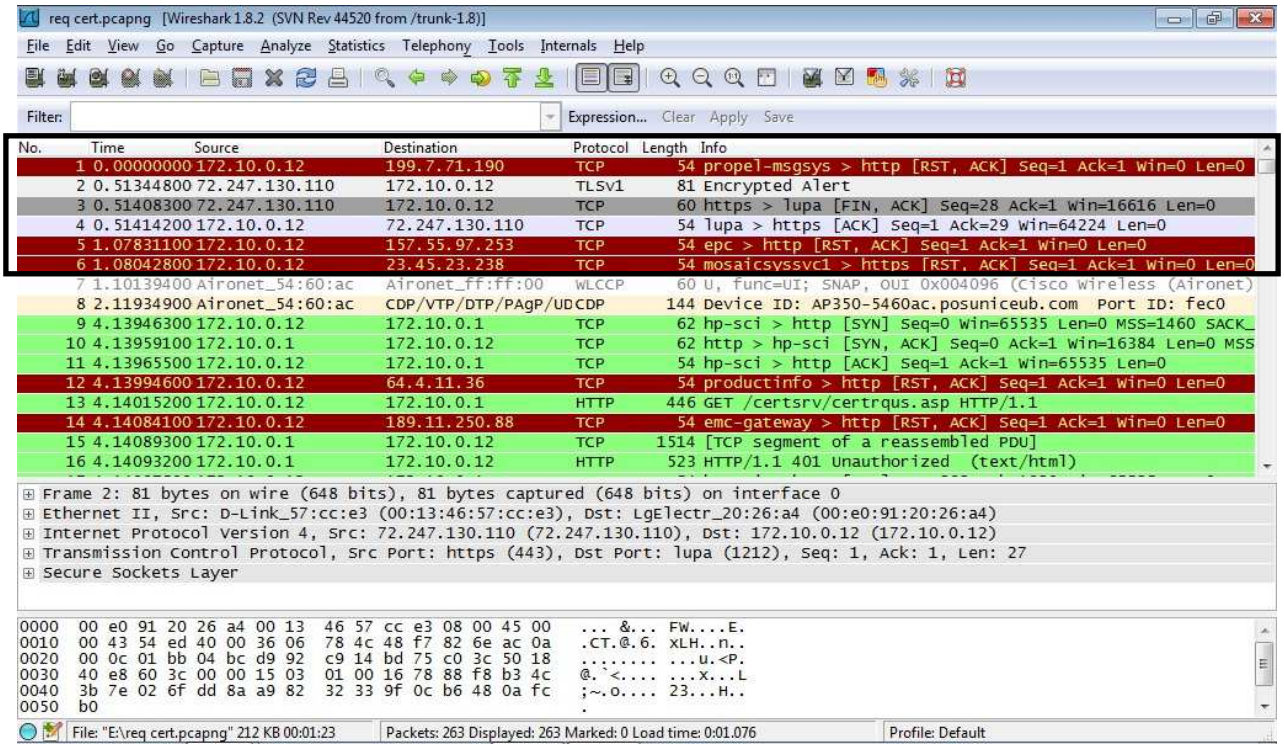
Figura 28 – Analise de pacotes de uma conexão sem certificado



Fonte: O próprio autor

Para que o usuário possa realizar a conexão na rede é necessária que ele seja autenticado na rede através de seu certificado digital, sendo esse solicitado a AC, este processo de requisição é feito através do navegador de internet no qual o usuário acessa o servidor através do endereço: HTTP://srvdhcp/certsrv, a comunicação e transmissão do certificado entre servidor ocorre de forma segura utilizando o protocolo TLS no qual os dados transmitidos na conexão são criptografados, a utilização do TLS pode ser confirmada pela captura de pacotes feita com *Wireshark* representada na figura 29 durante o processo de requisição de certificado.

Figura 29 – Captura de pacotes na requisição do certificado digital.

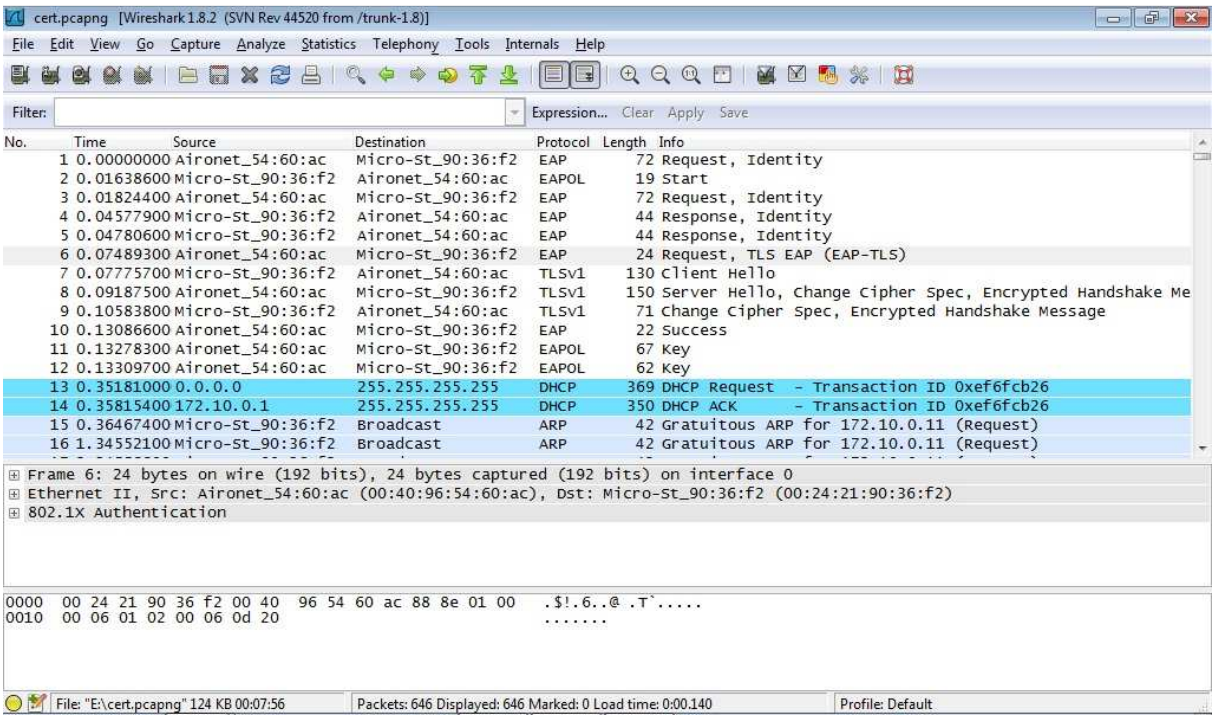


Fonte: O próprio autor

Alem da verificação de autenticação no servidor que pode ser vista na pagina de status do AP, outra forma de comprovar o sucesso da autenticação do usuário na rede implementada é através da captura de pacotes, conforme visto na figura 30 a autenticação é realizada seguindo os seguintes passos:

- suplicante(usuário) inicia a conexão e tem sua identidade solicitada pelo autenticador(AP).
- Uma vez enviada a identidade pelo suplicante o autenticador envia essa identidade ao servidor de autenticação,
- Após ser autenticado é estabelecida a conexão pelo autenticador(AP).
- O suplicante(usuário) então solicita que o servidor de autenticação informe sua identidade que é autenticada pelo suplicante(usuário).

Figura 30 – Captura de pacote na autenticação do usuário



Fonte: O próprio autor

CONCLUSÃO

O aumento da utilização de equipamentos ligados a rede sem fio tem atraído cada vez mais invasões a estes equipamentos através da quebra de chaves e outras formas de intrusão com objetivo de roubos de informações sigilosas de usuários, a possibilidade de invasão facilitada por uma rede sem fio de segurança fraca é dos fatores que inibe empresas de optarem por redes sem fio ao em vez de redes cabeadas.

O padrão IEE 802.1X e o protocolo de autenticação EAP-TLS permite uma segurança melhor que outros protocolos como o WEP por exemplo, pois para que um usuário possa se conectar a uma rede sem fio que utiliza o EAP-TLS como protocolo de autenticação, é necessário que este usuário esteja cadastrado no banco de usuários do domínio, além disso o mesmo deve ter o certificado digital emitido pela AC do controlador de domínio.

Pode - se concluir que mesmo com a máxima da segurança que não se pode afirmar que um ambiente de rede seja 100% seguro, a utilização do EAP-TLS como protocolo de autenticação permite uma possibilidade de invasão de maior grau de dificuldade, conseqüentemente o aumento da utilização de rede sem fio em grandes empresas pela possibilidade de implantação de um ambiente seguro.

REFERÊNCIAS

1 - TANENBAUM, A. S. **Rede de Computadores**. Campus, 2003

2 – PEIKARI, SETH FOGIE. **Maximum Wireless SecurityCyrus**, Sams, Dezembro 2002

3 - FARIAS Paulo César Bento. **Redes**, Digerati 2006

4 - CORDEIRO, Luis Gustavo. **Certificação Digital – Conceitos e Aplicações Modelos Brasileiro e Australiano**, 1ª Edição, Ciência Moderna

5 – EDNEY, ARBAUGH, **Real 802.11 Security: Wi-Fi Protected Access and 802.11i**, Addison Wesley, 2004

6 - BLUNK, L,VOLLBRECHT, J. RFC 2284 - **PPP Extensible Authentication Protocol (EAP)** , Disponível em <http://www.ietf.org/rfc/rfc2284.txt> Acesso em 22/07/2012

7 - J.RITTINGHOUSE, J.RANSOME - **Wireless Operational Security**. Elservier, 2004

8 – **CISCO. EAP-TLS Deployment Guide for Wireless LAN Networks** , Disponível em < http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml#wp39068> Acesso em 22/06/2012

9 - HASSELL, J. **Radius**, 1 ed, O'Reilly ,2002

10 - OHRTMAN, F. Roeder, K. **Wi-Fi Handbook: Building 802.11b Wireless Networks**, 1ed, 2003.