3
Aspectos e Mecanismos de Segurança no Padrão IEEE 802.11

3.1
Redes com Fio x Redes sem fio

As mensagens trocadas entre as entidades sem fio (pontos de acessos e terminais de usuários) podem ser facilmente interceptadas por um intruso. As redes locais sem fio, por utilizarem o ar como meio de transmissão, permitem que informações e recursos possam ser acessados e utilizados em qualquer lugar e a qualquer momento. Qualquer pessoa com um receptor apropriado pode interceptar as mensagens sem ser detectado.

A interceptação em redes com fio é mais complexa, pois o sinal está confinado no meio de transmissão (fibra ótica, cabo metálico ou cabo coaxial).

a) Redes com fio:
- ⇨ Os limites físicos da rede estão bem definidos;
- ⇨ O meio é controlável;
- ⇨ Apenas as estações fisicamente conectadas podem ter acesso à rede.

b) Redes sem fio:
- ⇨ Os limites físicos são amplos e difíceis de definir e restringir;
- ⇨ O meio é incontrolável;
- ⇨ Qualquer estação dentro da área de abrangência da rede pode ter acesso aos dados;
- ⇨ Há necessidade de mecanismos de autenticação, confidencialidade e integridade para tornar a rede equivalente a uma rede com fio.

3.2
Mecanismos Básicos de Segurança no Padrão IEEE 802.11

O padrão IEEE 802.11 possui mecanismos básicos para aumentar a segurança da rede, incluídos na própria especificação, que devem ser implementados pelo Administrador da Rede assim que o equipamento é ativado, para tornar a rede mais segura. Estes mecanismos, apesar de muito fracos, possibilitam o primeiro nível de segurança das redes IEEE 802.11 e não devem ser desconsiderados.

Mesmo com a adoção destes mecanismos, o risco potencial de ataque continua a existir.

Mecanismos básicos do padrão IEEE 802.11 para aumentar a segurança:

a) Controle de acesso pela identificação do endereço MAC;

b) Controle de acesso pela identificação da rede (*SSID- Service Set Identification*);

c) Autenticação, criptografia e integridade dos dados pelo WEP.

3.2.1
Controle de Acesso pela Identificação do Endereço MAC (*MAC Address Filtering)*

O AP identifica cada cartão *wireless* da estação pelo respectivo endereço MAC (*Media Access Control*), definido pelo fabricante durante o processo de industrialização.

Esta técnica baseia-se no uso de uma lista de endereços que estão autorizados a ligar-se à rede.

É possível configurar o AP de tal forma que os serviços só possam ser utilizados após o cartão ter sido registrado. Portanto, o AP determinará se o usuário está autorizado ou não a usar a rede pelo MAC do seu cartão. Contudo, este processo é complexo, pois o AP precisa manter uma lista de endereços de todos os usuários, o que, em termos de administração, é uma atividade bastante trabalhosa e, em certos casos, quase impossível, dependendo do tamanho da rede.

Portanto, só tem sentido para pequenas redes, pois o endereço MAC de um dispositivo tem que estar presente em todas as listas de AP às quais este possa

vir a ligar-se. Se um dispositivo é roubado ou alterado tem-se que proceder à correção do novo MAC em todas as listas de acesso, bem como à remoção do anterior.

Mesmo que esta estratégia seja implementada, não é possível evitar que uma pessoa mal-intencionada altere o endereço MAC por um localmente administrado, escolhendo-o, aleatoriamente, até que um MAC válido seja encontrado. Outra possibilidade é a utilização de um "*sniffer*" de rede para identificar o tráfego de usuários ativos e seus respectivos MAC's. Utilizando-se deste endereço, o elemento intruso pode participar da rede como se fosse um usuário válido.

Acrescenta-se ainda o fato de que o endereço MAC é enviado em claro pela rede.

Desta forma, conclui-se que a estratégia de utilizar o MAC como método de autenticação não é aconselhável.

3.2.2
Controle de Acesso pela Identificação do SSID (*Network ID*)

Uma rede IEEE 802.11 possui um identificador denominado SSID (*Service Set Identification*) que a distingue das demais. O SSID vem programado de fábrica com um nome *default*.

Exemplo de fabricantes e seus SSID *default*:

Cisco: SSID *default* = "*Tsunami*";

3Com: SSID *default* = "*101*";

Compaq: SSID *default* = "*Compaq*".

A comunicação é iniciada enviando-se o identificador SSID.

O SSID segue em claro na transmissão.

O controle de acesso realizado pela identificação do SSID é totalmente ineficaz como meio de segurança, pois existem softwares disponíveis que interceptam o SSID.

Desta forma, conclui-se que a estratégia de utilizar o SSID como método de autenticação também não é aconselhável.

Porém, para minimizar os riscos, é recomendada a desabilitação do *broadcast* de SSID e a escolha de um nome não óbvio para o SSID.

3.3
WEP - *Wired Equivalent Privacy*

3.3.1
Características

Como o objetivo é tornar o ambiente sem fio tão seguro quanto o de redes com fio, a encriptação dos dados e a autenticação das estações deverão ser sempre consideradas. Com esse intuito, o padrão IEEE 802.11 introduziu um conjunto adicional de procedimentos de segurança chamado WEP – *Wired Equivalent Privacy*.

O mecanismo WEP tem por objetivo fazer as redes sem fio tão seguras quanto às redes com fio.

O WEP transfere para a camada de enlace funções de segurança para que serviços superiores (desenvolvidos para redes com fio) possam ser executados.

O WEP utiliza uma chave de criptografia *(Chave Secreta)* compartilhada com as partes envolvidas na comunicação e tem a intenção de cumprir as seguintes metas de segurança:

a) ***Autenticação (Controle de Acesso)***: deve garantir que apenas pessoas autorizadas tenham acesso à rede. Ou seja, o protocolo deve evitar que um elemento estranho utilize a rede para enviar e receber mensagens;

b) ***Criptografia (Confidencialidade)***: deve evitar que o intruso compreenda o tráfego capturado. Ou seja, o protocolo deve evitar que elementos estranhos tomem conhecimento do conteúdo das mensagens transmitidas através da rede;

c) ***Integridade dos Dados***: o protocolo não deve permitir que o conteúdo da mensagem seja modificado. Ou seja, deve garantir que os dados indevidos não sejam inseridos ou removidos durante a transmissão.

Em todas as metas acima, a segurança da rede está baseada na dificuldade em se obter a chave de criptografia (*Chave*).

Como será visto adiante, o WEP dá aos administradores de rede uma falsa sensação de segurança. Mesmo quando o WEP é corretamente configurado e

implementado em uma rede sem fio, é possível "quebrar" a criptografia e ganhar o acesso à rede.

Algumas características importantes do WEP que serão dealhadas adiante:

a) A *Chave* é estática e configurada manualmente;

b) O WEP requer que a mesma *Chave* seja compartilhada com todos os usuários.

Existem duas formas de operação da chave de criptografia no WEP:

a) ***Clássica***: trabalha com *Chaves* de 64 bits (40 + 24). A operação com chaves de 64 bits é raramente usada, pois é curta o suficiente para tornar os ataques de força bruta possíveis; e

b) ***Estendida***: trabalha com *Chaves* de 128 bits (104 + 24). Esta chave torna os ataques de força bruta mais difícil. Porém, como será visto adiante, a insegurança do WEP não dependerá exclusivamente do tamanho da chave, o que torna a chave de 128 bits também ineficaz.

O tamanho das chaves clássica e estendida já considera a concatenação de 24 bits (IV), formando a chave que realmente será utilizada na criptografia, como será visto adiante.

3.3.2
Tipo de Criptografia

A forma mais simples (e a mais usada) para manter uma conexão segura é escolher um segredo (uma chave secreta pré-definida) e configurar dois pontos para criptografar seus dados usando a mesma chave. Esta criptografia é chamada de simétrica.

O ponto crítico da criptografia simétrica encontra-se na premissa de que os dois pontos acordaram sobre uma chave a ser usada e somente eles possuem conhecimento sobre esta chave. Em transações onde os pontos não podem obedecer a esta premissa, faz-se necessário o uso de algum algoritmo que não necessite de uma chave pré-estabelecida entre as duas partes.

A solução para este problema foi dada pela criptografia assimétrica.

Por realizar operações matemáticas relativamente simples, o tempo computacional gasto pelos algoritmos de chave simétrica é satisfatoriamente curto

para ser implementado sem adicionar sobrecarga nos sistemas físicos atualmente no mercado.

A figura a seguir ilustra o mecanismo de funcionamento de um sistema com criptografia de chave simétrica.

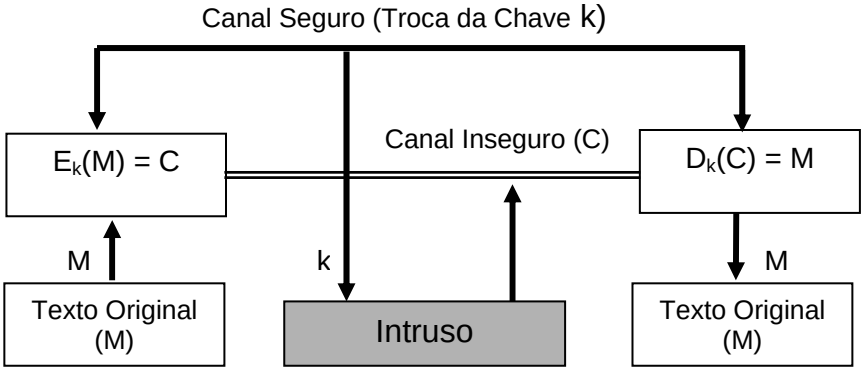


Figura 28: Esquema de criptografia com chave simétrica

Notação para cifragem e decifragem dos dados:

E: Processo (algoritmo) para cifrar um texto utilizando uma chave secreta "k";

M: Texto Fonte (*Plaintext*);

C: Texto Cifrado (*Cyphertext*).

D: Processo (algoritmo) para decifrar o texto utilizando uma chave secreta "k".

$$E_k(M) = C$$

Para decifrar, utiliza-se a mesma chave secreta "**k**":

$$D_k(C) = M$$

ou

$$D_k(E_k(M)) = M$$

A inconveniência do pré-estabelecimento de uma chave secreta exigida pelo algoritmo de chave simétrica é contornada utilizando-se a criptografia assimétrica.

Neste modelo de criptografia, duas chaves são utilizadas para realizar o processo de encriptação/desencriptação, o que uma encriptar somente a outra pode desencriptar. Desta forma, um ponto tentando estabelecer uma conexão segura com outro deverá gerar as duas chaves: a chave pública e a chave privada. A chave pública pode ser livremente distribuída, já que de nada adianta a chave pública sem a privada para completar a encriptação/desencriptação.

Como se utiliza de algoritmos reversos para desencriptar mensagens, o tempo computacional utilizado pelos algoritmos de criptografia assimétrica é muito elevado, tornando-se inviável o uso de uma comunicação intensa de dados.

3.3.3
Algoritmo RC4

O RC4 (*Ron's Cipher 4*) é um algoritmo do tipo *stream cipher*..

Neste algoritmo, a mensagem é codificada, caractere a caractere, através de uma seqüência (*keystream*) gerada a partir de uma chave inicial.

O RC4, inicialmente, realiza a expansão da chave. Posteriormente, é aplicado o algoritmo PRGA *(Pseudo-Random Generating Algorithm)* para gerar os bytes aleatórios.

Vantagens do algoritmo RC4:

a) É um algoritmo de fluxo (*stream*) e de grande desempenho;

b) Possui fácil implementação em hardware e software. Esta característica é importante devido à baixa capacidade de processamento dos equipamentos de redes sem fio;

c) Possui limitada ou nenhuma propagação de erros.

3.3.4
Criptografia no WEP

O WEP utiliza um vetor de inicialização IV *(Inicialization Vector*) de 24 bits, randômico, concatenado à chave de criptografia (*Chave Secreta*) para formar uma chave pseudo-randômica do tamanho da mensagem.

A chave pseudo-randômica é obtida a partir do algoritmo RC4, conforme apresentado na figura a seguir:

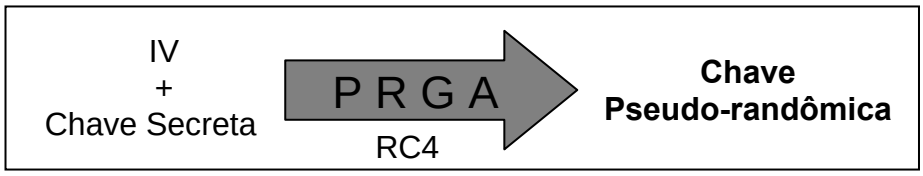


Figura 29: Mecanismo de formação da chave Pseudo-Randômica

Para possibilitar a proteção dos dados na transmissão da mensagem é inserido um verificador de integridade ICV - *Integrity Check Value* que utiliza o algoritmo de *Checksum* CRC32 - *Cyclic Redundancy Check de 32 bits.* Este algoritmo visa proteger a mensagem quanto a uma alteração não autorizada no texto durante a transmissão.

A seguir será apresentado o mecanismo de cifragem dos dados no WEP.

Seja uma mensagem M:

1. Inicialmente, calcula-se o *Integrity Checksum* de M (c(M)) através do CRC-32;
2. Concatena-se c(M) à mensagem M, obtendo-se P = < M,c(M)>.
3. Observa-se que P não depende da chave secreta k;

a. c) Posteriormente, deve-se escolher randomicamente um Vetor de Inicialização (IV) e concatená-lo à chave secreta, obtendo-se <IV,k>;

4. A partir de <IV,k>, gera-se a chave pseudo-randômica através do algoritmo PRGA do RC4;
5. Faz-se C = P ⊕ RC4 (IV,k);
6. Transmite-se IV e C.

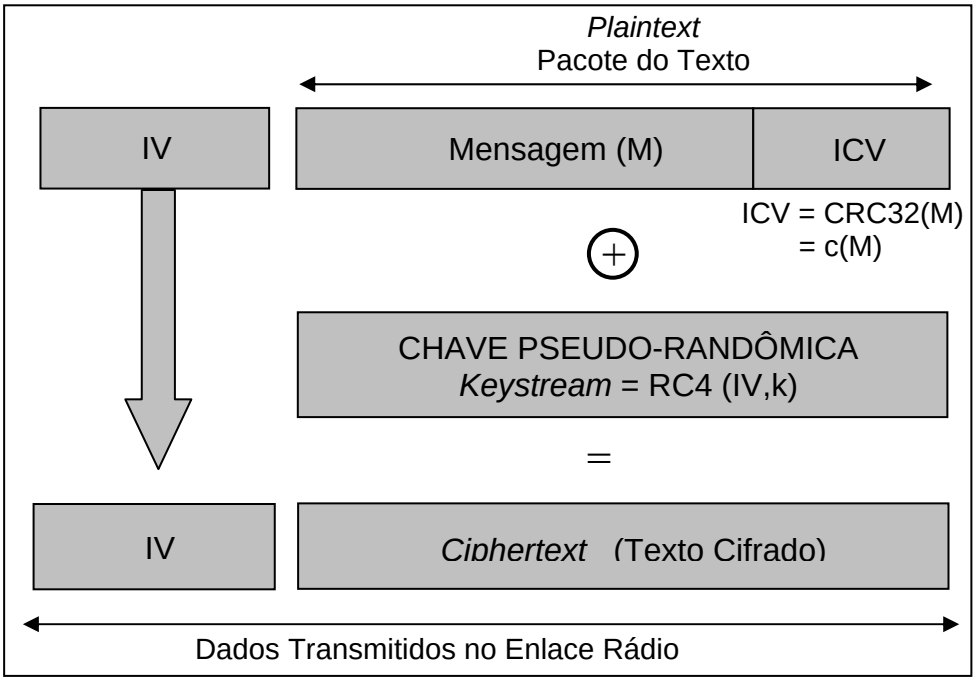


Figura 30: Cifragem dos dados no WEP

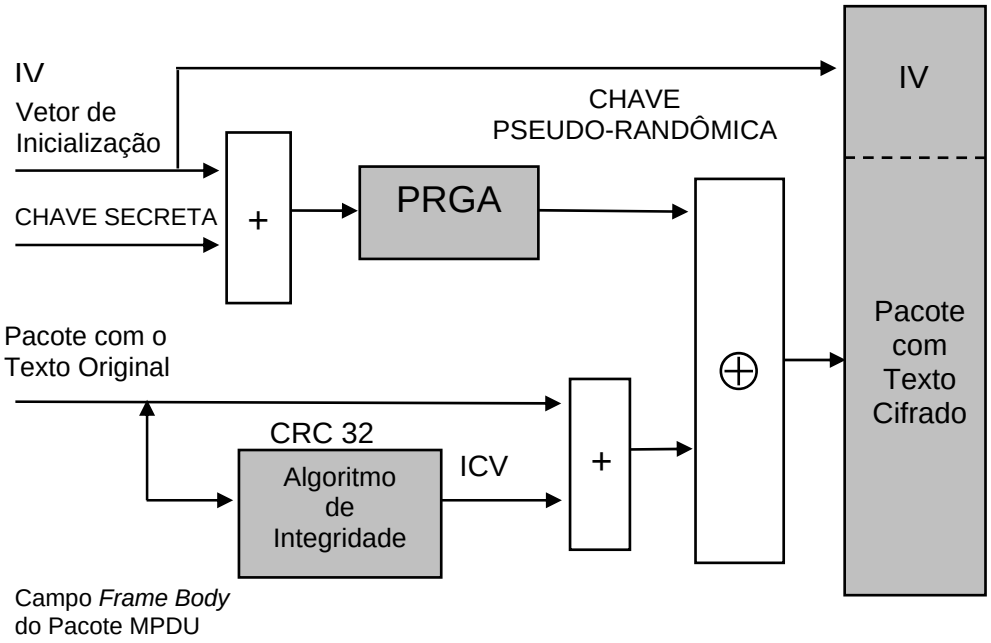


Figura 31: Cifragem dos dados no WEP (Diagrama em Blocos)

A estação destino, que possui a mesma chave secreta, usa o IV que é transmitido no início do pacote para criar a mesma Chave Pseudo-randômica gerada pelo PRGA, e decriptar o texto cifrado.

A estação processa o CRC-32 sobre esse texto decriptado e obtém um novo valor de ICV. A estação compara esse novo valor de ICV com o valor que foi transmitido no final do pacote (ICV_T). Se os valores forem diferentes, o pacote é descartado.

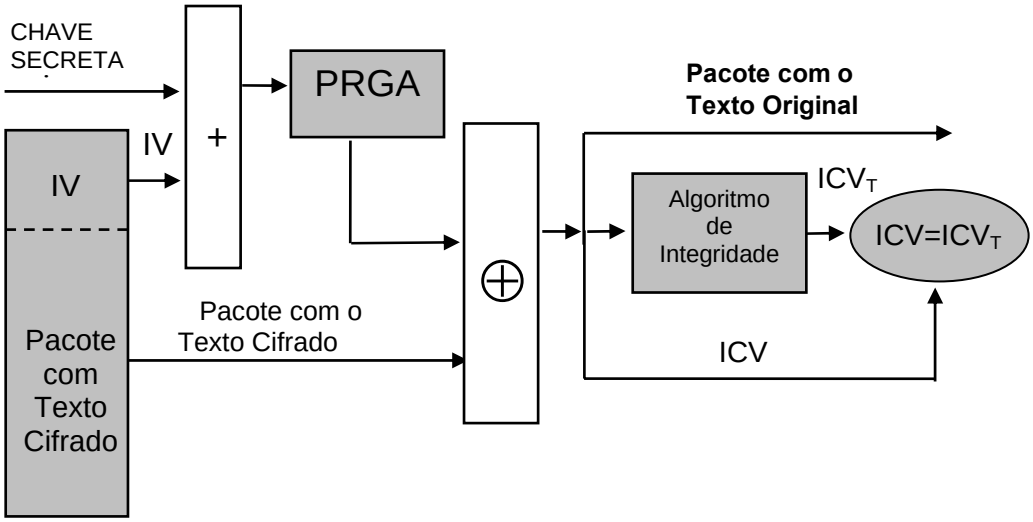


Figura 32: Decifragem dos dados no WEP (Diagrama em Blocos)

3.3.5
Autenticação no WEP

O Padrão IEEE 802.11 especifica dois modos de autenticação:

a) **Sistema Aberto (*Open System Authentication)***: serviço de autenticação padrão. Funciona apenas como mecanismo de identificação. O protocolo WEP é utilizado apenas para criptografia;

b) **Sistema com Autenticação através da Chave Compartilhada *(Shared Key Authentication)*:** utiliza-se a chave compartilhada tanto para autenticar as estações, quanto para criptografar/decriptografar as mensagens.

No sistema aberto não há autenticação. Qualquer estação pode se associar com qualquer ponto de acesso e ouvir todos os dados que estão sendo enviados. Este método de autenticação deve ser evitado.

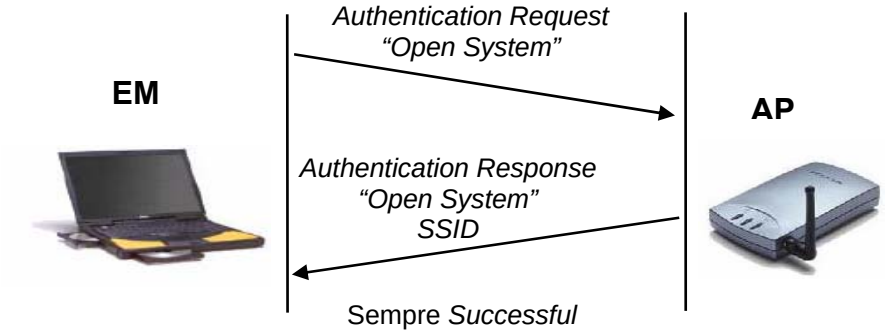


Figura 33: Troca de mensagens no sistema aberto

Problemas deste tipo de autenticação:

1º) Ataque passivo para captura legível de informação da rede: a rede fica sem criptografia. Neste caso, programas e serviços que não utilizam cifragem como, por exemplo: TELNET, FTP e e-mail, disponibilizam nomes de usuários e senhas. Além disso, todos os sistemas computacionais em execução nesta rede estarão disponíveis a qualquer pessoa dentro da área de cobertura do AP. Ou seja, o invasor pode perfeitamente mascarar-se sem ser notado.

2º) Ataque ativo durante a comunicação: um invasor pode se fazer passar por um AP. Neste caso, as EM's passam a confiar informações ao invasor, pois não há autenticação. Este tipo de ataque é chamado "*man-in-the-middle*". Nele o invasor pode se fazer passar por uma EM e receber permissão para usar a rede.

O sistema de chave compartilhada provê uma segurança melhor do que o de sistema aberto. No entanto, a mesma chave compartilhada utilizada para encriptar/decriptar mensagens também é utilizada para autenticar as estações. Isto é considerado um risco de segurança.

Neste sistema é necessário que o WEP seja ativado.

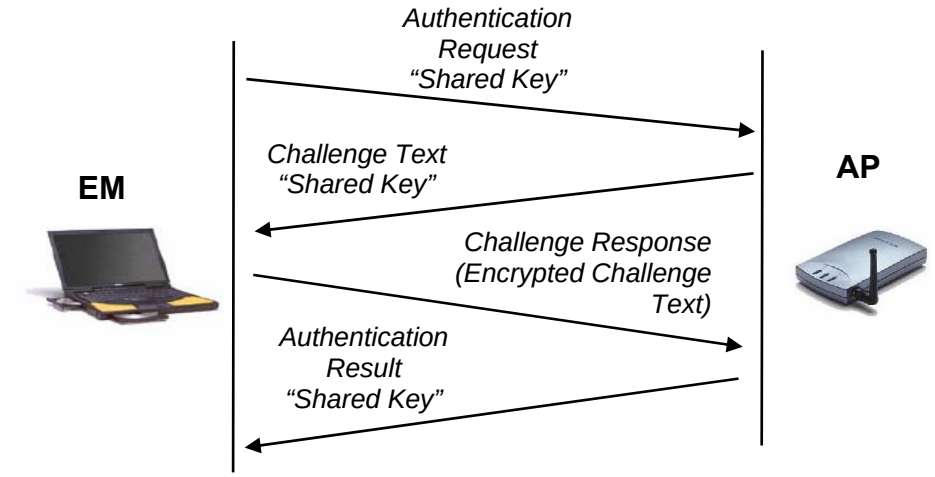


Figura 34: Troca de mensagens no sistema com autenticação através da chave compartilhada

Processo de autenticação:

1. A EM envia solicita de autenticação para o AP;
2. Quando o AP recebe a solicitação de autenticação, ele responde com um quadro de autenticação com 128 bytes de texto randômico de desafio gerado pelo WEP;
3. A EM deve então encriptar o texto com a chave compartilhada e devolver para o Ponto de Acesso;
4. O AP vai desencriptar o texto recebido com a chave compartilhada e comparar com o que foi enviado. Se estiver correto, ele responde que a autenticação teve sucesso.

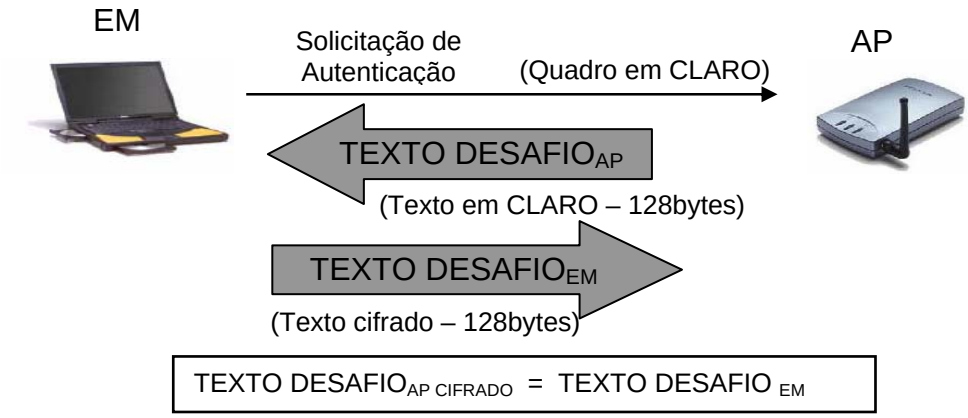


Figura 35: Fluxo de mensagens no sistema com autenticação através da chave compartilhada

O Sistema com Autenticação através da Chave Compartilhada provê um nível mais alto de autenticação. A chave secreta reside em cada estação. O Padrão IEEE 802.11 não especifica como se distribui as chaves entre as estações.

O PRGA (RC4) é o componente mais crítico do WEP, já que é o real responsável pela encriptação. O vetor de inicialização aumenta a vida da chave secreta e provê a auto-sincronização do algoritmo.

A chave secreta continua constante e o IV se altera periodicamente. O IV pode variar a cada envio de pacote.

3.3.6
Integridade no WEP

Como já visto anteriormente, para possibilitar a proteção dos dados na transmissão da mensagem é inserido um verificador de integridade ICV - *Integrity Check Value* que utiliza o algoritmo de *Checksum* CRC32 - *Cyclic Redundancy Check de 32 bits* para cada quadro transmitido.

Este algoritmo tem por objetivo proteger a integridade da mensagem quanto a uma alteração não autorizada no texto durante a transmissão.

3.3.7
Fragilidades e Vulnerabilidades do WEP

Conforme os trabalhos de [9] à [14], o protocolo WEP possui diversas falhas de criptografia que tornam o padrão IEEE 802.11 inseguro.

As principais falhas e violações estão relacionadas às três metas de segurança que constituem a base do WEP, como será apresentado adiante.

3.3.7.1
Fragilidade na Criptografia

A criptografia, como já visto, utiliza a chave pseudo-randômica gerada pelo RC4.

Assim, sejam dois textos legíveis distintos P_1 e P_2 que são criptografados através da mesma chave pseudo-randômica RC4(k,IV) em C_1 e C_2.

Temos que : $\boldsymbol{P} = \langle \boldsymbol{M}, \boldsymbol{c}(\boldsymbol{M}) \rangle$

Sejam duas mensagens criptografadas C_1 e C_2 :

$$\boldsymbol{C_1} = \boldsymbol{P_1} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k}) \quad \boldsymbol{e} \quad \boldsymbol{C_2} = \boldsymbol{P_2} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k})$$

Logo ***teremos*** :

$$\boldsymbol{C_1} \oplus \boldsymbol{C_2} = [\boldsymbol{P_1} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k})] \oplus [\boldsymbol{P_2} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k})]$$

$$\boldsymbol{C_1} \oplus \boldsymbol{C_2} = \boldsymbol{P_1} \oplus \boldsymbol{P_2} = \langle \boldsymbol{M_1}, \boldsymbol{c}(\boldsymbol{M_1}) \rangle \oplus \langle \boldsymbol{M_2}, \boldsymbol{c}(\boldsymbol{M_2}) \rangle$$

$$\boldsymbol{Assim}, \quad \boldsymbol{C_1} \oplus \boldsymbol{C_2} = [\boldsymbol{P_1} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k})] \oplus [\boldsymbol{P_2} \oplus \boldsymbol{RC4}(\boldsymbol{IV}, \boldsymbol{k})] = \boldsymbol{P_1} \oplus \boldsymbol{P_2}$$

$$\boldsymbol{Logo\ tem-se} : \boldsymbol{C_1} \oplus \boldsymbol{C_2} \oplus \boldsymbol{P_1} = \boldsymbol{P_1} \oplus \boldsymbol{P_2} \oplus \boldsymbol{P_1} = \boldsymbol{P_2}$$

Assim, conclui-se que, de posse de 02 textos criptografados (C_1 e C_2) e de 01 texto legível (P_1), é possível descobrir o outro texto legível (P_2).

Uma operação XOR entre duas mensagens criptografadas com o mesmo vetor de inicialização (IV) cancela a chave pseudo-randômica e torna-se um XOR entre os dois textos em claro. Assim, se um dos textos é conhecido, pode-se facilmente encontrar o outro.

A fim de tentar evitar esse problema, o WEP utiliza um vetor de inicialização para cada pacote, mas a chave secreta compartilhada dificilmente se altera.

3.3.7.2
Fragilidade Provocada pela Vetor de Inicialização

O Vetor de Inicialização (IV) no WEP tem 24 bits e, junto com a chave secreta, é o responsável por gerar a chave pseudo-randômica que encripta o texto legível.

O Vetor de Inicialização (IV) no WEP tem dois graves problemas:

a) O primeiro problema é o tamanho do IV, que é muito pequeno. O IV é alterado a cada pacote enviado, começando no zero e indo até o valor máximo 2^{24} - 1. Este número é pequeno, e o IV volta a assumir o valor 0 em curto espaço de tempo, com a taxa de transmissão do Padrão IEEE 802.11;

b) O Padrão IEEE 802.11 não especifica como o IV deve ser gerado.

⇨ Alguns fabricantes o fazem sequencialmente, com a desvantagem de ser fácil de prever e detectar, e outros ainda inicializam em zero quando o cartão é inserido;

⇨ Outros geram aleatoriamente, com a desvantagem do *Paradoxo do Aniversário*, onde, estatisticamente, tem-se 50% de chances de repetir o mesmo IV depois de 4.823 pacotes transmitidos;

⇨ A maioria dos fabricantes inicializa o IV em zero e o incrementa a cada pacote transmitido. Isto torna a colisão entre os vetores de valores baixos muito maior;

⇨ A mesma chave ***k*** é utilizada na comunicação EM => AP e AP => EM, e diferentes estações compartilham a mesma chave ***k***. Deste modo, tem-se colisão (dois pacotes com o mesmo IV) também entre pacotes enviados por máquinas diferentes. Isto torna a colisão ainda mais abundante.

É a partir dessa repetição do IV que o WEP pode ser quebrado.

A chave *k* é fixa e foi configurada nas estações que estão se comunicando, logo o par <*k*,IV> repetir-se-á sempre que o IV se repetir. E sempre que eles se repetirem, gerarão a mesma chave pseudo-randômica RC4(*k*,IV).

3.3.7.3
Fragilidade na Integridade dos Dados

A principal fraqueza do WEP é o seu algoritmo CRC32 de garantia de integridade (ICV - *Integrity Check Value*).

O CRC-32 possui duas propriedades importantes:

a) CRC 32 é independente da chave secreta (k);

b) CRC 32 é linear: $c(a \oplus b) = c(a) \oplus c(b)$, $\forall$ a e b. Esta propriedade é válida para qualquer tipo de algoritmo CRC.

O CRC 32 é um detetor de erros de transmissão, mas é inadequado para prover garantias criptograficamente aceitáveis contra adulteração intencional.

Como conseqüência imediata destas propriedades, tem-se o comprometimento da integridade dos dados. É possível se fazer modificações controladas no pacote sem que sejam detectadas por qualquer um dos dispositivos (transmissor ou receptor).

Utilizando a propriedade da linearidade do CRC-32 pode-se demonstrar que as mensagens podem ser modificadas em trânsito, sem detecção, violando uma das metas de segurança do WEP.

Na figura abaixo, a estação EM_A envia para a estação EM_B uma mensagem M encriptada. Observa-se que durante a transmissão, a mensagem M não é conhecida.

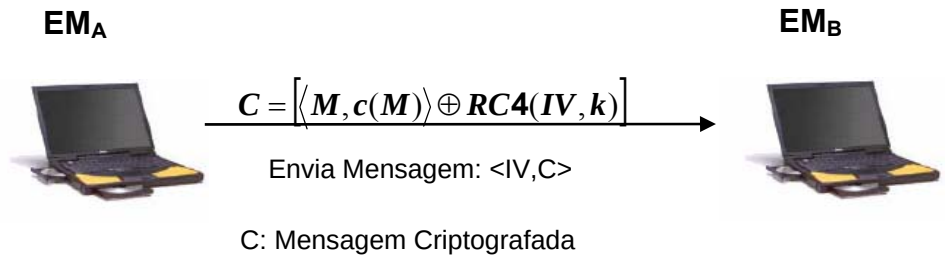


Figura 36: Fluxo de mensagens entre duas estações

Seja então C=<M,c(M)>⊕RC4(IV,*k*)) um texto cifrado capturado por um invasor que deseja modificá-lo para C'.

É possível encontrar uma nova mensagem criptografada C' que será desencriptada para M', com M'=M⊕Φ, onde Φ é uma mensagem "ruído" que pode ser escolhida e inserida arbitrariamente pelo adversário.

Ao desencriptar C', a estação EM_B irá obter a mensagem modificada M' com o CRC correto.

$$M' = M \oplus \Phi$$

$$C' = RC4(IV, k) \oplus \langle M' \oplus c(M') \rangle$$

$$c(M') = c(M) \oplus c(\Phi)$$

$$C' = RC4(IV, k) \oplus \langle M \oplus \Phi, c(M) \oplus c(\Phi) \rangle$$

$$C' = RC4(IV, k) \oplus \langle M, c(M) \rangle \oplus \langle \Phi, c(\Phi) \rangle$$

$$C' = C \oplus \langle \Phi, c(\Phi) \rangle$$

Assim, o invasor é capaz de substituir a transmissão original C pelo novo texto criptografado C', enganando a fonte.

Portanto, é possível inserir um ruído numa mensagem alterando não só a mensagem original como também o *checksum* da mensagem original, fazendo isso, prova-se que o CRC-32 não foi capaz de manter a integridade dos dados.

Isso significa que é possível fazer modificações arbitrárias nas mensagens sem receio de detecção.

Resumindo: pode-se interceptar o pacote, fazer a alteração (substituir M por M'), corrigir o CRC e a alteração não será detectada.

Assim, conclui-se que não há como garantir a integridade dos dados com o WEP.

3.3.7.4
Fragilidade na Autenticação (Controle de Acesso)

Além de modificar uma mensagem, é possível também inserir na rede uma nova mensagem, violando o controle de acesso à rede.

Utilizando a propriedade do CRC ser independente da chave secreta ***k***, pode-se mostrar que é possível injetar mensagens indevidas na rede.

Se o invasor conhecer uma mensagem P em claro, ele pode descobrir a chave pseudo-randômica relativa a um dado IV e utilizá-la para injetar tráfego na rede.

$$P \oplus C = P \oplus (P \oplus RC4(IV,k)) = RC4(IV,k)$$

A partir deste momento, o invasor terá a chave pseudo-randômica e o vetor de inicialização correspondente, podendo validar qualquer mensagem. A partir desta seqüência, é possível injetar na rede um novo pacote cifrado de uma nova mensagem M.

Com isso, um invasor estará apto a enviar para o AP o desafio cifrado corretamente, e, conseqüentemente, receberá a confirmação de autenticação na rede.

$$C' = \langle M', c(M) \rangle \oplus RC4(IV, k)$$

É importante lembrar que isso só é possível se for usado o mesmo IV da mensagem original. Mas, apesar do protocolo recomendar que não se reutilize o IV, ele não exige que os IV´s sejam trocados a cada pacote.

Como será visto posteriormente, uma das possíveis soluções para este problema seria utilizar um código de autenticação de mensagem (MAC – *Message Authentication Code*) com resistência criptográfica. Por exemplo, uma função de *Hash* que evitasse que o ICV fosse alterado por algum intruso.

3.3.7.5
Gerenciamento da Chave Secreta

O padrão IEEE 802.11 não especifica como deve ser realizada a distribuição das chaves secretas.

A distribuição é feita manualmente pelo Administrador da Rede. Dependendo da dimensão da rede e do número de usuários, fica bastante difícil a troca da chave periodicamente.

3.3.8
Ameaças mais Importantes

Estes mecanismos são insuficientes para dotar a rede de segurança e confiabilidade, e podem permitir a violação das informações e ataque por invasores.

Existem diversas ameaças, porém as mais importantes são:

a) MITM - *Man in the Middle* (interceptação de conteúdo): Consiste em interceptar o tráfego entre dois computadores e, para ambos, continuar parecendo que a comunicação é direta. Porém, a entidade que intercepta o tráfego também o altera, de forma que a requisição de rede pareça original e autêntica. Este tipo de ataque requer um grande conhecimento de programação e da rede que se deseja comprometer. Normalmente, este tipo de ataque requer que um dos pontos de conexão já tenha sido comprometido, seja um servidor de rede em que se deseja acessar, ou um provedor ao qual se esteja conectado. Este tipo de ataque normalmente é utilizado contra sistemas criptográficos, interceptação de informações cifradas em uma conexão utilizando chaves públicas;

b) *DoS (Denial of Service)*. Aqui existem muitas opções para um invasor. A interrupção do sinal de rádio pode ser feita usando tecnologia de baixo custo e de fácil aquisição no mercado. Existem os ataques mais sofisticados que visam os próprios protocolos sem fio de nível inferior, e os menos sofisticados que visam as redes, simplesmente inundando a WLAN com tráfego aleatório;

c) *Ataque de dicionário*: Este ataque tem por objetivo montar uma biblioteca com o par <chave, IV> e, desta forma, obter a chave de criptografia por força bruta;

d) Spoofing (roubo de endereço MAC): O acesso imediato à rede permite que um invasor falsifique informações que possam parecer provenientes de um usuário legítimo (por exemplo, uma mensagem de *e-mail* falsa) de maneira que não seria possível fora da rede;

e) *Eavesdropping*: facilidade com que se consegue escutar uma conversação, quer em tempo real, quer mesmo guardando os dados para uma posterior análise. É um dos ataques mais facilmente perpetráveis em WLAN;

f) *Hijack (roubo de sessão):* Este tipo de autenticação pode ser comprometido através da desassociação do dispositivo autorizado feita pelo

atacante, que assume sua identidade (captura de sessão). Pelo fato de as mensagens não serem autenticadas individualmente, é possível que um atacante falsifique um aviso de desassociação proveniente do servidor, e assuma a identidade da vítima da rede;

g) *Espionagem (divulgação de dados transmitidos)*. Pode resultar na revelação de dados confidenciais e de credenciais desprotegidas de usuários. Também permite que invasores coletem informações sobre os sistemas de TI da empresa/instituição, as quais podem ser usadas para organizar um ataque a outros sistemas ou dados que poderiam não estar vulneráveis;

h) *Ameaças acidentais*: Alguns recursos de WLAN fazem com que as ameaças não-intencionais pareçam mais reais. Por exemplo, um visitante legítimo pode iniciar um computador portátil sem intenção de se conectar à sua rede, mas se conectar automaticamente à WLAN da empresa. O computador portátil do visitante é agora um ponto de entrada potencial para vírus em sua rede. Este tipo de ameaça é um problema apenas nas WLAN sem proteção;

i) *Roubo de equipamento*: Em caso de roubo de equipamento *wireless*, a rede pode ser acessada sem que os administradores tenham conhecimento. Isto acontece porque o equipamento já está configurado para acessar a rede. Neste caso, pode ser necessário reconfigurar a rede para eliminar esta vulnerabilidade. A política de segurança deve requerer que os usuários notifiquem os administradores da rede em caso de perda ou roubo de laptops ou PDA, e os usuários devem ser educados neste sentido.

3.3.9
Conclusão sobre o WEP

Como mostrado nos itens anteriores, cada uma das metas de segurança propostas para o WEP é vulnerável:

a) Criptografia: pode-se ler o tráfego protegido;

b) Autenticação: pode-se injetar mensagens na rede;

c) Integridade dos Dados: pode-se modificar o conteúdo das mensagens.

Logo, somente o WEP não é suficiente para prover segurança às redes IEEE 802.11, sendo necessária a adoção de mais um nível de segurança.

3.4
Padrão IEEE 802.1x (*Port-Based Network Access Control*)

Conforme abordado neste capítulo, existe uma série de vulnerabilidades na segurança de rede sem fio. Estas deficiências são, na melhor das hipóteses, apenas corrigidas parcialmente com o uso do WEP (*Wired Equivalent Privacy*).

A solução proposta para melhorar a segurança precisa ter os seguintes recursos:

- Autenticação robusta de clientes sem fio. Ela deverá incluir a autenticação mútua do cliente e do AP;
- Processo de autorização para determinar quem está e quem não está autorizado ao acesso à rede sem fio;
- Controle de acesso para permitir o acesso à rede para clientes autorizados, e negá–lo a clientes não autorizados;
- Criptografia de alta segurança do tráfego da rede sem fio; e
- Gerenciamento seguro das chaves de criptografia.

Com objetivo de melhorar os mecanismos de segurança, o IEEE criou um novo comitê denominado 802.1x, com a intenção de padronizar a segurança em portas de redes cabeadas. Essa padronização tornou-se também aplicável às redes sem fio.

O padrão IEEE 802.1x fornece um conjunto de autenticação muito mais robusto e, opcionalmente, permite gerenciar as chaves usadas para proteger o tráfego. Esta característica possibilitará um gerenciamento das chaves de criptografia para operação do WEP, possibilitando a transmissão segura dos dados na rede sem fio. Deve-se garantir que as chaves de sessão do cliente sejam atualizadas em intervalos de tempo inferiores ao tempo necessário para capturar o tráfego e executar operações de força bruta.

O padrão IEEE 802.1x implementa controle de aceso à rede com base em portas. Existem dois tipos de portas no 802.1X: não-controladas e controladas. Uma porta não-controlada permite que o dispositivo conectado a ela se comunique com qualquer outro dispositivo da rede. Uma porta controlada, por outro lado, limita os endereços da rede com os quais o dispositivo conectado pode se comunicar. Desta forma, o 802.1x permite que todos os clientes se conectem a portas controladas, mas estas portas somente transmitem o tráfego a servidores de

autenticação. Depois que o cliente tiver sido autenticado, será permitido que ele comece a usar a porta não controlada. A diferença do 802.1x é que portas não controladas e controladas são entidades lógicas que podem existir na mesma porta de rede física.

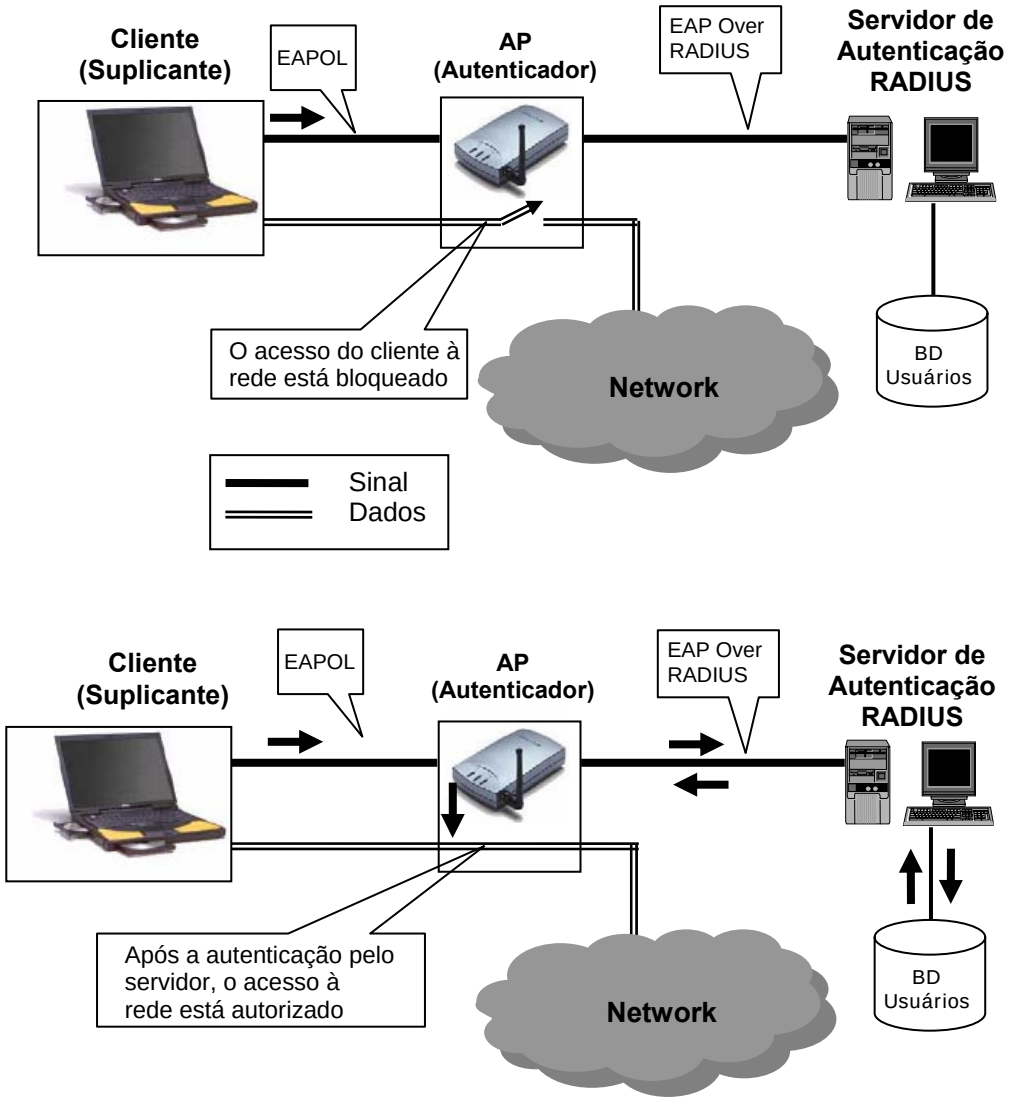


Figura 37: Configuração básica do padrão IEEE 802.1x

Com relação à autenticação, o 802.1x define, adicionalmente, duas funções para dispositivos de rede: suplicante e autenticador. O suplicante é um dispositivo (como um notebook com uma placa 802.11b) que solicita acesso a recursos da rede. O autenticador é um dispositivo que autentica os suplicantes e decide se concederá ou não acesso a eles.

Entidades envolvidas, quando usado com o Padrão IEEE 802.11:

a) ***Suplicante (Cliente)***: entidade (*notebook* ou *desktop* com uma placa 802.11b) que necessita ser autenticada. O cliente executa um aplicativo que requer acesso aos recursos da rede, e ainda possui a capacidade de criptografar seu tráfego de rede, e de armazenar e intercambiar com segurança as credenciais (como chaves ou senhas);

b) ***Autenticador (AP)***: entidade que disponibiliza o acesso aos usuários da rede. O AP 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;

c) ***Servidor de Autenticação (RADIUS)***: entidade que provê o serviço de autenticação ao autenticador. O serviço de autenticação provido determina, a partir das credenciais apresentadas pelo suplicante, as características do acesso obtido. A entidade Servidor pode ser combinada com o autenticador, ou pode ser acessada remotamente, através de rede que o autenticador acesse.

O padrão IEEE 802.1x considera um elemento autenticador no processo de autenticação. O AP passa a ser um repassador de pacotes de autenticação, já que toda a base é armazenada no autenticador. O autenticador pode ser definido no próprio AP, mas as atuais soluções de mercado têm optado pela implementação dessa funcionalidade em servidor especializado, como por exemplo o RADIUS (*Remote Authentication Dial-In User* Service).

3.5
Protocolo EAP - *Extensible Authentication Protocol*

O padrão IEEE 802.1x emprega o protocolo EAP (*Extensible Authentication Protocol*), definido pela RFC 2284, para permitir uma grande variedade de mecanismos de autenticação.

O EAP é um protocolo de autenticação genérico, tendo sido projetado para conexões discadas PPP, e sendo, posteriormente, adaptado para redes convencionais IEEE 802 e redes sem fio. O IEEE 802.1x não usa WEP para a autenticação. Em vez disso, ele usa o EAP.

O 802.1x depende de um Servidor RADIUS, de uma autenticação de rede e de um serviço de autorização para verificar as credenciais do cliente na rede. O 802.1x utiliza o EAP como meio de fazer o pacote de conversação da autenticação

entre diversos componentes da solução, e gerar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso da rede.

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

Os protocolos de autenticação mais comuns oferecidos pelas camadas superiores são o EAP-MD5, LEAP, PEAP, EAP-TLS e EAP-TTSL. Existem outros métodos menos utilizados: EAP-GTC (*Generic Token Card*), EAP-OTP (*One-Time Passwords*) e EAP-SIM (*Subscriber Identity Module*). O *access point* serve apenas como um meio para que as mensagens cheguem ao servidor de autenticação.

Mecanismo	EAP-TLS	EAP-TTLS	PEAP	LEAP	MD5
Autenticação Mútua	SIM	SIM	SIM	SIM	NÃO
Chave Dinâmica	Gerada durante a Autenticação	Gerada durante a Autenticação	Gerada durante a Autenticação	Gerada durante a Autenticação	Depende de Chave Estática
Nível de Tecnologia de Segurança	Autenticação por CERTIFICADO	Autenticação por LOGIN/SENHA	Autenticação por LOGIN/SENHA	Autenticação por LOGIN/SENHA	
Requer Certificado no Usuário	SIM	NÃO	NÃO	NÃO	NÃO
Proteção da Credencial do Usuário	Autenticação por CERTIFICADO	Protegido por Túnel TLS	Protegido Por Túnel TLS		Não há proteção
Suporta WPA	SIM	SIM	SIM	SIM	NÃO

Tabela 3: Comparativo dos métodos de autenticação EAP

Em resumo:

a) EAP – TLS: baseado em Certificados;

b) LEAP: baseado em senha de sessão;

c) EAP – TTLS: baseado em senha/certificado;

d) PEAP : baseado em senha/certificado.

O EAP possui 04 tipos de mensagens: EAP *Request*, EAP *Response*, EAP *Success* e EAP *Failure*.

O EAP é extensível à medida que permite que qualquer mecanismo de autenticação seja encapsulado dentro de mensagens EAP *Request/Response*. Os melhores tipos de EAP normalmente utilizam a criptografia para proteger a conversação de autenticação e podem gerar, dinamicamente, as chaves usadas para a criptografia durante o processo.

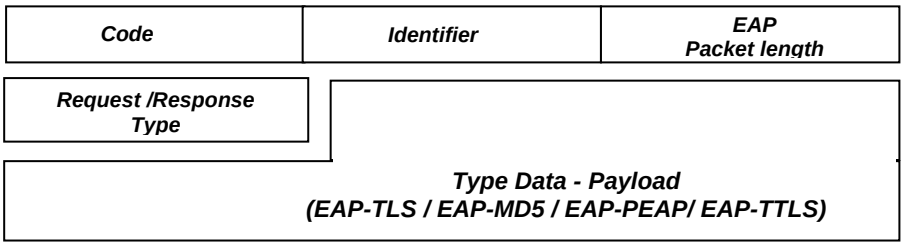


Figura 38: Formato do pacote EAP

A figura a seguir ilustra a pilha de Protocolos IEEE 802.1x/RADIUS sobre uma Rede IEEE 802.11

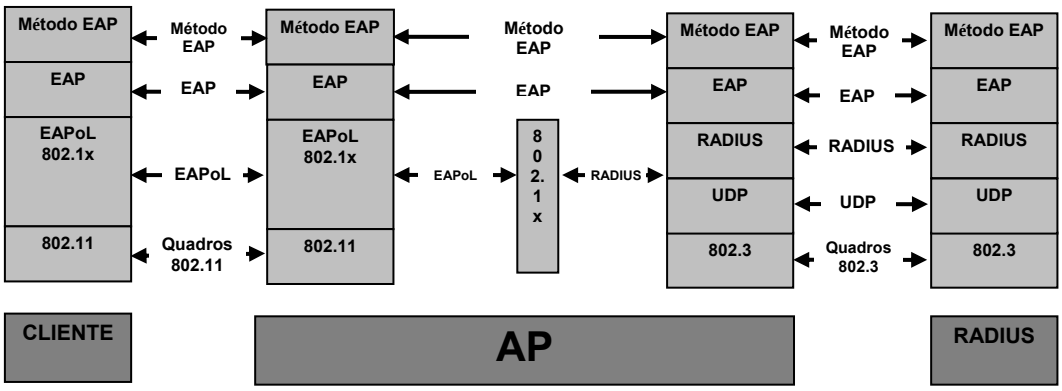


Figura 39: Pilha de protocolos IEEE 802.1x/RADIUS sobre uma rede IEEE 802.11

3.6
Servidor RADIUS

O RADIUS, definida pela RFC 2865, utiliza uma arquitetura cliente-servidor. Geralmente, o servidor RADIUS é usado por provedores de serviços de Internet (ISP — *Internet Service Providers*) para executar tarefas de AAA. As fases de AAA (*Authorization, Authentication, and Accounting*) são:

- ***Autenticação***: compara o nome do usuário e a senha com os existentes no banco de dados local. Depois que as credenciais são confirmadas, o processo de autorização é iniciado;
- ***Autorização***: determina se a solicitação de acesso ao recurso será aceita ou não;
- ***Contabilidade***: coleta informações sobre o uso do recurso para análise de tendências, auditoria, cobrança por tempo da sessão ou alocação de custos.

Esta nova arquitetura adiciona um novo elemento, o *Network Access Server* (NAS), ou servidor de acesso, que nas redes sem fio é desempenhado pelo próprio AP. A função do NAS é permitir a conexão remota via rede sem fio, gerenciar esses pedidos de conexão, e liberá-los, ou não.

O AP (NAS) é configurado para operar como um cliente RADIUS, nesse caso, cada pedido passa pelo AP, que repassa ao servidor RADIUS, e recebe um retorno do servidor e o encaminha à estação móvel.

O usuário solicita conexão ao AP. Quando a conexão é estabelecida, o AP solicita um nome de conta e a senha para efetuar a autenticação. Depois de receber o nome do usuário e a senha, o AP cria um pacote com essas informações. Como o AP faz o papel de cliente RADIUS, esse pacote é enviado para o servidor RADIUS criptografado. O servidor RADIUS recebe a requisição e valida o nome do usuário e a senha.

Se o nome e a senha conferirem, o RADIUS devolve ao AP uma autorização que inclui informações da rede do cliente e serviços os quais ele está autorizado a utilizar.

O RADIUS possui 06 tipos de mensagens: *Access Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request e Accounting-Response*.

O padrão IEEE 802.11x provê a autenticação e integridade por pacote entre o servidor RADIUS e o AP. Cada autenticador tem uma única chave secreta compartilhada com o servidor RADIUS. Todas as mensagens RADIUS contêm um campo de *Request Authenticator*, que é um HMAC-MD5 do pacote inteiro, utilizando a chave compartilhada como chave. Esse campo é configurado pelo Servidor e verificado pelo autenticador. O reverso é feito pelo atributo EAP *Message Authenticator.*

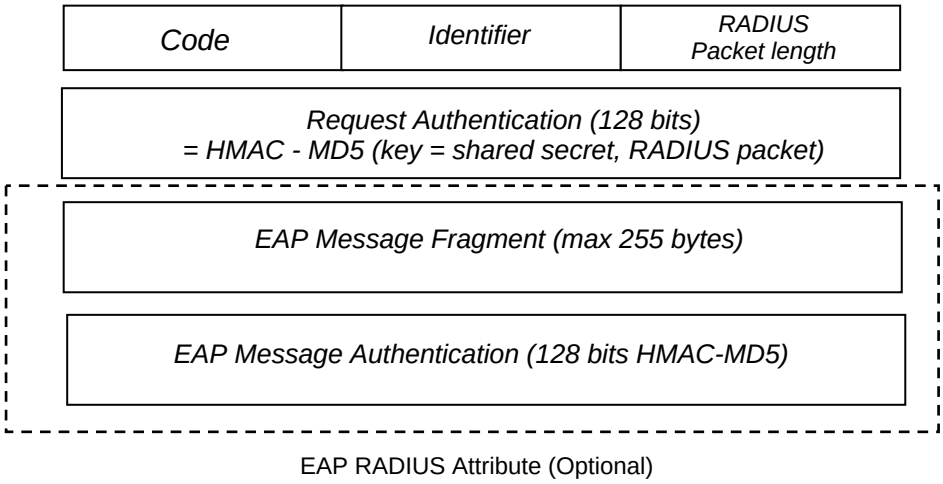


Figura 40: Formato do pacote RADIUS

3.6.1
Autenticação no Padrão IEEE 802.1x

O padrão IEEE 802.11x tem, como principais metas de segurança, o controle de acesso e a autenticação mútua.

As mensagens EAP são encapsuladas por si mesmas. O protocolo EAPoL (EAP *Over Lan*) leva os pacotes entre o suplicante e o autenticador.

O protocolo RADIUS contém mecanismos de autenticação e verificação de integridade por pacote, entre o ponto de acesso e o servidor RADIUS.

O fluxo de mensagens para autenticação tem a seguinte básica:

1. A estação tenta conectar-se ao AP pela porta não-controlada. Como a estação não foi autenticada ainda, ela não pode usar a porta controlada. O AP emite um desafio de texto sem formatação à estação;

2. A estação responde identificando-se;
3. O AP encaminha a mensagem de identidade da estação ao servidor RADIUS, pela LAN com fio;
4. O servidor RADIUS busca, no BD, a conta especificada para determinar que tipo de credencial é exigida. Essas informações são transformadas em uma solicitação de credencial e são retornadas à estação;
5. A estação envia suas credenciais pela porta não-controlada no AP;
6. O servidor RADIUS valida as credenciais. Se elas passarem, uma chave de autenticação é enviada ao AP. A chave é criptografada, de modo que apenas o AP possa descriptografá-la;
7. O AP descriptografa a chave e a usa para criar uma nova chave específica para aquela estação. Essa chave é enviada à estação, onde é usada para criptografar a chave de autenticação global mestre para a estação.

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

A figura a seguir ilustra a seqüência de troca de mensagens para autenticação entre a estação, o AP e o RADIUS.

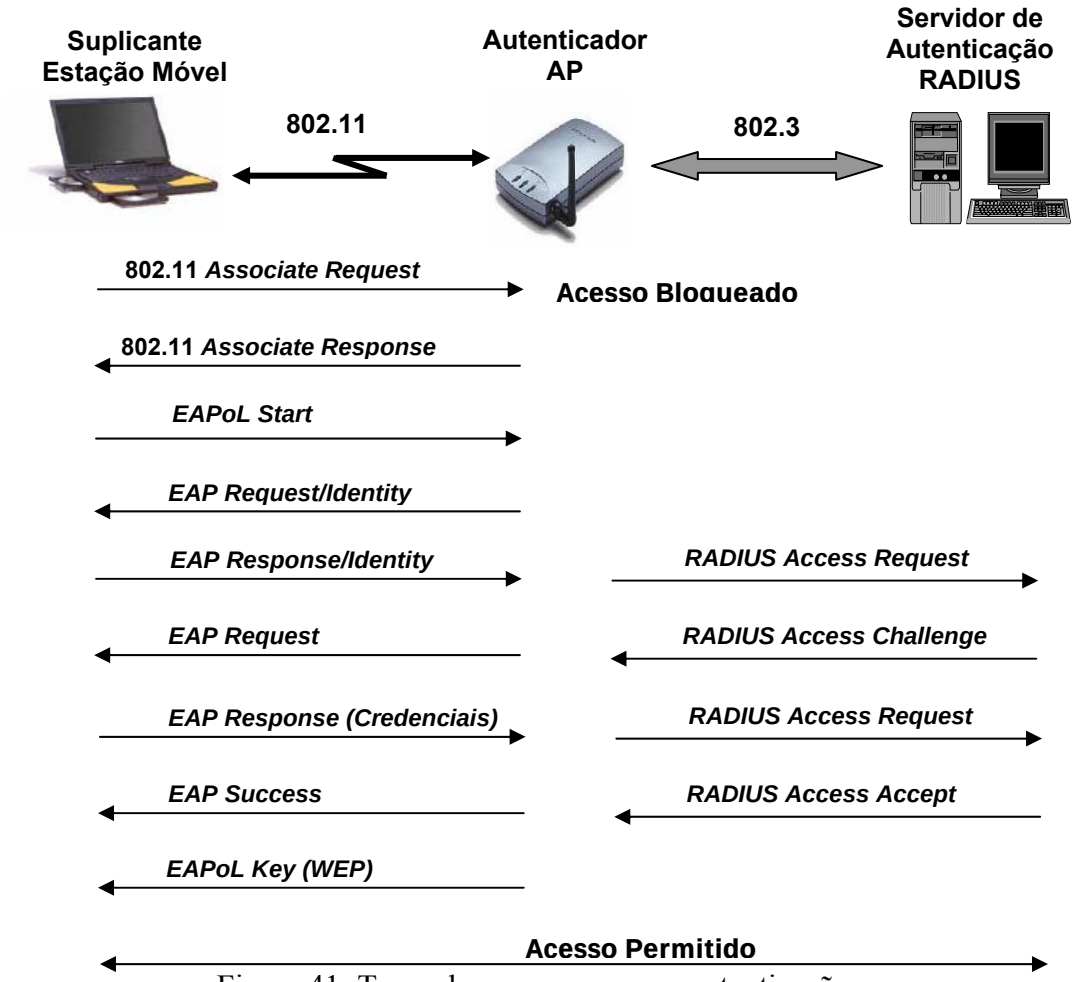


Figura 41: Troca de mensagens para autenticação

3.7
Protocolo TLS – *Transport Layer Security*

O protocolo TLS (RFC 2246), tem como objetivo principal oferecer privacidade e integridade dos dados em uma conexão, operando de forma transparente para as camadas superiores. Proporciona, assim, fácil portabilidade.

O protocolo TLS combina as criptografias simétrica e assimétrica para contornar o problema do segredo pré-estabelecido da simétrica, e o alto gasto computacional da assimétrica. Neste protocolo, a solução consiste em uma etapa inicial de negociação (*handshake*), na qual se utiliza a criptografia assimétrica para autenticar os nós, e combinar uma chave secreta para uso na criptografia simétrica. Terminada esta etapa, o algoritmo por chave pública garante que a negociação da chave secreta foi feita em um canal seguro, e que somente as duas partes a conhecem. Portanto, pode-se trabalhar durante todo o restante da conexão

utilizando-se os algoritmos de chave simétrica, tornando a transmissão computacionalmente viável.

A conexão baseada em protocolo TLS possui uma arquitetura do tipo cliente/servidor bem definida, já que a negociação delega papéis distintos às duas partes. O cliente é responsável por iniciar a conexão, e é ele quem propõe a configuração com a qual os nós trabalharão. Mesmo sendo o servidor quem determina os parâmetros que serão realmente utilizados, ele o faz baseado somente nos parâmetros propostos pelo cliente.

A seguir é apresentada a seqüência de comandos para estabelecimento de conexão segura:

1. Inicialmente, o Cliente envia *Client Hello* propondo o TLS. Nesta etapa, o Cliente informa uma lista com os algoritmos criptográficos e os métodos de compressão de dados suportados, um identificador de sessão e um valor aleatório para criação da chave criptográfica;
2. O servidor responde, com *Server Hello,* selecionando a opção TLS. Nesta etapa, o Servidor define e envia os parâmetros que realmente serão usados na conexão;
3. O Servidor envia mensagem *Server Key Exchange* com a sua chave pública;
4. O Servidor encerra sua parte com a mensagem *Server Hello Done,* e aguarda resposta do Cliente. Nesta etapa, o Cliente configura seus parâmetros de segurança e informa ao Servidor;
5. O Cliente envia mensagem *Client Key Exchange,* contendo sua chave de sessão (simétrica) encriptada com a chave pública do Servidor. Esta chave simétrica será utilizada durante toda a conexão;
6. O Cliente envia mensagem *Change Cipher Spec,* para ativar as opções negociadas às demais mensagens enviadas por ele;
7. O Cliente envia mensagem *Finished* de forma que o Servidor possa conferir as opções ativadas;
8. O Servidor envia mensagem *Change Cipher Spec,* para ativar as opções negociadas às demais mensagens enviadas por ele;

9. O Servidor envia mensagem *Finished* de forma que o cliente possa conferir as opções ativadas;

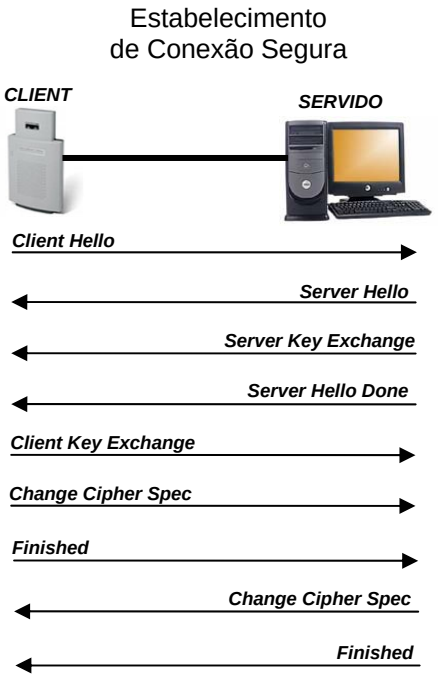


Figura 42: Mensagens trocadas entre cliente-servidor durante o *handashake*

A seguir é apresentada a seqüência de comandos, no *handshake,* para realização da autenticação do Servidor:

1. O Cliente envia *Client Hello* propondo o TLS;
2. O servidor responde, com *Server Hello,* selecionando a opção TLS;
3. O Servidor envia mensagem *Certificate,* seu Certificado de chave pública;
4. O Servidor encerra sua parte com a mensagem *Server Hello Done* e aguarda resposta do Cliente;
5. O Cliente envia mensagem *Client Key Exchange,* contendo sua chave de sessão (simétrica) encriptada, com a chave pública do Servidor. A chave pública do Servidor é enviada no Certificado;
6. O Cliente envia mensagem *Change Cipher Spec* para ativar as opções negociadas às demais mensagens enviadas por ele;

7. O Cliente envia mensagem *Finished* de forma que o Servidor possa conferir as opções ativadas;
8. O Servidor envia mensagem *Change Cipher Spec,* para ativar as opções negociadas às demais mensagens enviadas por ele;
9. O Servidor envia mensagem *Finished* de forma que o cliente possa conferir as opções ativadas;

A seguir é apresentada a seqüência de comandos no *handshake* para realização da autenticação do Cliente:

1. O Cliente envia *Client Hello* propondo o TLS;
2. O servidor responde com *Server Hello* selecionando a opção TLS;
3. O Servidor envia mensagem *Certificate,* seu Certificado de chave pública;
4. O Servidor envia mensagem *Certificate Request* solicitando que o Cliente envie seu Certificado;
5. O Servidor encerra sua parte com a mensagem *Server Hello Done,* e aguarda resposta do Cliente;
6. O Cliente envia mensagem *Certificate,* seu Certificado;
7. O Cliente envia mensagem *Client Key Exchange,* contendo sua chave de sessão (simétrica) encriptada com a chave pública do Servidor. A chave pública do Servidor é enviada no Certificado;
8. O Cliente envia mensagem *Certificate Verify,* encriptada com sua chave para conferência da chave pública enviada no Certificado. Nesta etapa, o Servidor irá confirmar se o Cliente possui a chave privada associada ao Certificado enviado. Para isso ele solicita a encriptação de uma mensagem com a chave privada, de tal forma que o Servidor desencripte com a chave pública por ele recebida;
9. O Cliente envia mensagem *Change Cipher Spec,* para ativar as opções negociadas às demais mensagens enviadas por ele;
10. O Cliente envia mensagem *Finished,* de forma que o Servidor possa conferir as opções ativadas;

11. O Servidor envia mensagem *Change Cipher Spec,* para ativar as opções negociadas às demais mensagens enviadas por ele;
12. O Servidor envia mensagem *Finished,* de forma que o cliente possa conferir as opções ativadas.

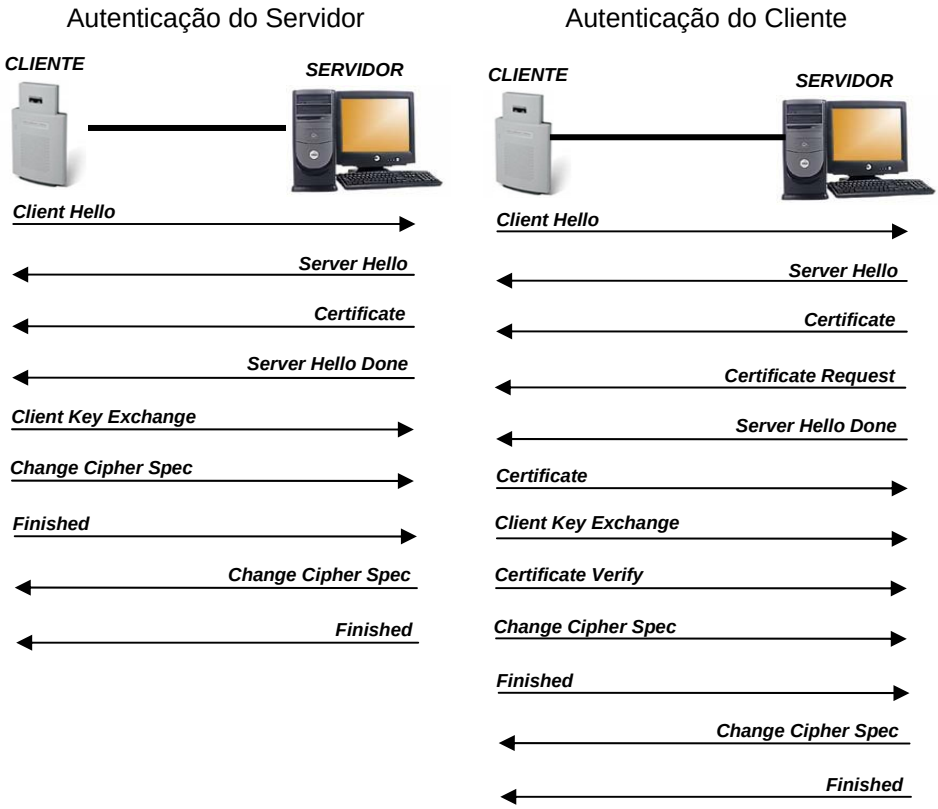


Figura 43: Seqüência de comandos no *handshake* para realizar a autenticação do servidor e do cliente

3.8
Protocolo EAP - TLS

O EAP–TLS (RFC 2716) usa o protocolo TLS de certificado para autenticar os clientes sem fio e o servidor RADIUS mutuamente, usando métodos de criptografia de alta segurança e gerando chaves de criptografia usadas para proteger o tráfego sem fio.

A geração dinâmica de chaves criptográficas resolve a vulnerabilidade do WEP quanto à confidencialidade dos dados. Assim, uma vez gerada a chave pelo protocolo TLS, os dados no enlace sem fio passam a ser criptografados pelo WEP.

O algoritmo de criptografia RC4 do WEP passa a ser seguro se a chave for alterada constantemente.

O método EAP-TLS requer certificados de chave pública do cliente e do servidor RADIUS. Os certificados digitais devem ser configurados, individualmente, em cada cliente da rede e no servidor de autenticação.

O EAP-TLS é um dos métodos mais seguros de EAP para usar com o 802.1x. Porém, sua potencialidade tem um alto custo no que se refere à necessidade da empresa/instituição, que implementá-lo, possuir Certificado (X.509) emitido por Autoridade Certificadora.

Uma infra-estrutura de chave pública é viável apenas para grandes empresas/instituições, que já possuem (ou planejam implementar) outros serviços e aplicações que utilizam certificados, tais como: acesso remoto, *logon* com cartão inteligente, criptografia de arquivos, e-mail seguro, etc.

O EAP-TLS é suportado pelo Windows. É necessária apenas a definição dos certificados.

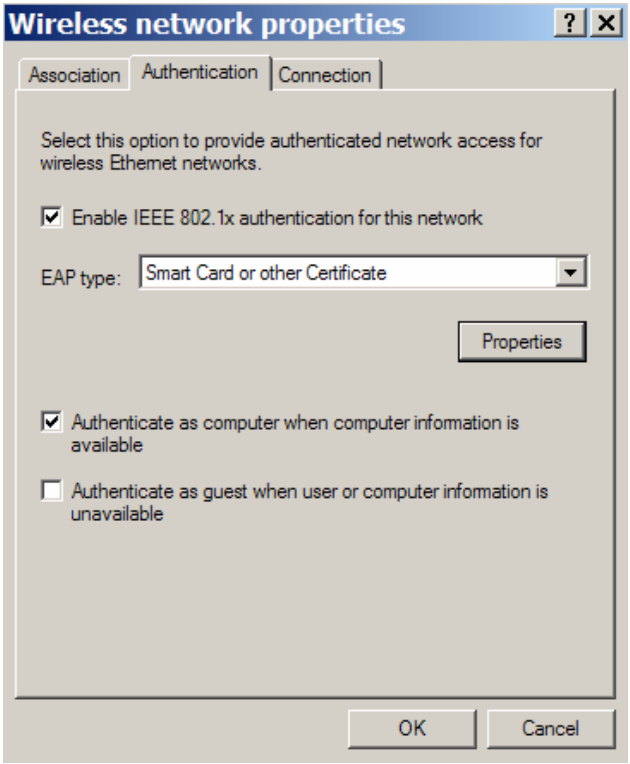


Figura 44: Configuração do Windows XP (EAP-TLS)

Características básicas do EAP-TLS:

a) Garante uma nova chave secreta a cada vez que a estação se associar ao AP;

b) Não há necessidade de *User Name* e *Password*;

c) Implementa autenticação mútua, o que proporciona um forte controle de acesso;

d) A autenticação EAP-TLS ocorre automaticamente, sem intervenção do usuário;

e) Utiliza criptografia assimétrica com PKI (*Public Key Infrastructure)*;

f) O AP e a estação deverão possuir certificado emitido por CA (Autoridade Certificadora);

g) A estação é forçada a se autenticar depois de um certo tempo, para renovar a chave secreta.

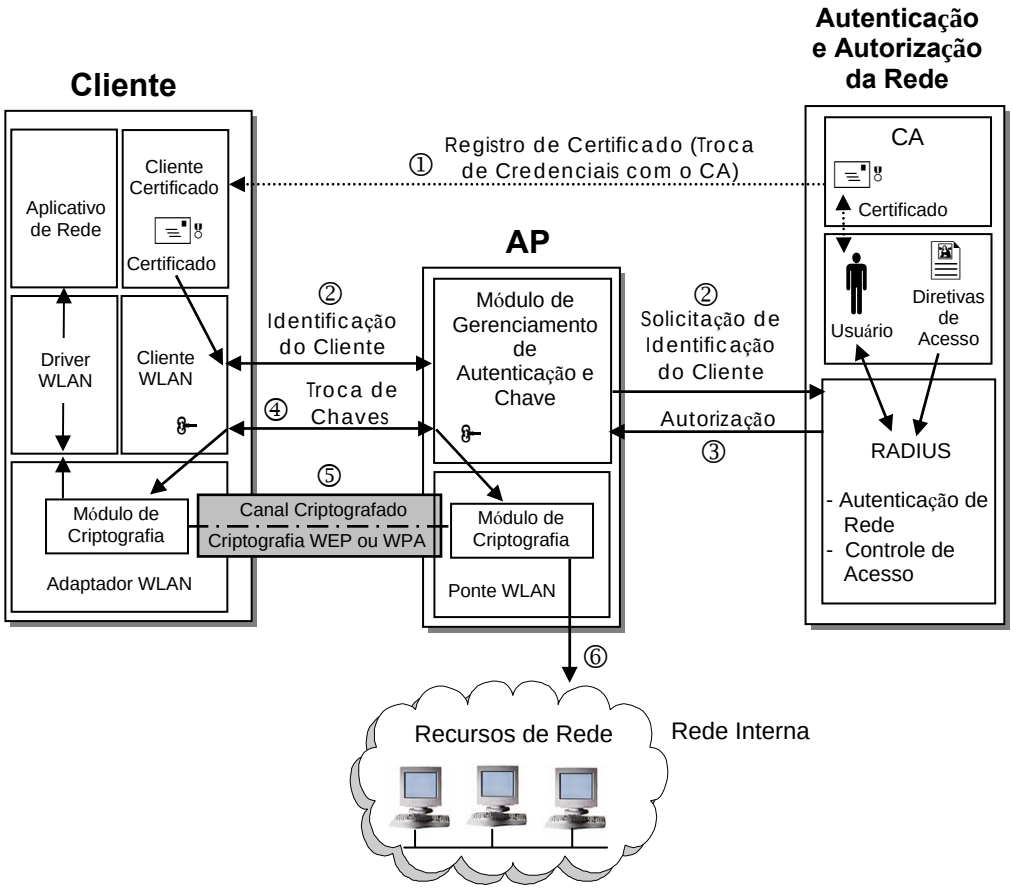


Figura 45: Conceito da solução baseada na autenticação EAP–TLS

Descrição das etapas:

1. O Cliente sem fio deve, em algum momento, estabelecer as credenciais com uma Autoridade Certificadora (CA) central antes do acesso à rede sem fio ser estabelecido. Este pode ser por um método fora de padrão. Por exemplo, por intermédio da troca de disquete, ou pode ocorrer em rede cabeada ou 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. O AP as repassa em seguida, ao Servidor RADIUS para solicitar autorização;
3. O Servidor RADIUS 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. O mesmo fará o intercâmbio das chaves de criptografia, em segurança, com o AP. As chaves são geradas pelo Servidor e transmitidas ao AP por um canal seguro. Se o cliente não foi autorizado pelo Servidor, o acesso é negado e nenhuma comunicação posterior ocorre;
5. Com o uso de chaves de criptografia, o Cliente e o AP estabelecem uma conexão segura com o enlace 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.

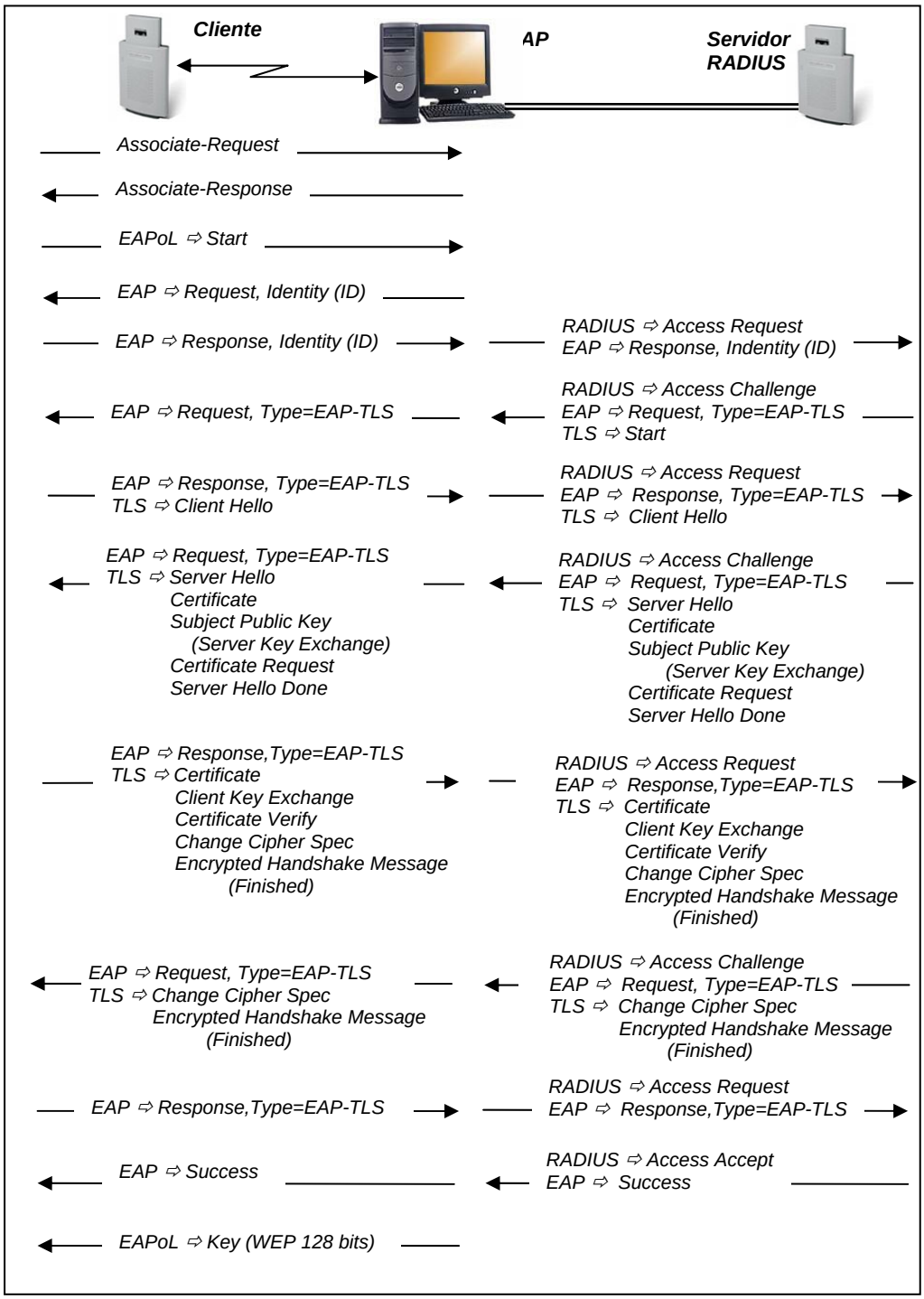


Figura 46: Seqüência de comandos do mecanismo EAP-TLS

3.9
Protocolo PEAP - *Protected Extensible Authentication Protocol*

O método PEAP está em processo de aceitação no IETF, não existindo ainda em forma de RFC. O PEAP oferece autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificado no cliente. O PEAP foi projetado para transportar os tipos de EAP dentro de um canal protegido pelo protocolo TLS.

O método PEAP permite a utilização de diversos tipos de protocolos para fazer a autenticação da senha, tais como: PAP, CHAP, MS-CHAP e MS-CHAPv2.

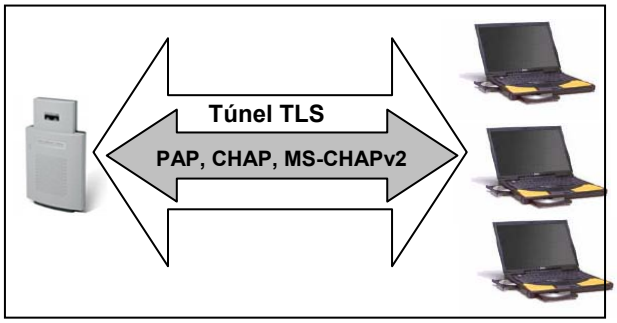


Figura 47: Esquema de autenticação PEAP (Túnel TLS)

O PEAP foi desenvolvido pela Microsoft, Cisco e RSA Security. O protocolo foi adotado pela Microsoft no Windows XP e Windows Server 2003.

Neste trabalho, os clientes foram configurados em plataforma Windows XP, que utiliza o método MS-CHAPv2 (*Microsoft Challenge Authentication Protocol versão 2*).

Pode-se dividir o processo do método PEAP em duas fases:

FASE 1: estabelecimento do túnel TLS.

FASE 2: estabelecimento da autenticação MS-CHAPv2 dentro do túnel TLS.

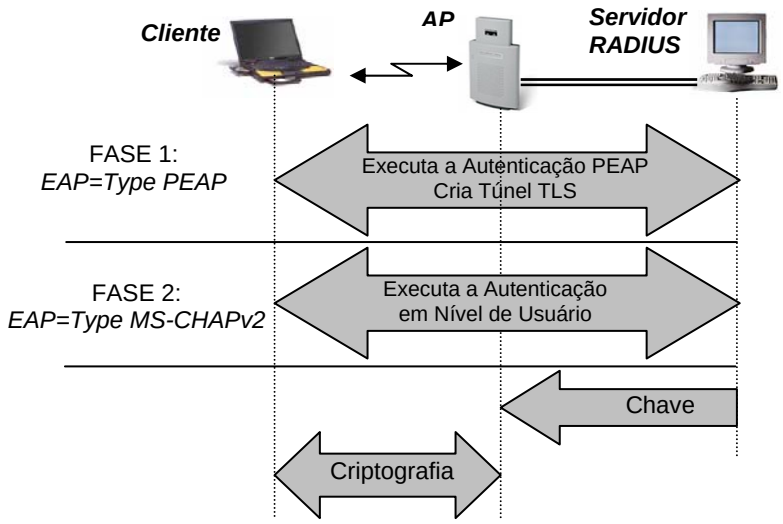


Figura 48: Esquema de autenticação PEAP

A autenticação por senha do 802.1X é uma boa solução para as pequenas/médias empresas que, atualmente, não têm uma infra–estrutura de certificado e não precisam de certificados para outras finalidades.

O fato de o PEAP ser suportado pelo Windows torna esta solução bastante vantajosa para as pequenas/médias empresas.

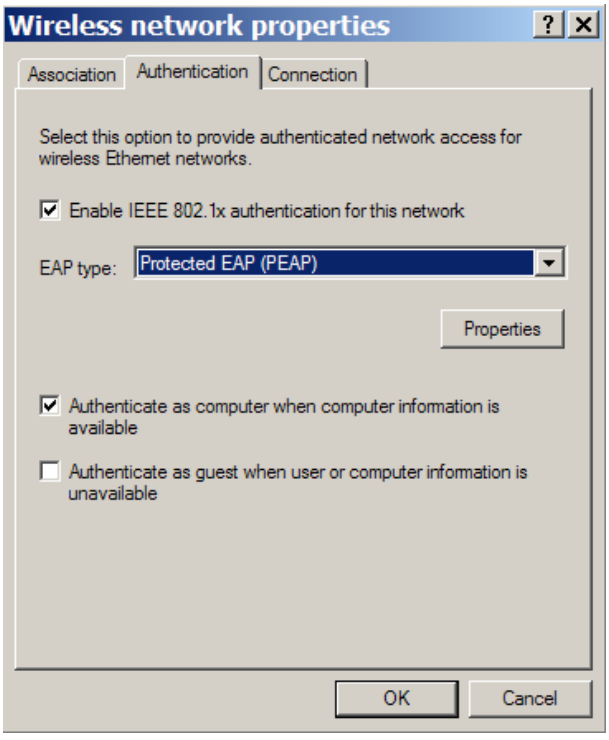


Figura 49: Configuração do Windows XP (PEAP)

Características básicas do PEAP:

a) Utilização de certificados para autenticar o servidor e credenciais baseadas em senha para autenticar o cliente;

b) O servidor deverá possuir certificado emitido por CA (Autoridade Certificadora);

c) Autenticação por senha. Há necessidade de *User Name* e *Password.* As credenciais do usuário são protegidas pelo túnel TLS;

d) Garante uma nova chave secreta a cada vez que a estação se associar ao AP;

e) Implementa autenticação mútua, o que proporciona um forte controle de acesso;

f) Utiliza criptografia assimétrica com PKI (*Public Key Infrastructure)*;

g) A estação é forçada a se autenticar depois de um certo tempo, para renovar a chave secreta.

O protocolo *MS-CHAP v2* utilizado neste trabalho é uma atualização do *MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol*), que oferece maior segurança durante o processo de autenticação. O servidor de autenticação envia um desafio contendo um identificador de sessão e uma cadeia de caracteres arbitrária. O cliente remoto responde com o nome de usuário, uma cadeia de caracteres arbitrária e uma encriptação do conjunto de: cadeia de caracteres recebida, cadeia de caracteres enviada, *ID* da sessão e senha do usuário. O servidor então checa a resposta do cliente e envia de volta um indicador de conexão, bem sucedida ou não, e uma resposta autenticada baseada na cadeia de caracteres enviada pelo cliente, a resposta encriptada do cliente e a senha do usuário. O cliente verifica a resposta e, se estiver correta, utiliza a conexão, caso contrário, termina. Dessa forma o *MS-CHAP v2* oferece uma mútua autenticação, onde o servidor verifica que o cliente sabe a senha de usuário e o cliente também sabe que o servidor conhece a senha.

As etapas a seguir descrevem como o cliente faz uma solicitação e recebe acesso à WLAN e, conseqüentemente, à rede interna.

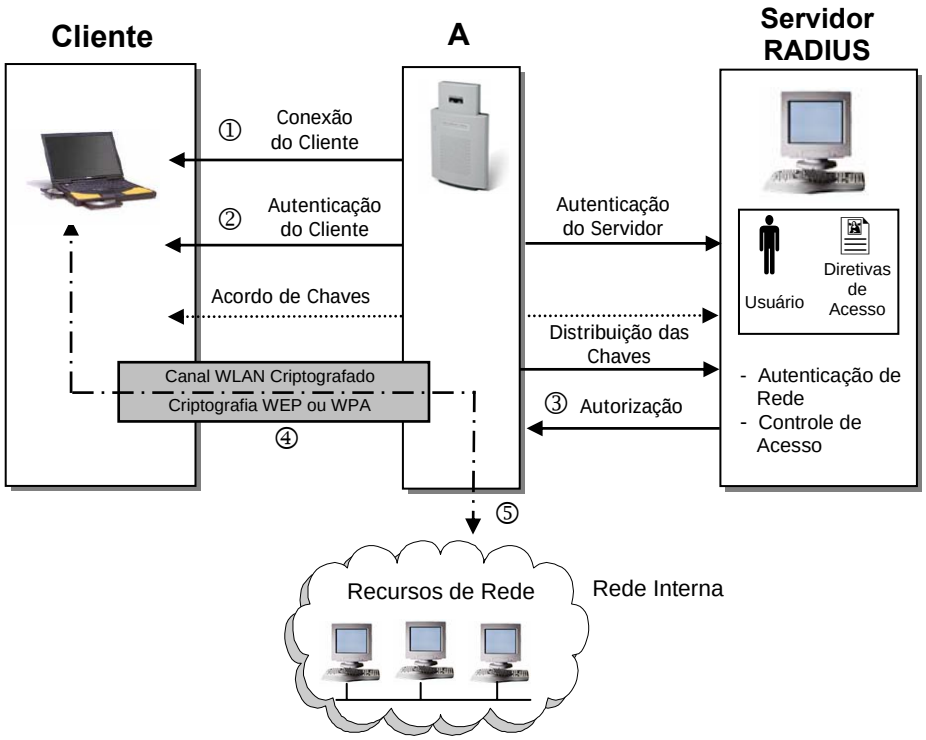
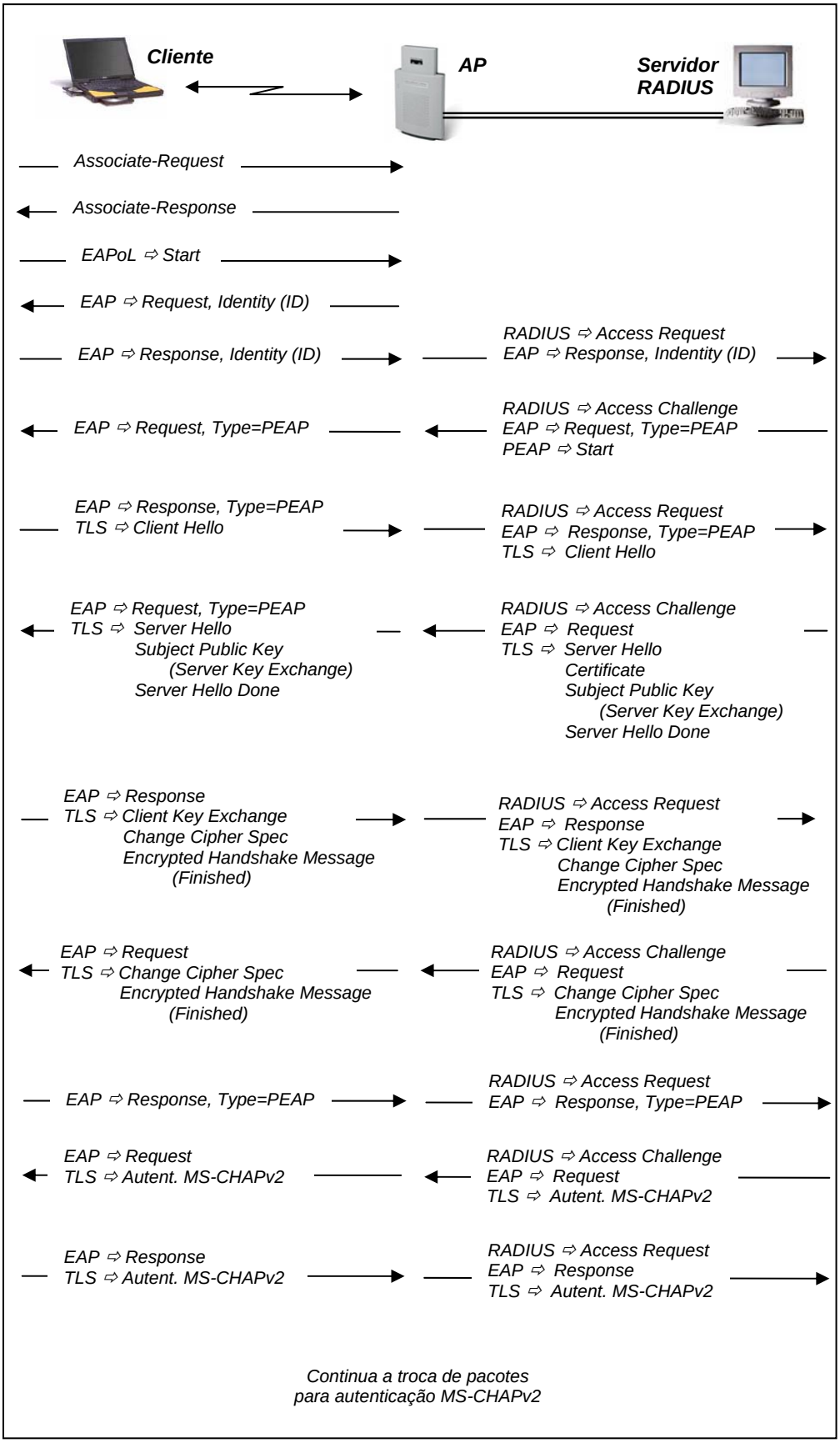


Figura 50: Conceito da solução baseada na autenticação PEAP

1. O Cliente solicita conexão ao AP;
2. O Cliente tenta se autenticar no servidor RADIUS usando 802.1x. Como parte da negociação PEAP, o Cliente estabelece uma sessão TLS com o servidor RADIUS. Protegido no canal PEAP, o Cliente se autentica no servidor RADIUS usando o protocolo MS-CHAPv2. Durante esse intercâmbio, o tráfego no túnel TLS é visível somente para o cliente e para o servidor RADIUS. Ele nunca é exposto ao AP. O uso da sessão TLS como parte do PEAP atende a uma série de objetivos:
   - ⇨ Permite que o cliente autentique o Servidor RADIUS, o que significa que o Cliente só estabelecerá a sessão com um servidor que tenha um certificado em que o cliente confie;
   - ⇨ Protege o protocolo de autenticação MS-CHAP v2 contra escuta de pacotes;
   - ⇨ A negociação da sessão TLS gera uma chave que será usada pelo Cliente e pelo Servidor RADIUS para estabelecerem chaves mestras comuns. Essas chaves são

usadas a fim de gerar chaves de criptografia do tráfego da WLAN;

3. O servidor RADIUS verifica as credenciais do cliente no diretório. Se o cliente for autenticado com êxito, o servidor RADIUS montará as informações que permitirão decidir se autoriza o cliente a usar a WLAN. O RADIUS retransmite a decisão de acesso ao AP. Se o acesso for concedido ao cliente, o servidor RADIUS transmitirá a chave mestra do Cliente para o AP. Então, o Cliente e o AP compartilharão as informações de chaves que poderão usar para criptografar e descriptografar o tráfego da WLAN entre eles;
4. Em seguida, o AP liga a conexão WLAN do cliente à LAN interna, permitindo que o cliente se comunique livremente com sistemas da rede interna. O tráfego enviado entre o cliente e o AP é criptografado;



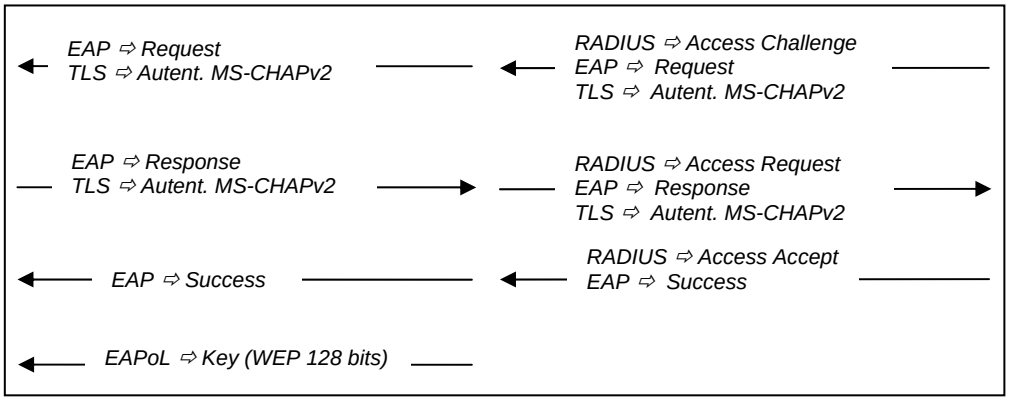


Figura 51: Seqüência de comandos do mecanismo PEAP

3.10
Protocolo EAP-TTLS - *Tunnuled Transport Layer Security*

O método EAP-TTLS também está em processo de aceitação no IETF (*Funk Software e Certicom*), não existindo ainda em forma de RFC.

O EAP-TTLS foi projetado para transportar os tipos de EAP dentro de um canal protegido pelo protocolo TLS e requer um certificado baseado em servidor.

O método EAP-TTLS permite a utilização de diversos tipos de métodos de autenticação, tais como: EAP-MD5, PAP, CHAP, MS-CHAP e MS-CHAPv2. Neste trabalho, foi utilizado o método EAP-MD5 para autenticação da senha.

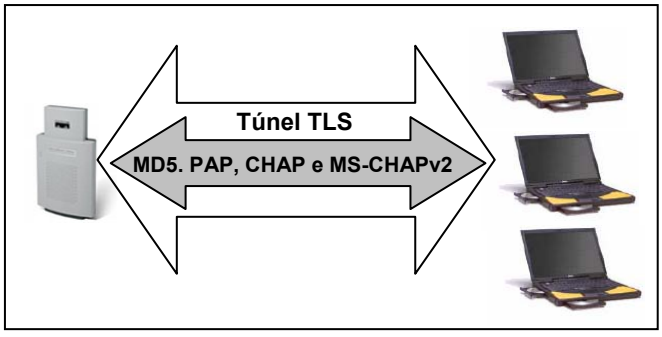


Figura 52: Esquema de Autenticação EAP-TTLS (Túnel TLS)

O mecanismo EAP-TTLS também é uma boa solução para as pequenas/médias empresas que, atualmente, não têm uma infra–estrutura de certificado, e não precisam de certificados para outras finalidades.

A operação do EAP-TTLS é similar à do PEAP.

A diferença é que pelo fato do EAP-TTLS não ser suportado pelo Windows, há necessidade de instalação de um Cliente de Autenticação.

Clientes de Autenticação disponíveis:

a) *SECURE W2 Client (open source)*

b) *Meetinghouse AEGIS Client*

c) *Funk Odyssey*

Neste trabalho, foi utilizado Cliente *SecureW2*.

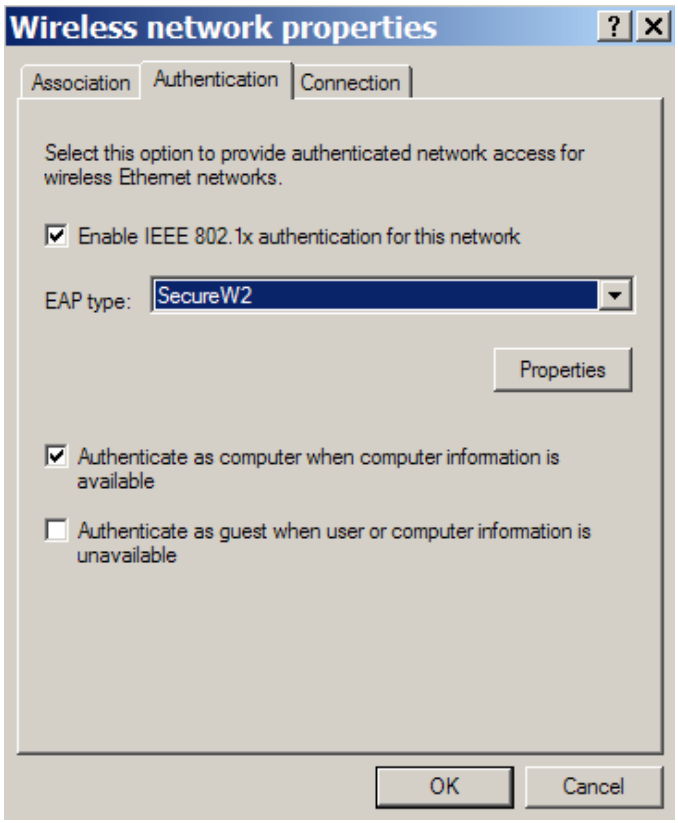


Figura 53: Configuração do Windows XP (EAP-TTLS)

Características básicas do EAP-TTLS:

a) Utilização de certificados para autenticar o servidor e credenciais baseadas em senha para autenticar o cliente;

b) O servidor deverá possuir certificado emitido por CA (Autoridade Certificadora);

c) Autenticação por senha. Há necessidade de *User Name* e *Password.* As credenciais do usuário são protegidas pelo túnel TLS;

d) Garante uma nova chave secreta a cada vez que a estação se associar ao AP;

e) Implementa autenticação mútua, o que proporciona um forte controle de acesso;

f) Utiliza criptografia assimétrica com PKI (*Public Key Infrastructure)*;

g) A estação é forçada a se autenticar depois de um certo tempo, para renovar a chave secreta.

3.11
Protocolo LEAP - *Lightweight Extensible Authentication Protocol*

O LEAP foi desenvolvido pela *Cisco Systems,* foi um dos primeiros protocolos de autenticação disponível para redes sem fio e é baseado em senha de sessão.

Características básicas do LEAP:

a) Autenticação de usuário por senha. Há necessidade de *User Name* e *Password;*

b) Garante uma nova chave secreta a cada vez que a estação se associar ao AP;

c) Implementa autenticação mútua.