Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Andre Washington Garcia Suarez

CRIPTOGRAFIA EM REDES WIRELESS:
Um Estudo sobre os Métodos de Segurança e Tipos de Criptografias Usados em Redes sem Fio

Rio de Janeiro

2010

Andre Washington Garcia Suarez

CRIPTOGRAFIA EM REDES WIRELESS:
Um Estudo sobre os Métodos de Segurança e Tipos de Criptografias Usados em Redes sem Fio

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:
Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

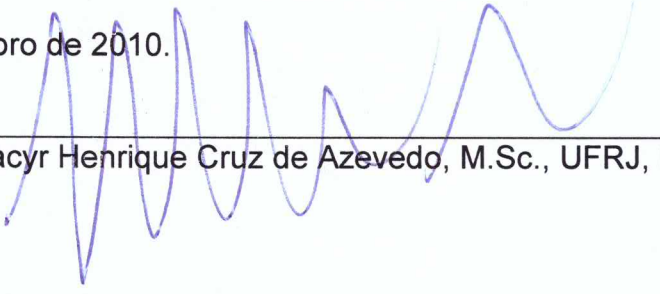
2010

Andre Washington Garcia Suarez

CRIPTOGRAFIA EM REDES WIRELESS: Um Estudo sobre os Métodos de Segurança e Tipos de Criptografias Usados em Redes sem Fio

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Setembro de 2010.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

AGRADECIMENTOS

Gostaria de agradecer a Deus por permitir tudo o que acontece comigo e ao meu redor, aos meus pais Iolanda e Edmundo por nunca terem medido esforços para que eu consiga os meus objetivos, a minha esposa Jaqueline e a minha filha Thayná, que com amor e incentivo, me deram forças para chegar até aqui, aos professores do MOT, que tão bem souberam transmitir seus conhecimentos e ao meu orientador Moacyr Henrique Cruz de Azevedo pela demonstração de incentivo, persistência e paciência.
Obrigado.

RESUMO

SUAREZ, Andre Washington Garcia. **CRIPTOGRAFIA EM REDES WIRELESS - Um Estudo sobre os Métodos de Segurança e Tipos de Criptografias Usados em Redes sem Fio.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Os métodos de transporte físico utilizados na comunicação sem fio diferem da comunicação com fio. Essas diferenças afetam o modo como um canal seguro pode ser estabelecido em um ambiente wireless. O propósito deste estudo é fornecer uma visão geral de como um canal seguro pode ser configurado em um ambiente sem fio que usa o 802.11, mostrando os métodos de criptografia e técnicas que podem ser empregadas neste ambiente.

ABSTRACT

SUAREZ, Andre Washington Garcia. **CRIPTOGRAFIA EM REDES WIRELESS - Um Estudo sobre os Métodos de Segurança e Tipos de Criptografias Usados em Redes sem Fio.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Methods of physical transportation used in wireless communication are different from the ones with wire. These differences affect how a secure channel can be established in a wireless environment. The purpose of this study is to provide an overview of how a secure channel can be configured in a wireless environment that uses the 802.11 standard, showing the encryption methods and techniques that can be employed in this environment.

LISTA DE SIGLAS

WLAN	Wireless Local Area Network
PDA	Personal Digital Assistant
LAN	Local Area Network
AP	Access Point
BSS	Basic Service Set
WNIC	Wireless network interface card
ESS	Extended Service Set
RF	Radio Frequencia
IR	Infra Red
FHHS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
ISM	Industrial, Scientífic and Medical
DCF	Distributed Coordination Function
PCF	Point Coordination Function
MAC	Media Access Control
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access With Collision Detection
DIFS	Distributed Interframe Space
RTS	Request to Send
SIFS	Short Interframe Space
CTS	Clear to Send
NAV	Network Allocation Vector
WAPs	Wireless Access Points
IEEE	Institute of Electrical and Electronics Engineers
PAN	Personal Area Network
CIA	Confidentiality, integrity, availability
SSID	Service Set Identifier
GPS	Sistema de Posicionamento Global
TCP	Transmission Control Protocol
WEP	Wired Equivalent Privacy
AES	Advanced Encryption Standard
IV	Vetor de Inicialização
3DES	Triplo Data Encryption Standard
CRC	Verificação de Redundância Cíclica
IP	Internet Protocol
ARP	Address Resolution Protocol
VPN	Virtual Private Network
IPsec	Internet Protocol Security
DHCP	Dynamic Host Configuration Protocol
RSA	Agoritmo de Criptografia de Dados
XOR	Exclusive or
ANSI	American National Standards Institute
FDDI	Fiber Distributed Data Interface
EAPOL	Extensive Authentication Protocol over Local Area Network
RADIUS	Remote Authentication Dial-In User Service
AAA	Authentication Authorization Accounting
MS-AD	Microsoft Active Directory
NDS	Novell Network Directory System

LDAP	Lightweight Directory Access Protocol
RFC	Request for Comments
EAP	Extensible Authentication Protocol
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
PPP	Point-to-Point Protocol
IETF	Internet Engineering Task Force
EAP-MD5	Extensible Authentication Protocol-Message Digest version 5
LEAP	Lightweight Extensible Authentication Protocol
NDA	Non-disclosure Agreement
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
SSL	Secure Socket Layer
PCT	Microsoft Private Communications Technology
CA	Autoridade de Certificação
EAP-TTLS	Extensible Authentication Protocol-Tunnel Transport Layer Security
MS-CHAP	Microsoft Challenge-handshake authentication protocol
PKI	Public Key Infrastructure
PEAP	Protected Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
Wi-Fi	Wireless Fidelity
PAC	Protected Access Credential
WPA	Wi-Fi Protected Access
GMK	Chave Mestre de Grupo
PTK	Par de Chaves Transitório
QoS	Quality of Service
TKIP	Temporal Key Integrity Protocol
SOHO	Small Office/Home Office
RSN	Robust Secure Network
CCMP	Counter Mode com CBC-MAC Protocol
RNSA	Robust Secure Network Association
RSN IE	Elemento de Informação RSN
TSN	Transition Secure Network
TSC	Contador Sequencial TKIP
SA	Source Address
DA	Destiny Address
Ttak	Transmissão Mista de Endereço e Chave
MIC	Message Integrity Check
FCS	Soma de verificação de quadro
MAC	Message Authentication Code
CBC-MAC	Cipher Block Chaining Message Authentication
CCM	CTR/CBC-MAC
KCK	Key confirmation key
KEK	Key encryption key
WAPI	Wlan Authentication and Privacy Infrastructure

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Redes sem fio e redes móveis estão rapidamente estendendo as suas capacidades. Além de aumentar a sua largura de banda, e devido à sua flexibilidade e liberdade, estas tendem a tornar-se a infra-estrutura de comunicação escolhida. A comunicação sem fio oferece ao usuário a capacidade de conduzir negócios a qualquer momento, com poucos recursos, de qualquer lugar, usando um canal de comunicação móvel. Este canal de comunicação móvel pode também ser usado como um meio de acesso à Internet.

Como a comunicação sem fio e a Internet se tornaram verdadeiramente interoperáveis, os usuários vão querer que esse canal de comunicação esteja seguro e disponível quando necessário. Para que uma mensagem seja enviada usando este canal de comunicação, o usuário espera ter a garantia de:

- autenticação (o remetente e o destinatário são quem dizem ser);
- confidencialidade (a mensagem não pode ser compreendida senão pelo receptor);
- integridade (a mensagem não foi alterada).

O objetivo deste estudo é fornecer uma visão geral do que é necessário para proporcionar um canal de comunicação seguro em um ambiente wireless. O foco é sobre técnicas de segurança e criptografias disponíveis para o Wireless Local Area Network (WLAN) e para dispositivos sem fio (por exemplo, telefones celulares e PDA's) utilizados para acessar a Internet.

2 PADRÃO 802.11

WLANs são mais adequadas para usuários domésticos, pequenas redes, ou redes com requisitos de segurança baixo.

Com a implantação de redes sem fio em ambientes empresariais, as organizações estão trabalhando para implementar mecanismos de segurança que são equivalentes aos de LANs com fios. Um componente adicional do requisito de segurança é a necessidade de restringir o acesso à rede sem fio apenas para os usuários válidos. O acesso físico à rede sem fios é diferente do que o acesso a uma LAN com fio. Uma rede cabeada existente tem pontos de acesso, que normalmente precisam usar conectores RJ45, localizada no interior de edifícios que podem ser protegidos contra o acesso não autorizado através da utilização de dispositivos como chaves e/ou crachás. Um usuário deve ter acesso físico ao edifício para conectar um computador cliente em uma tomada de rede. Um ponto de acesso sem fios (AP) pode ser acessado de fora da empresa, se o sinal for detectado.

Assim, as redes sem fio precisam de acesso seguro para o AP de uma maneira diferente de LANs com fio. Em particular, é necessário isolar o AP da rede interna até que a autenticação seja verificada. O dispositivo que tentar se conectar ao AP deve ser autenticado. Uma vez que o dispositivo é autenticado, o usuário do dispositivo pode ser autenticado. Neste ponto, o usuário pode desejar ter um canal seguro de comunicação.

O padrão 802.11 fornece os meios para satisfazer esses requisitos de segurança - de validação do dispositivo de acesso, autenticação de usuário e um canal seguro. Para apreciar plenamente a forma como estes requisitos são cumpridos será visto um panorama do transporte físico wireless.

2.1 ARQUITETURA WLAN

Uma arquitetura WLAN é construída a partir de estações e de um ponto de acesso (*Access Point* – AP). A estrutura básica de um WLAN é o *Basic Service Set* (BSS). A BSS podem ser um BSS independente ou uma infra-estrutura BSS.

Em um BSS independente as estações se comunicam entre si diretamente, se eles estão dentro do alcance um do outro. Estes são muitas vezes referidas como redes *ad hoc* e geralmente duram pouco tempo. Estes WLANs *ad hoc* são normalmente utilizadas para reuniões e permitem aos participantes compartilhar dados entre si. Para participar de um WLAN *ad hoc*, os participantes devem colocar o cartão de interface de rede sem fio (WNIC) de seus dispositivos em *ad-hoc*. Este modo permite que uma estação estabeleça uma conexão com qualquer outra estação de sua proximidade.

Uma infra-estrutura BSS requer o uso de um AP. O AP é usado para todas as comunicações entre as estações. Se uma estação deseja enviar uma transmissão para outra, a estação emissora envia a sua transmissão para o AP, e o AP repassa essa transmissão para a estação receptora. Esta transmissão requer dois saltos que irão retardar a WLAN. No entanto, a distância percorrida pela WLAN é aumentada usando o AP como um dispositivo de *relay*. Uma característica importante da infra-estrutura BSS é a necessidade de estações se associarem a um AP. Este recurso pode ser usado para configurar uma WLAN que tem uma forma de acesso restrito. A figura 2.1-1 ilustra esses conceitos.

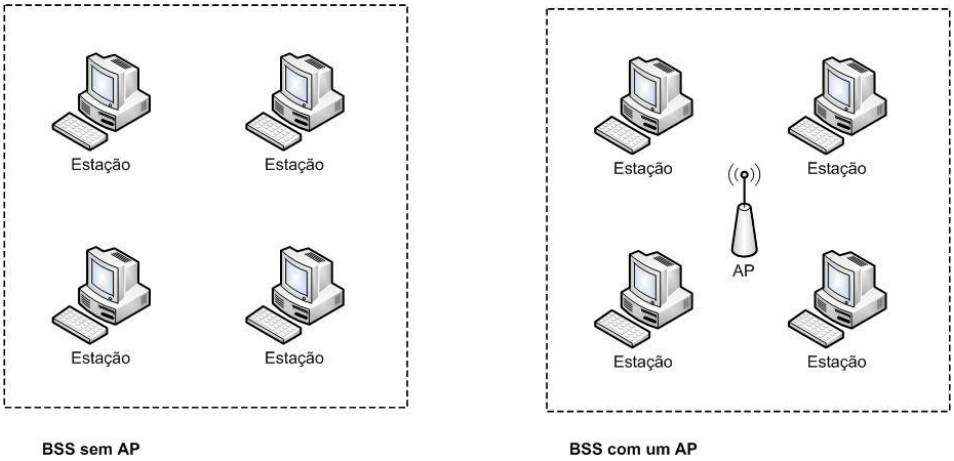


Figura 2.1-1 – Basic Service Sets com e sem um AP

Estes BSSs podem ser combinados para formar um *Extended Service Set* (ESS). O ESS é criado encadeando uma série de BSSs usando uma rede backbone. A finalidade de um ESS é permitir que uma estação tenha mobilidade de transição. Se uma estação tem a mobilidade de transição, o usuário é capaz de andar de BSS em BSS e continuar a estar associado a um BSS e também ter acesso ao backbone da rede, sem perda de conectividade. A figura 2.1-2 ilustra esta idéia.

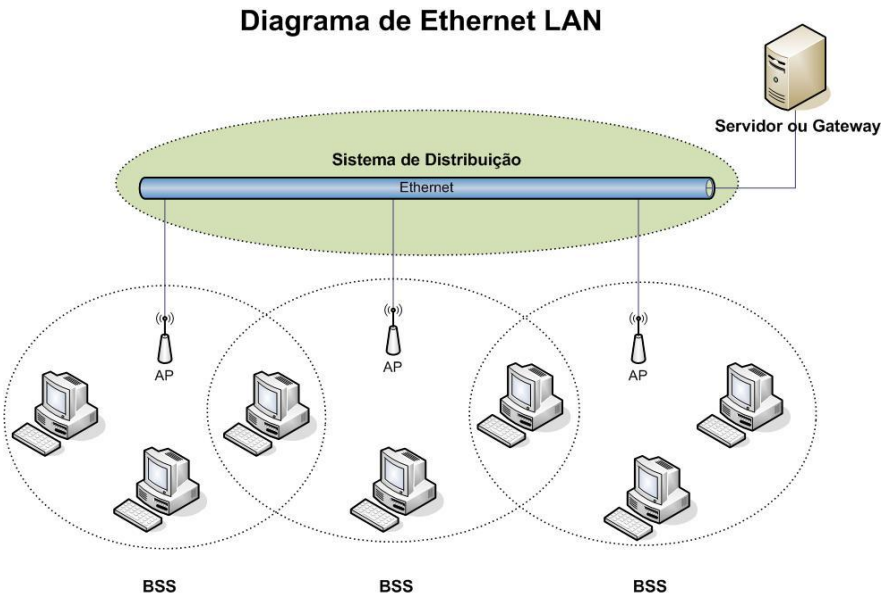


Figura 2.1-2 – Extended Service Set – ESS

2.2 TRANSPORTE NA CAMADA FÍSICA WIRELESS

O sinal sem fio que transporta os dados pode ser transmitido através de ondas eletromagnéticas ou por rádio frequência (RF) ou por frequência infravermelho (IR), parte do espectro de ondas eletromagnéticas.

Se for utilizado transporte RF então o método *Spread Spectrum* é empregado para gerar o sinal. O método de espalhamento espectral expande a largura de banda inicial e "espalha" para usar uma porção da largura de banda expandida para a parte da mensagem. Duas variações comuns da técnica de espalhamento espectral são a *Frequency Hopping Spread Spectrum* (FHHS) e a *Direct Sequence Spread Spectrum* (DSSS).

Quando a variação do *spread espectrum* FHSS é utilizado, as parcelas não consecutivas do espectro de propagação são usados para transmitir parcelas consecutivas da mensagem. A mensagem transmitida será recebida fora de ordem, a menos que o receptor saiba qual a parte da frequência de propagação para sintonizar e quanto tempo ouvir antes de entrar para a frequência por um período de tempo específico. Uma analogia seria ouvir uma canção no rádio, onde as parcelas consecutivas da canção são transmitidos sequencialmente, mas em estações diferentes. Para ouvir a música corretamente o ouvinte terá de sintonizar as estações na sequência correta. O objetivo da utilização FHSS é a segurança e também reduzir a interferência de sinal.

Quando o método DSSS é utilizado, cada parte da mensagem contém bits adicionais para fins de correção de erros - os bits de mensagem, juntamente com seus bits redundantes são chamado de *Chip Code*. Por causa dos bits de correção de erro, DSSS reduz a necessidade de retransmissão de um sinal e o resultado será uma utilização mais eficiente da largura de banda.

Se o transporte IR é usado, então o sinal pode ser gerado ou como um sinal difundido ou como um sinal ponto-a-ponto.

Um sinal difundido pode ser refletido nas superfícies existentes, tais como um limite, e o sinal pode ser recebido por qualquer dispositivo no intervalo. Um sinal ponto-a-ponto é enviado como feixe de IR Switch onde IR Switch retransmite o sinal para a próxima IR Switch e assim por diante.

RF é o mais comumente usado de dois modos de transporte físico. Em particular, o padrão 802.11 utiliza a banda RF *Industrial, Scientific and Medical* (ISM) do espectro eletromagnético. Esta banda ISM é especificada como:

• I-Band de 902 MHz a 928 MHz,
• S-Band de 2.4GHz a 2.48GHz, e
• M-Band de 5.725GHz a 5.85GHz.

Estas bandas são regulamentadas, uma vez que são utilizados equipamentos com baixa potência. No entanto, como operam em baixa potência, limitam a distância em que esses sinais podem ser detectados. Por exemplo, dependendo das circunstâncias, usando-se S-band com uma largura de banda de 1 Mbps a distância pode variar de 300 metros em transmissões interiores até 1500 metros ao ar livre.

2.3 SUBCAMADA MAC

O padrão 802.11 estabelece duas subcamadas MAC: ***Distributed Coordination Function* (DCF)** e ***Point Coordination Function* (PCF)**, como mostrado na Figura 2.3-1.

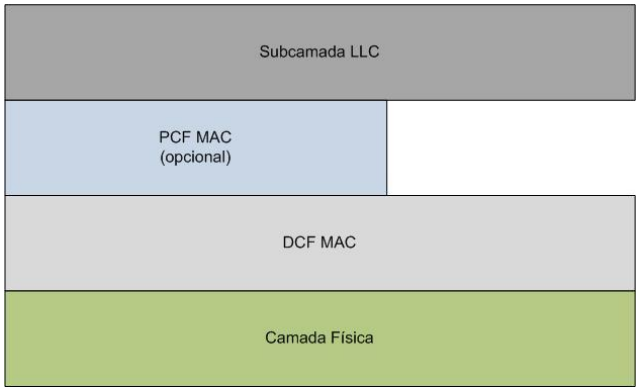


Figura 2.3-1 – Camadas MAC no padrão IEEE 802.11

A subcamada PCF é um método complexo e opcional que pode ser implementado na configuração de infra-estrutura (a rede *ad-hoc* não admite PCF). A subcamada DCF utiliza um método similar ao CSMA/CA, com algumas características de controle adicionais. Neste estudo analisaremos somente o método de acesso.

2.3.1 CSMA/CA

As LANs sem fio não podem implementar o CSMA/CD por três motivos:

1. Detecção de colisão implica que a estação deve ser capaz de enviar dados e receber sinais de colisão ao mesmo tempo. Isto implica no aumento do custo das estações e aumento dos requerimentos de banda.
2. Uma colisão pode não ser detectada devido a algum tipo de problema relacionado ao fato do dispositivo estar “escondido”. Uma estação pode se apresentar escondida de outra num ambiente *wireless* (devido aos obstáculos naturais, tais como montanhas, ou artificiais, como construções). Por exemplo, suponha que as estações A e B tenham dados para transmitir à estação C. Suponha ainda que a estação B não seja “vista” pela estação A, tal que se ocorrer colisão próximo a estação B, a estação A não tomará conhecimento. Este tipo de situação não ocorre numa LAN cabeada porque todas as estações estão conectadas através de cabos, assim todas as estações são ouvidas pelas demais.
3. A distância entre estações numa LAN sem fio pode ser muito grande. Um sinal desvainecido pode impedir uma estação numa extremidade de ouvir a colisão gerada na outra extremidade.

Fluxo do processo CSMA/CA: A Figura 2.3-2 indica um fluxograma CSMA/CA.

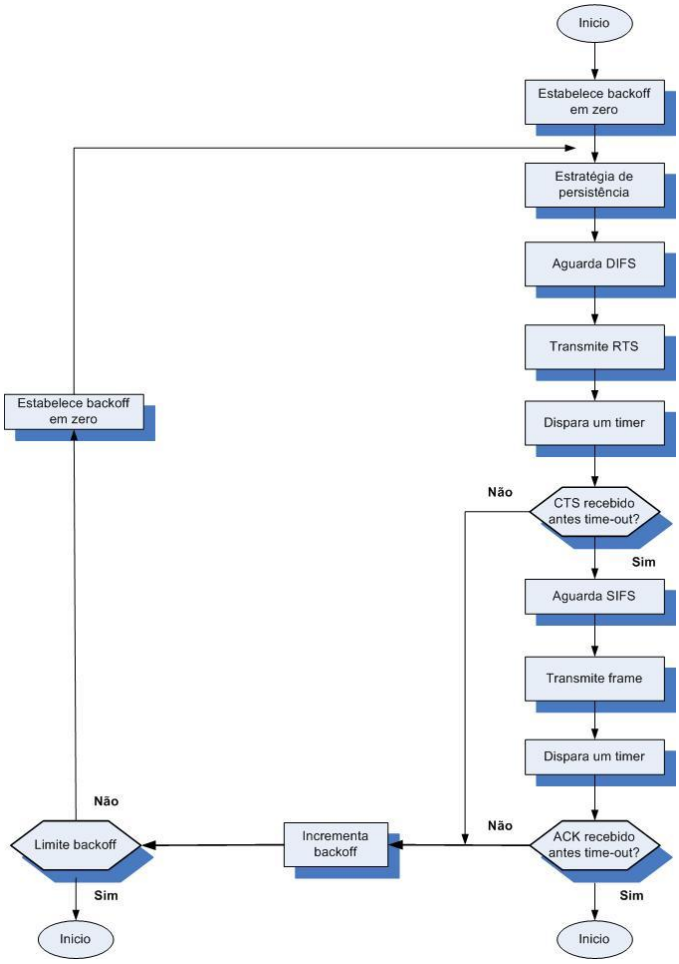


Figura 2.3-2 – Fluxograma CSMA/CA.

Linha de tempo – troca de frames: A Figura 2.3-3 mostra a linha de tempo durante a troca de frames de dados e de controle.

1. Antes de iniciar a transmissão de um frame, a estação de origem ouve o meio verificando o nível de energia da portadora de frequência.
    a. O canal utiliza a estratégia de persistência com *backoff* até que o canal fique livre.
    b. Após a estação detectar que o meio está livre, ela espera um período de tempo, denominado ***Distributed Interframe Space*** **(DIFS)**, para então iniciar a transmissão de um frame de controle conhecido como *Request to Send* (RTS).

2. Após receber o RTS e esperar um curto intervalo de tempo, denominado ***Short Interframe Space*** **(SIFS)**, a estação de destino também envia um frame de controle, conhecido como *Clear to Send* (CTS), à estação de origem. Esse frame indica que a estação de destino está pronta para receber dados.
3. Após um período de tempo igual a SIFS a estação de origem envia os dados.
4. Após um período de tempo igual a SIFS, a estação de destino envia um ACK para mostrar que o frame foi recebido. A confirmação (ACK) é necessária neste protocolo porque a estação de origem não tem como verificar o sucesso do recebimento dos dados no destino. De outro modo, a falta de colisão no CSMA/CA é um modo de indicar à fonte que os dados chegaram ao destino.

Network Allocation Vector (NAV): Como as outras estações adiam o envio de dados quando uma estação já recebeu acesso ao meio? Em outras palavras, como o aspecto *collision avoidance* deste protocolo é realizado? O elemento chave é denominado NAV.

Quando uma estação envia um frame RTS, ela inclui o tempo de duração necessário para ocupar o canal. As estações que são afetadas pela transmissão criam um relógio de temporização, denominado ***Network Allocation Vector*** **(NAV)**, exibindo quanto tempo resta antes das estações olharem se o canal esta livre outra vez. Sempre que uma estação acessar o sistema e enviar um frame RTS, as outras estações disparam os respectivos relógios NAV. Com isto, verificamos que as estações olham primeiramente os relógios NAV para verificar se está liberado o acesso ao meio, antes de verificar se o meio está disponível para transmissão. Na Figura 2.3-4 podemos ter uma idéia melhor do funcionamento do NAV.

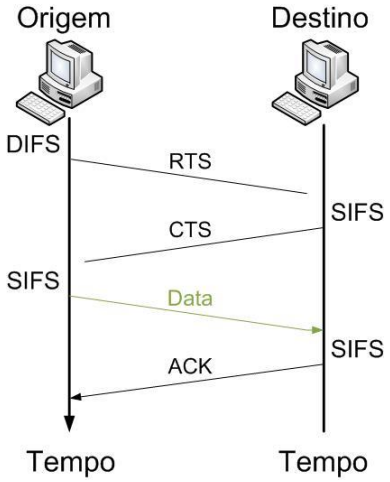


Figura 2.3-3 – CSMA/CA

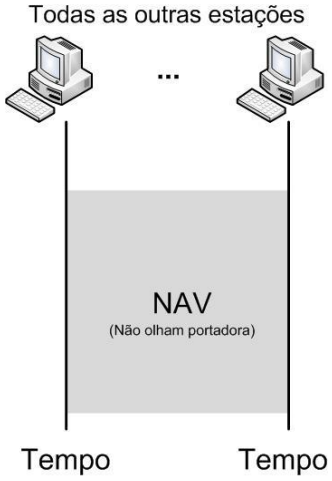


Figura 2.3-4 – NAV

Colisao durante o estabelecimento da comunicacao (*Handshaking)*: O que acontece se ocorrer colisão durante o tempo de transição dos frames RTS ou CTS, frequentemente denominado período de ***handshaking***? Por exemplo, duas ou mais estações podem tentar transmitir frames RTS ao mesmo tempo. Neste caso, os frames podem colidir. Entretanto, visto que não existe mecanismo para detecção de colisão, o transmissor assume que ocorreu colisão se um frame CTS não for recebido do receptor. Assim, é utilizada a estratégia de *backoff* e o transmissor tenta transmitir novamente.

2.3.2 Fragmentação

Um ambiente wireless é bastante susceptível a ruídos. Um frame corrompido tem de ser retransmitido. Desse modo, o protocolo recomenda a fragmentação dos frames, ou seja, a divisão de frames maiores em frames menores. A retransmissão tem mais chances de sucesso se ela tentar enviar frames menores.

3 AMEAÇAS ÀS REDES WIRELESS

A liberdade e a mobilidade que as *WLANs* prometem, também apresentam alguns problemas de segurança graves.

WLANs não estão limitadas por cabos de rede nem são limitadas pela geografia. WLANs proporcionam flexibilidade sem precedentes em que uma área originalmente concebida como um espaço de trabalho colaborativo pode acomodar um grande número de clientes sem fio. Auditórios podem acomodar centenas de computadores em rede apenas conectando alguns *Wireless Access Points* (WAPs) e disponibilizando-os nesta rede. As ondas de rádio usadas pelas WLAN se propagam muito bem. As distâncias prometidas pelos fabricantes de placas de rede sem fio atingem aproximadamente 100 metros. Na realidade, as redes 802.11b podem ser acessadas por mais de meio quilômetro de distância em um ambiente urbano. [1]

As ameaças de segurança discutidas aqui servem para praticamente todos os protocolos da família 802.11, já que a diferença entre eles na questão da segurança é mínima.

Todas WLANs 802.11 usam pacotes da camada 2, a diferença está na camada física. 802.11a usa uma frequência maior do que 802.11b ou uma das variáveis possíveis de 802.11g. Esta frequência maior significa que a transmissão de rádio não vai viajar tão longe e não vai se propagar através de objetos sólidos, bem como o padrão de baixa frequência. Isso tende a ajudar a limitar escutas, mas de forma alguma elimina a ameaça. Também o 802.11a tem cerca de 5 vezes a largura de banda que o 802.11b. Esta maior largura de banda proporciona aos ataques que requerem coleta de dados, uma maior rapidez na sua execução em uma WLAN 802.11a que em uma WLAN 802.11b. A maioria das técnicas de ataque discutidas aqui pode ser aplicada a outros protocolos de rede sem fio, como IEEE 802.15, uma

especificação de rede sem fio de área pessoal (PAN) similar ao Bluetooth. Costuma-se olhar para as ameaças sob dois pontos de vista: o de informação privilegiada, ou seja, alguém que tem acesso interno à rede e do intruso que vem de fora.

O intruso tem acesso à rede sem fio, e o software e o hardware que proporcionam este acesso podem ser comprados ou obtidos publicamente. O atacante que possui informações privilegiadas é um usuário válido da rede sem fio, cujo objetivo é obter o acesso às informações que ele não teria direito. O usuário tem um software válido, hardware e certificados, tanto para a rede com fios como a sem fios.

Comecemos por examinar os ataques contra a confidencialidade de comunicação na rede. Em seguida, passaremos para os ataques que realmente alteram o tráfego na rede, destruindo assim a integridade das informações na rede. Não serão discutidos aqui ataques contra a disponibilidade de uma rede sem fio, que incluem técnicas como a interferência eletrônica, que vai além do escopo deste trabalho. Ao olhar para os ataques de confidencialidade iremos analisar do menos intrusivo e passaremos aos ataques mais intrusivos. Das sete técnicas de ataque mostradas aqui, apenas três violam o sigilo ou a privacidade da sessão: análise de tráfego, escuta passiva ou ativa e espionagem. Uma técnica pode ser utilizada para violar a confidencialidade e ou a integridade física – que é denominada de ataque *man-in-the-middle*. Três técnicas de ataque violam a integridade do tráfego da rede: o acesso não autorizado, o sequestro de sessão, e o ataque de repetição. As técnicas de ataque à integridade geralmente requerem o uso bem sucedido de uma ou mais das técnicas de ataque de confidencialidade.

Nesta seção iremos descrever sete técnicas de ataque que usamos para comparar as tecnologias de segurança disponíveis. Escolhemos estas técnicas de ataque na intenção de generalizar o suficiente para que possam ser utilizadas na avaliação das

tecnologias de segurança representantes. É verdade que estas técnicas não são as únicas, mas de alguma forma poderíamos considerar outras técnicas como sendo variantes ou provindas das citadas aqui.

A informação completa da avaliação da garantia de risco exige um foco sobre as ameaças contra os três componentes fundamentais que garantem a informação. Ou seja, o sistema de informação deve proteger de ataques a confidencialidade, integridade e disponibilidade (CIA). Não será discutido aqui ataque à disponibilidade da WLAN, também conhecido como ataque de negação de serviço. Ataques de negação de serviço contra a camada 1 ou camada 2 não podem ser derrotados por qualquer das tecnologias de segurança de que temos conhecimento, por isso não sentimos que vale a pena discutir aqui.

3.1 ANÁLISE DE TRÁFEGO

Análise de tráfego é uma técnica simples em que o atacante determina a carga sobre o meio de comunicação pelo número e tamanho dos pacotes a serem transmitidos, a origem e o destino dos pacotes, e os tipos de pacotes. A suposição é que o *payload* dos pacotes seja criptografado e que o atacante não consiga decriptografá-lo. Isso deixa o cabeçalho e qualquer parte da informação visível para o atacante. O atacante só precisa de uma placa de rede sem fio operando em modo promíscuo (ouvindo) e um software de modo a contar número e tamanho dos pacotes a serem transmitidos. Uma antena do tipo *yagi* simples ou antena direcional helicoidal fornece uma gama maior de possibilidades para o atacante analisar o tráfego.

A antena *yagi* é uma antena direcional simples que consiste de um condutor horizontal com vários dipolos isolados em paralelo e no plano do condutor. Foi demonstrado que a confecção de uma simples antena *yagi* feita de uma lata de

batatas *Pringles* pode possibilitar, com uma haste de aço e algumas anilhas, um atacante dobrar a escala em que são recebidas transmissões. A antena helicoidal, ou espiral, construída por menos de US$ 100,00 de canos de PVC e fios de cobre, aumenta mais que o dobro da distância original. [2].

A análise de tráfego permite ao atacante obter três formas de informação. O ataque principalmente identifica que há uma atividade na rede. Semelhante ao padrão de comunicações de rádio, um aumento significativo na quantidade de atividade de rede serve como um indicador para a ocorrência de um evento de grande porte.

A identificação e localização física de pontos de acesso sem fio (*Access Points* - APs) na área circundante é uma segunda forma de informação obtida a partir da análise de tráfego. A menos que explicitamente desativado, pontos de acesso difundem os seus *Service Set Identifiers* (*SSIDs*) a fim de identificar se há nós sem fio desejando o acesso à rede. O *SSID* é um parâmetro que deve ser configurado no software do driver da placa *wireless* para qualquer estação sem fio desejando o acesso a uma LAN sem fios. Transmitindo essa informação, pontos de acesso permitem que qualquer um em sua área possam identificá-los com um software localizador simples. Se uma antena direcional é usada junto com um Sistema de Posicionamento Global (GPS), um atacante pode saber não só que existem APs na área, mas também pode obter a localização física do ponto de acesso ou o centro da rede sem fio. Do ponto de vista militar, é a mesma técnica utilizada na triangulação de comunicações de rádio ou baterias de artilharia de campo com a finalidade de parar um ataque inimigo.

A terceira peça de informação que um invasor pode aprender por meio de análise de tráfego é quais os tipos de protocolos estão sendo utilizados nas transmissões. Este conhecimento é obtido com base no tamanho, tipo e número de pacotes que são

transmitidos ao longo de um período de tempo. Um exemplo simples deste ataque é a análise de um *Transmission Control Protocol* (TCP) *three-way handshake*. TCP sincroniza a comunicação entre dois nós finais, transmitindo uma série de três pacotes. Cada pacote usado no “aperto de mão” é de tamanho fixo em termos de número de bytes transmitidos.

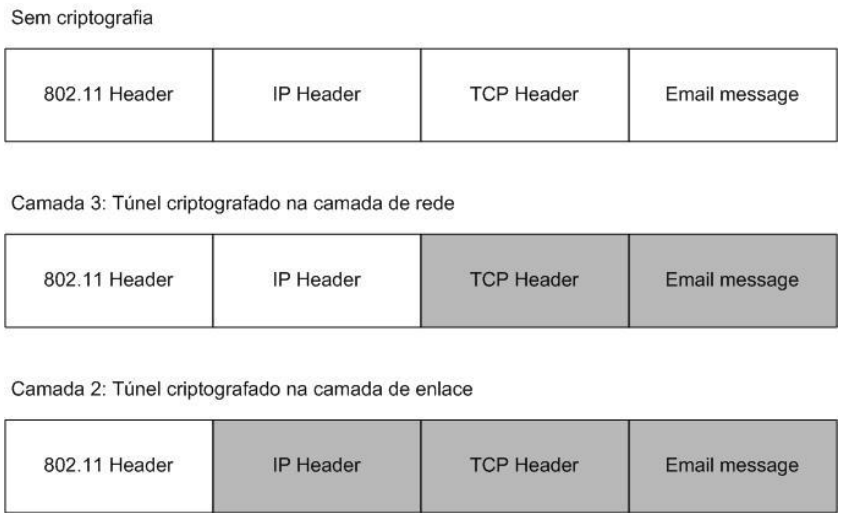


Figura 3.1-1 – Camada de Criptografia

A maioria dos túneis criptografados são implementados na camada 2 ou 3. Isso deixa as informações do cabeçalho expostos para a camada de aplicação e todas as camadas inferiores, como ilustrado na Figura 3.1-1. O atacante pode identificar a origem e o destino por endereço MAC quando a criptografia na camada 2 é empregada. Criptografia na camada 3 deixa o endereço IP do remetente e destinatário expostos. Na maioria dos tipos de tráfego é evidente a leitura do cabeçalho na camada 3.

3.2 ESCUTA PASSIVA

Nesta técnica o atacante monitora passivamente a sessão sem fio (Figura 3.2-1) e o *payload* do pacote. Se a carga é criptografada, isto inclui quebrar a criptografia para ler o *plaintext*. A única condição é que o invasor tenha acesso à transmissão.

Conforme descrito na seção anterior, uma antena direcional pode detectar transmissões 802.11 sob certas condições, ao longo de quilômetros de distância. Portanto, este é um ataque que não pode facilmente ser interrompido através de medidas de segurança física.

Deveríamos acreditar que os utilizadores da rede sem fio podem configurar os seus pontos de acesso sem fio para incluir alguma forma de criptografia, no entanto, estudos têm mostrado que aproximadamente, 50% ou mais dos pontos de acesso sem fio em uso utilizam os mais vulneráveis padrões de segurança wireless, a *wired equivalent privacy* (privacidade equivalente com fios - protocolo WEP), devidamente configurado e funcionando. [1]

O atacante pode obter dois tipos de informações com as escutas passivas. O atacante pode ler os dados transmitidos na sessão e também pode coletar informações indiretamente, examinando os pacotes na sessão, especificamente origem, destino, tamanho, número e tempo de transmissão. O impacto deste tipo de ataque não é só a privacidade da informação que é comprometida, mas a informação recolhida é uma condição importante para outros ataques mais prejudiciais.

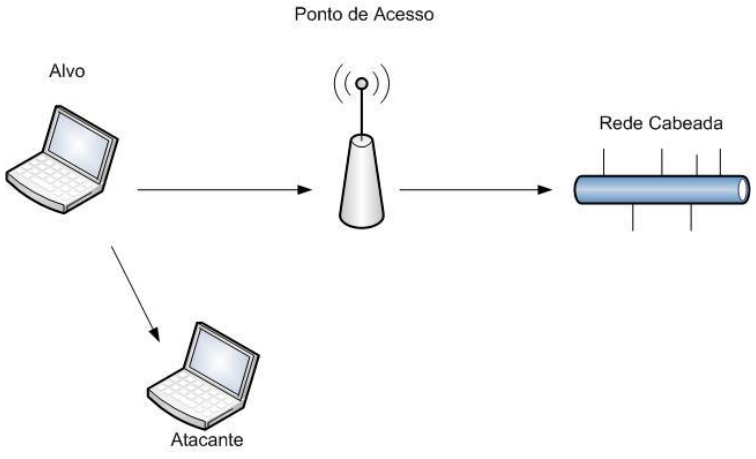


Figura 3.2-1 – Escuta passiva

Se a sessão é criptografada na camada 2 ou superior usando um protocolo como *Wired Equivalent Protocol* (WEP) ou o *Advanced Encryption Standard* (AES), em seguida, a fim de ler os dados, o atacante terá que descriptografar os pacotes. [1] [3] [4] [5] [6] [7] [8] [9]

Escuta passiva exige leitura do *payload* dos pacotes. Fluxos de criptogramas como WEP, são vulneráveis a uma série de ataques passivos. WEP é particularmente vulnerável devido ao pequeno tamanho do Vetor de Inicialização (IV) e sua fraca implementação de criptografia. [10] Devido ao número finito de sequencias do vetor de inicialização (IV), a reutilização de IV pelo WEP o torna suscetível a ataques. Trocas rápidas de chaves e outras modificações fazem o fluxo de cifras menos vulneráveis, mas um fluxo de cifra é sempre uma corrida entre o atacante e o defensor. Cifras por blocos como AES ou 3DES são uma forma muito mais forte de criptografia. Atualmente não há ataques públicos em prática nessas técnicas de criptografia. De um ponto de vista prático escuta passiva só é possível contra a criptografia e codificação de fluxo de pacotes criptografados.

3.3 ESCUTA ATIVA

A técnica de escuta ativa envolve o atacante injetar dados na comunicação para ajudar a decifrar a carga útil (*payload*). O atacante acompanha a sessão sem fio, conforme descrito em escuta passiva. Ao contrário da escuta passiva, no entanto, durante a escuta ativa o atacante não só ouve a conexão sem fio, mas também ativamente injeta mensagens para o meio de comunicação a fim de ajudar a determinar o conteúdo das mensagens. Os pré-requisitos para este ataque são de que o invasor tenha acesso à transmissão e também acesso a qualquer parte do *plaintext*, como um endereço IP de destino ou o conteúdo de todo o *payload*.

Ataques de escuta ativa podem assumir duas formas: o atacante pode modificar um pacote ou pode injetar pacotes completos para o fluxo de dados. Apesar do WEP utilizar uma verificação de redundância cíclica (CRC) que verifica a integridade dos dados no pacote, um atacante pode modificar as mensagens (mesmo que de forma criptografada) para que a alteração de dados no pacote (ou seja, o endereço IP de destino ou o destino de porta TCP) não possa ser detectada. A única exigência para o invasor é determinar a diferença entre os bits de dados que ele quer e injetar os dados originais. Um exemplo de escuta ativa com *plaintext* parcialmente conhecido é o *IP Spoofing*. O atacante muda o endereço IP de destino do pacote para o endereço IP de um host que ele controla. O ponto de acesso faz a decodificação antes de encaminhar o pacote alterado para hospedeiro atacado. No caso de um pacote modificado, o nó receptor irá requisitar o reenvio do pacote e assim o ataque não será aparente.

Usando os pontos fracos do WEP e outros fluxos de cifras, o atacante pode injetar tráfego conhecido na rede a fim de decifrar futuros pacotes enviados por outros. Por exemplo, se o atacante é um usuário privilegiado e envia uma mensagem de correio eletrônico destinada a seu próprio computador na LAN sem fio ou para a vítima, o IV (vetor de inicialização) associado a essa mensagem agora permite que o invasor o use para decifrar os pacotes, no futuro, usando o mesmo IV. Matematicamente, quando o mesmo IV é utilizado onde C é encriptado e P é plaintext,

$$\mathbf{C_1 \oplus C_2 = P_1 \oplus P_2}$$

Se você sabe P1 e pode adquirir C1 e C2 por escutas, então é trivial para calcular P2. O mesmo tipo de ataque pode ocorrer através do envio de tráfego na Web ou saber onde o usuário está navegando. Pode-se criar rapidamente uma base de dados (IV, P1), a fim de decifrar qualquer pacote da camada 2 usando criptografia WEP. A única defesa contra este ataque é de mudar frequentemente a chave WEP

de forma a garantir que você terá um exclusivo par IV e chave. A implementação bem sucedida de mudar frequentemente chaves WEP depende do método de autenticação inicial, a troca da chave privada, e a frequência em que a chave WEP é atualizada. Tais implementações são complicadas, só uma garantia para retardar um atacante, e não necessariamente evitar ataques WEP descritos anteriormente.

3.4 ACESSO NÃO AUTORIZADO

O acesso não autorizado é diferente de qualquer um dos tipos de ataques anteriores que temos discutido, na medida em que não é dirigido a qualquer usuário individual ou conjunto de usuários da WLAN. Ele é dirigido contra a rede como um todo. Uma vez que um atacante tem acesso à rede, ele pode, então, lançar ataques adicionais ou simplesmente desfrutar do uso gratuito da rede. Embora o uso liberado da rede possa não ser uma ameaça significativa para muitas redes, o acesso é um passo fundamental em um ataque ARP (*Address Resolution Protocol*) baseado no ataque *man-in-the-middle*.

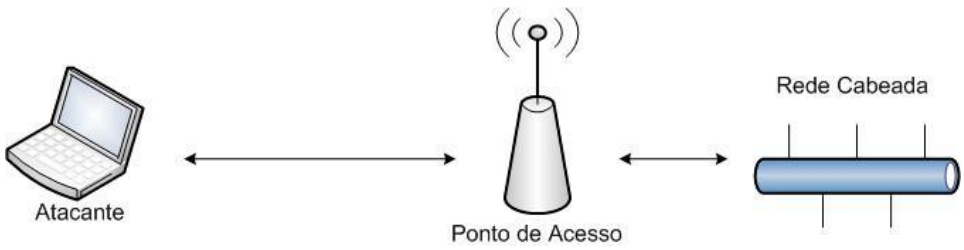


Figura 3.4-1 – Acesso não autorizado

Devido às propriedades físicas das WLANs, os atacantes sempre terão acesso ao componente wireless da rede (Figura 3.4-1). Em algumas arquiteturas de segurança sem fio este será também o acesso do atacante para o dispositivo com fio da rede. Em outras arquiteturas, o atacante deve usar uma técnica como a falsificação de endereço MAC para ter acesso ao dispositivo com fio da rede.

3.5 ATAQUE *MAN-IN-THE-MIDDLE*

Se os pacotes que estão sendo transmitidos são criptografados apenas na camada de rede, ou camada 3, o atacante pode obter as informações do cabeçalho da camada de enlace de dados (camada 2) e da camada 3. Uma VPN (*Virtual Private Network*) ou utilização de IPsec como solução de segurança, serviriam como uma contramedida. Embora essas soluções possam proteger os usuários de um ataque direto contra a confidencialidade dos dados de aplicação, elas não impedem ataques de confidencialidade indiretos, tais como o *man-in-the-middle*, sequestro de sessão (*session highjack*), ou ataques de replay.

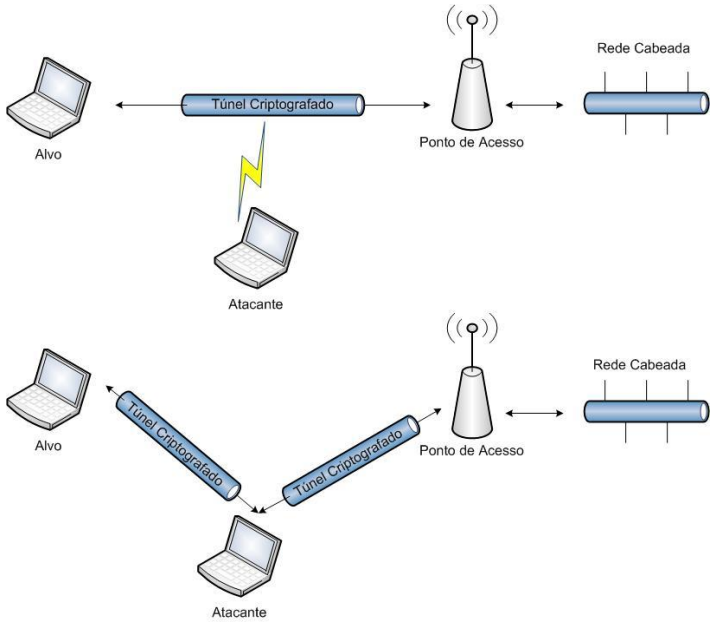


Figura 3.5-1 – Man-in-the-Middle Attack

Um ataque *man-in-the-middle* (Figura 3.5-1) pode ser usado para ler dados de uma sessão privada ou para modificar os pacotes, violando assim a integridade desta sessão. Este é um ataque em tempo real, os dados podem ser lidos ou modificados na sessão em que ocorre. O atacante vai saber o conteúdo da mensagem antes de o destinatário recebê-lo, ou alterar a rota da mensagem.

Existem várias maneiras de implementar este ataque. Um exemplo é quando o alvo está em andamento para autenticar uma sessão. Na primeira etapa, o atacante

quebra a sessão e não permite que o cliente volte a associar-se com o ponto de acesso. Na etapa dois, a máquina destino tenta associar novamente com a rede *wireless* através do ponto de acesso e só é capaz de associar-se a máquina do atacante que está imitando o ponto de acesso. Também na etapa dois, o atacante se associa e se autentica com o ponto de acesso em nome do alvo. Se um túnel criptografado está sendo utilizado, o atacante estabelece dois túneis criptografados entre ele e o alvo e entre ele e o ponto de acesso. [4] [8] [9] [12]

Variações sobre esta técnica de ataque são baseados de acordo com os mecanismos de segurança empregados. Quanto mais mecanismos de segurança em uso, mais mecanismos de segurança que o atacante terá de subverter quando restabelecer a ligação com ambos, o alvo e o ponto de acesso. Sem criptografia ou autenticação em uso o atacante estabelece um ponto de acesso não autorizado (*rogue access point*). O alvo inconscientemente associa-se ao ponto se acesso não autorizado, que age como um *proxy* para a rede sem fio atual. Se a autenticação está ocorrendo, o atacante deve derrotar o mecanismo de autenticação para estabelecer novas conexões entre ele e o alvo e entre ele e o ponto de acesso. Se a criptografia está em uso, o atacante também deve subverter a criptografia para ler ou modificar o conteúdo da mensagem. Como a autenticação no 802.11 não é mútua entre o ponto de acesso e o cliente, e o padrão de criptografia (WEP) é fácil de quebrar, ataques *man-in-the-middle* são algo trivial em redes 802.11.

Os ataques *Address Resolution Protocol* (ARP) são um subconjunto particularmente perigoso de *man-in-the-middle* porque esses ataques podem ser dirigidos contra alvos no dispositivo da rede cabeada, e não apenas nos clientes sem fio. O ataque pode exigir que o mecanismo de autorização seja contornado, se existir, ou sejam fornecidas credenciais falsas. O ataque ARP difere das outras técnicas de ataque

em que as credenciais podem, na verdade, pertencer a um usuário válido. O atacante está apenas tendo acesso à rede e não está aparecendo como destino. Esta pode ser uma distinção ambígua, mas pode ser útil ao analisar as tecnologias de autorização. [5] [9] [12] [13] [14] [15]

O *Address Resolution Protocol* (ARP) mapeia o endereço do controlador de mídia (MAC) (Layer 2) de um nó de rede para o endereço Internet Protocol (Layer 3). Alterando o mapeamento do endereço MAC para o endereço IP permite que um invasor redirecione o tráfego de rede através de sua máquina. Com a sessão passando pelo computador do invasor o atacante pode ler o *plaintext*, coletar pacotes criptografados para descriptografá-los mais tarde, ou modificar os pacotes na sessão. Ataques ARP *cache poison* podem ser contidos pelos roteadores, mas um dano muito grande pode ser feito com um bem sucedido ataque ARP *Cache Poisoning*. [16] [17] [18]

Para realizar um ataque bem-sucedido, o invasor deve ter acesso à rede, nada mais. O atacante envia uma mensagem de resposta ARP forjado que muda o mapeamento do endereço IP para o endereço MAC dado. O endereço MAC não é mudado, apenas o mapeamento. Uma vez que o cache foi modificado o atacante pode atuar como um *man-in-the-middle* entre dois hosts no domínio de broadcast. Isto é ilustrado abaixo na Figura 3.5-2, onde um atacante em um cliente sem fio têm acesso a sessões entre dois hosts com fio.

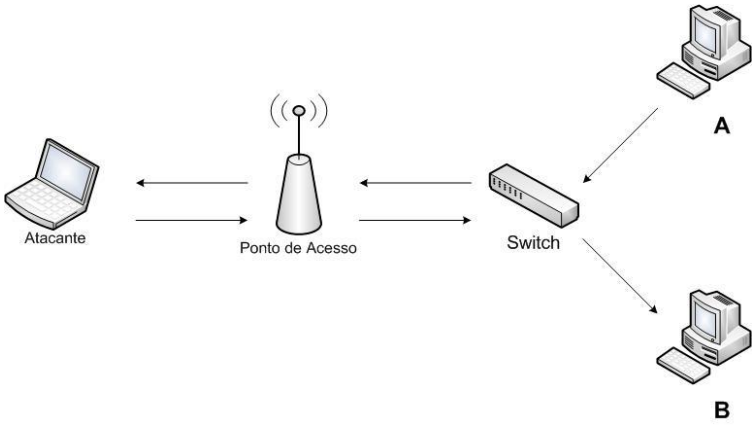


Figura 3.5-2 – ARP ataque

Negar esta técnica de ataque é um passo absolutamente essencial para projetar a arquitetura de segurança. Negar o acesso à WLAN limita as possibilidades do atacante para o ataque posterior, que provavelmente será a rede cabeada. É importante separar ataques de redirecionamento ARP dos ataques *man-in-the-middle* porque redirecionamento ARP não exige que o atacante estabeleça sessões com o alvo e a rede. Ataques ARP podem ser uma maneira de realizar a análise de tráfego ou escuta passiva.

3.6 SEQUESTRO DE SESSÃO

Sequestro de Sessão (*Session High Jacking*) é um atentado contra a integridade de uma sessão. O atacante tem acesso a uma sessão autorizada e autenticada longe do seu verdadeiro proprietário. O alvo sabe que não tem mais acesso à sessão, mas pode não estar ciente de que a sessão foi tomada por um atacante. O alvo pode atribuir a perda de sessão a um mau funcionamento normal da WLAN. Uma vez que o atacante é dono de uma sessão válida ele pode usar a sessão para que finalidades ele quiser e manter a sessão por um tempo prolongado. Esse ataque ocorre em tempo real, mas pode continuar por muito tempo depois de a vítima achar que a sessão terminou.

Para executar com êxito o sequestro de sessão (*session high jacking*) o atacante deve realizar duas tarefas. Primeiro ele deve se mascarar como sendo o alvo para a rede sem fio. Isto inclui a elaboração de pacotes de nível superior para manter a sessão, usando algum *token* de autenticação persistente e empregando alguma criptografia de proteção. Isso exige um ataque de espionagem bem sucedido contra o alvo em questão, com o objetivo de recolher as informações necessárias, como mostrado em uma etapa da Figura 3.6-1 abaixo. A segunda tarefa que o atacante deve fazer é impedir que o alvo continue com a sessão. O atacante normalmente vai usar uma sequência de pacotes falsificados (*spoofed*) para manter o alvo fora da sessão como descrito na etapa dois da figura 3.6-1. [13] [14] [19]

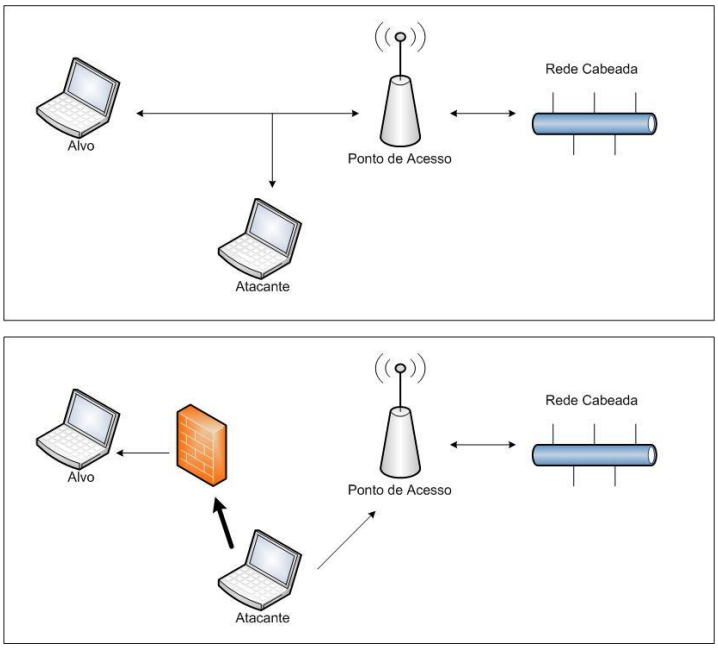


Figura 3.6-1 – Sequestro de sessão

3.7 ATAQUE DE REPETIÇÃO (*REPLAY ATTACK*)

Ataques de repetição (*Replay Attack*) visam igualmente a integridade das informações na rede e, necessariamente, a integridade de uma sessão específica. Ataques de repetição são usados para acessar a rede com as autorizações do alvo, mas a sessão real, ou sessão que é atacada, não é alterada ou sofre qualquer

interferência. Este ataque não é um ataque em tempo real, o atacante para ser bem sucedido, terá que ter acesso à rede em algum momento depois da sessão, ou das sessões, originais.

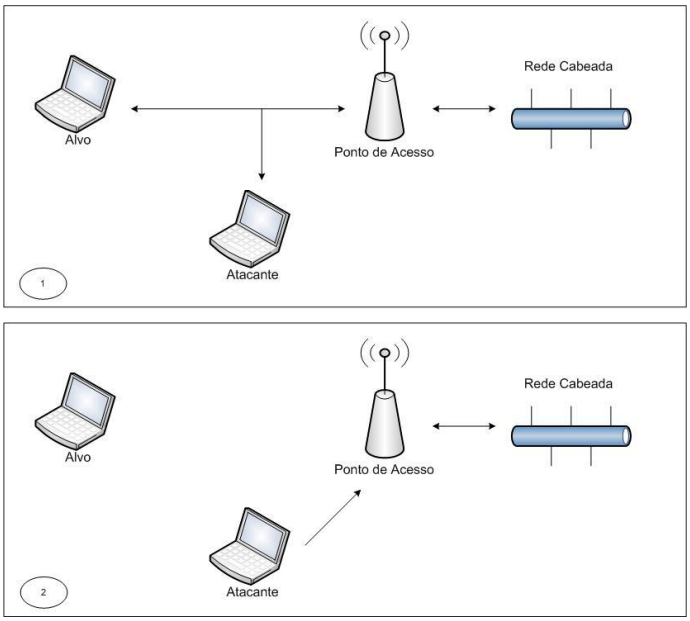


Figura 3.7-1 – Ataque de repetição

Em um ataque de repetição (Figura 3.7-1), o atacante captura a autenticação de uma sessão ou sessões. O atacante então repete a sessão de autenticação em um momento posterior, ou usa várias sessões para sintetizar a parte de autenticação de uma sessão. Uma vez que a sessão foi validada, o atacante estabelece uma sessão autenticada sem estar a par de algum segredo compartilhado usado na autenticação. Sem os mecanismos de segurança adicionais, o atacante pode interagir com a rede, usando as autorizações e as credenciais do alvo. Se a WLAN utilizar alguma criptografia que o atacante não consegue derrotar, o atacante pode ainda ser capaz de manipular a WLAN e modificar seletivamente partes dos pacotes para alcançar o resultado desejado. [4] [5] [7] [20] [21]

4 Segurança Usada em Redes Wireless

As comunicações sem fio sempre estiveram propensas a problemas de segurança antes de qualquer um dos padrões 802.11. A maioria dos usuários talvez nunca tenha pensado sobre segurança sem fio até que o mercado reagiu com notícias, anúncios e produtos para tornar o público ciente dos perigos. O que faz das redes sem fio serem sensíveis às ameaças de segurança tem a ver com serem sem fio. Isto significa que os dados são transmitidos através do ar e são suscetíveis à espionagem por qualquer pessoa em uma determinada área. Ao longo dos anos, diferentes tipos de criptografia têm sido utilizados para proteger os dados dentro dessa transmissão, porém nem sempre têm sido bem sucedidas. Este capítulo tenta identificar a maioria dos métodos de segurança disponíveis hoje. Com esta seção pretendemos ter uma compreensão clara dos métodos utilizados no passado e no presente para proteger as redes sem fio.

4.1 AUTENTICAÇÃO

Ao se conectar a uma rede sem fio, deve-se realizar algum tipo de autenticação. Existem dois tipos principais de autenticação para os padrões IEEE atuais: autenticação de chaves compartilhadas e autenticação de chaves abertas.

4.1.1 Autenticação de chave compartilhada

Autenticação de chave compartilhada foi criada para ser o mais seguro dos dois tipos, no entanto, esse método tornou-se menos seguro devido a um pequeno descuido no modo como ele valida chaves de usuário.

Autenticação de chave compartilhada funciona através de um mecanismo de resposta de desafio. Para explorar esse processo é preciso primeiro se conectar à rede. O dispositivo cliente envia um *probe frame*. Este *frame* irá procurar redes sem fios disponíveis e suas configurações de conexão. Uma vez que um ponto de acesso

"ouve" este *probe*, ele irá responder com um *probe frame response*. Este quadro vai identificar todas as suas configurações de conexão para o dispositivo final.

Em alguns casos, um dispositivo final ouvirá muitas respostas de diferentes pontos de acesso na área. Para se certificar de que o dispositivo se conectara apenas ao ponto de acesso com o melhor sinal, o quadro de resposta do *probe* tem um valor para a intensidade do sinal atual. Um cliente pode ouvir várias respostas, embora ele só irá conectar-se ao ponto de acesso com o valor mais alto de intensidade do sinal. Depois, o cliente final determina se suporta as mesmas configurações do ponto de acesso, e o passo seguinte (chamado de autenticação) ocorre.

Quando o dispositivo final quer autenticar, ele envia um quadro de resposta de autenticação para o ponto de acesso. O ponto de acesso determina se é um pedido de autenticação, e irá enviar um pacote desafio de volta ao cliente. O pacote desafio consiste de um bloco de dados em texto claro. O dispositivo final é requisitado a criptografar os dados, neste caso com a sua chave WEP (*Wired Equivalent Privacity*), que é também configurada no ponto de acesso, e enviar de volta ao ponto de acesso. Uma vez feito isso, o ponto de acesso compara com a versão que ele tem do pacote criptografado. Se os resultados coincidirem, o ponto de acesso permitirá que o dispositivo final acesse a rede. Se os resultados não corresponderem, a autenticação falhará e será negada uma conexão para o dispositivo final.

Para obter um completo entendimento de como isso funciona, veja Figura 4.1.1-1, que descreve o processo de conexão e autenticação.

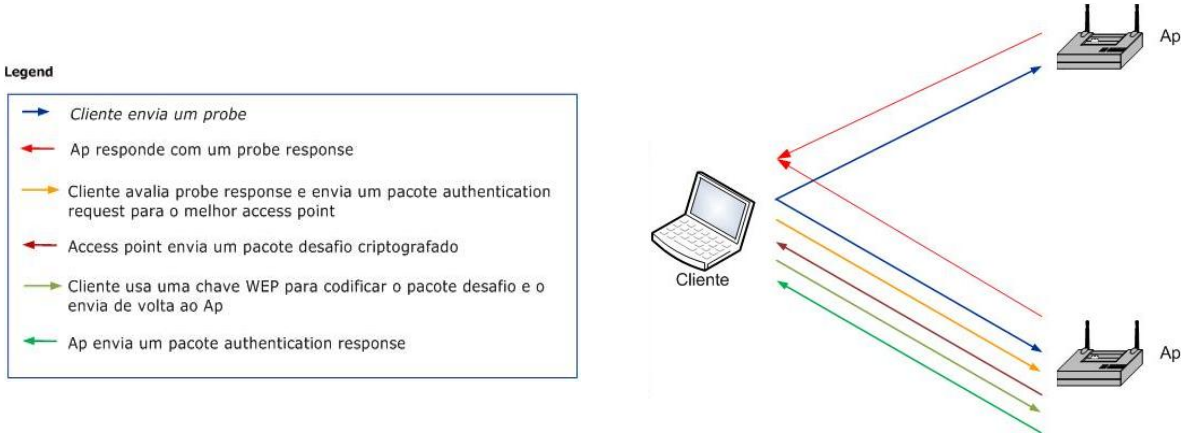


Figura 4.1-1 – Autenticação de chave compartilhada

4.1.2 Autenticação de chave aberta

Autenticação de chave aberta foi originalmente vista como um método menos seguro do que autenticação de chave compartilhada. A intenção era fazer uma rede aberta, portanto, não exigindo que os clientes tenham conhecimento da chave WEP. Como a segurança tornou-se uma questão cada vez mais visível, muitos fornecedores idealizaram novos métodos.

Isso criou um problema real: como ter uma solução que melhore a segurança e ainda se manteria dentro das normas padrão. Estes esforços levaram à idéia de usar a autenticação aberta e, ao contrário de antes, ela exigiria o uso de uma chave WEP. Quando usada, a chave WEP era necessária para se conectar à rede. Isso funcionou porque quando se fala direito com uma chave WEP, uma verificação de redundância cíclica (CRC) é feita e testada no quadro, permitindo que o quadro acesse a rede para o destino.

Olhando como a autenticação de chave aberta funciona, vê-se que o dispositivo final conecta-se à rede como fez com chave compartilhada. Como a autenticação aberta e autenticação de chave compartilhada diferem? A autenticação aberta envia uma solicitação de autenticação, mas não recebe um desafio, em vez disso, é permitido se comunicar, por padrão. Quando a WEP é ativada, o processo é ligeiramente diferente. Quando o cliente sem fio começa a falar, ele automaticamente encripta

todos os dados com criptografia WEP. Quando o ponto de acesso ouve os dados a serem enviados, ele decifra os quadros e os encaminha. Se os quadros são criptografados com uma chave diferente do ponto de acesso, o processo de descriptografia falhará e o pacote é descartado. Para obter uma melhor compreensão de como funciona a autenticação aberta, bem como ela difere de autenticação de chave compartilhada, veja a Figura 4.1.2-1.

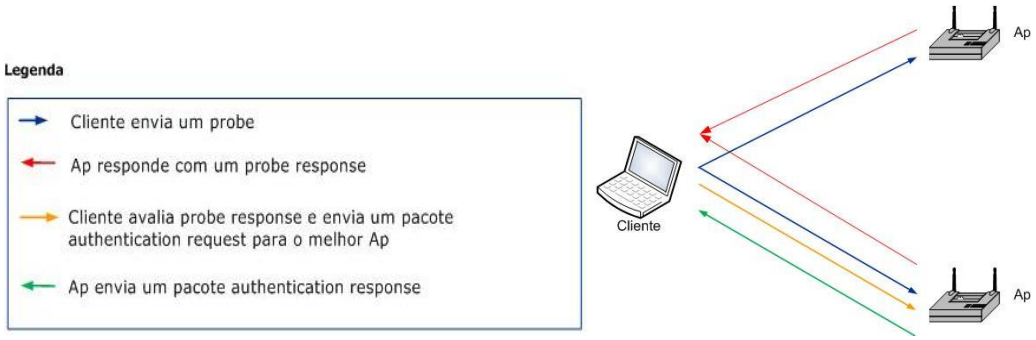


Figura 4.1-2 – Autenticação de chave aberta

4.2 SSID

Quando se olha para a segurança no que diz respeito ao campo SSID (*Service Set Identifier*), vê-se que a maioria das redes, por padrão, transmite essa informação para quem está ouvindo. Percebeu-se que se o SSID não for transmitido, a existência de uma rede sem fio pode ser um pouco mascarada. Este mascaramento exigiria ao cliente enviar um *probe frame* para todas as redes sem fio disponíveis. Na maioria das redes sem fio IEEE a existência do SSID é facilmente atingível com algum tipo de *sniffer wireless*. Isso ocorre porque o SSID é parte do processo de se conectar a uma rede sem fio. Analisando a Tabela 4.2-1, pode-se ver que o SSID está presente no cabeçalho de um *probe frame request* sem fio.

Mesmo com o SSID mascarado, cada vez que um cliente quer se conectar a uma rede, ele irá transmitir todas as suas configurações de conexões, incluindo o SSID como parte do seu processo de sondagem.

Tabela 4-1 – Captura do SSID por Sniffer

802.11 Beacon	FC =....., SN = 448, FN = 0, BI = 100, SSID =, DS = 11
802.11 Probe Req	FC =....., SN = 689, FN = 0, SSID = AEE
802.11 Probe Req	FC =....., SN = 690, FN = 0, SSID = AEE
802.11 Beacon	FC =....., SN = 449, FN = 0, BI = 100, SSID =, DS = 11
802.11 Probe Req	FC =....., SN = 691, FN = 0, SSID = AEE
802.11 Probe Req	FC =....., SN = 692, FN = 0, SSID = AEE
802.11 Probe Req	FC =....., SN = 693, FN = 0, SSID = AEE
802.11 Probe Rsp	FC =....., SN = 451, FN = 0, BI = 100, SSID = AEE, DS = 11
802.11 Probe Rsp	FC =... R. ..., SN = 451, FN = 0, BI = 100, SSID = AEE, DS = 11
802.11 Probe Req	FC =....., SN = 694, FN = 0, SSID = AEE
802.11 Probe Rsp	FC =....., SN = 452, FN = 0, BI = 100, SSID = AEE, DS = 11
802.11 Probe Req	FC =....., SN = 695, FN = 0, SSID = AEE
802.11 Probe Rsp	FC =....., SN = 453, FN = 0, BI = 100, SSID = AEE, DS = 11

Diversos fornecedores têm seus SSIDs padrões configurados nos programas que acompanham seus equipamentos. Esta é uma das primeiras opções a ser checada pelos hackers quando se tenta explorar uma rede sem fio. Muitas empresas também utilizam SSIDs muito simples, como *Wireless*, WLAN, e *Bridge*. A Tabela 4.2-2 descreve alguns dos SSIDs comumente utilizados.

Tabela 4-2 – Detalhes de SSIDs padrões

Cisco (All Aironet Access Points/Bridges)	
– SSID:	Tsunami
LINKSYS Product Families:	
– SSID:	Linksys
Netgear 802.11 DS products, ME102, and MA401Default	
– SSID:	Wireless
SMC Access Point Family	
– SSID:	WLAN
SMC2682W EZ-Connect Wireless Bridge	
– SSID:	BRIDGE Wave LAN Family:
– SSID:	"WaveLAN Network"
Symbol AP41x1 and LA41x1/LA41x3	
– SSID:	101
TELETRONICS WL-Access Points	
– SSID:	Any

4.3 SEGURANÇA BÁSICA WIRELESS

Antes de entrar em todos os diferentes tipos de criptografia e de métodos avançados de segurança, vamos dar uma olhada em algumas coisas básicas que podem ser feitas para criar uma rede sem fio segura. Como demonstrado, o SSID não contribui para a segurança, no entanto, ainda é uma boa idéia evitar a sua transmissão. Além disso, outra coisa importante é mudar os nomes de usuário e senhas padrão em todos os pontos de acesso. Alguns até têm chaves WEP padrão que devem ser mudadas. Em seguida, execute a autenticação aberta com alguma criptografia ativada. Outras mudanças recomendadas são a de evitar DHCP para o segmento de rede sem fio. Um dos objetivos principais seria a de desenvolver uma política de classificação de informação para educar a todos, como o que deve ou não deve ser acessado em redes sem fio.

4.4 WIRED EQUIVALENT PRIVACY (WEP)

O padrão *Wired Equivalent Privacy* (WEP) foi criado para dar às redes sem fio recursos de segurança semelhantes ao de redes cabeadas.

WEP é definido como um mecanismo opcional de criptografia usado para fornecer confidencialidade de dados que é subjetivamente equivalente à confidencialidade de uma rede de área local (LAN), meio que não emprega técnicas de criptografia para aumentar a privacidade. Isso nos dá a idéia básica de como WEP foi criado e quais os objetivos a que inicialmente se destina a satisfazer. Para cumprir essas metas, o *wireless* teve de enfrentar os três princípios da segurança da informação: confidencialidade, disponibilidade e integridade.

1. O objetivo fundamental do WEP é evitar a espionagem, mantendo a confidencialidade.

2. O segundo objetivo é permitir o acesso autorizado a uma rede sem fio, que é a disponibilidade.

3. O terceiro objetivo é evitar a adulteração de qualquer dado na comunicação sem fio, que é a integridade.

O protocolo WEP é utilizado para criptografar dados de um cliente sem fio a um ponto de acesso. Isto significa que os dados vão viajar sem criptografia dentro da rede wired.

O protocolo WEP é baseado em cifra RSA *Securities* RC4. Esta cifra é aplicada ao corpo de cada quadro e do CRC. Existem dois níveis de WEP geralmente disponíveis: uma base numa chave de 40 bits de criptografia e 24 bits de vetor de inicialização (IV), o que equivale a 64 bits; e uma base numa chave de 104 bits de criptografia e 24 bits de vetor de inicialização (IV), que é igual a 128 bits.

Este protocolo tem sido afetado com problemas desde seu início. A eficiência dos *exploits* (em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional – como o próprio sistema operacional), elementos de design pobre, e problemas gerais de gerenciamento de chaves, fizeram o WEP um mecanismo de segurança muito insuficiente. Esta seção, no entanto, discute como WEP opera. Uma das funções originais do WEP era ter a criptografia incapaz de ser afetada pela perda do quadro devido à interferência. Isto significa que quando dados são enviados através do ar e perde-se um frame, não haveria nenhuma perda para o frame anterior. Com os métodos de segurança mais recentes e métodos antigos de proteção em redes cabeadas, é comum que os pacotes subsequentes tenham uma dependência de criptografia no quadro seguinte ou anterior.

4.4.1 Processo de criptografia WEP

O WEP utiliza uma cifra de fluxo RC4 para criptografar os dados em uma rede *wireless*. Ao realizar o processo de criptografia WEP várias etapas são executadas. O primeiro passo é gerar um valor de semente (*seed value*).

Este valor de semente é usado para iniciar o processo de *keying*. Este valor pode ser referido como um agendamento de chaves ou como o valor da semente. Não importa como este valor é chamado, é considerada a chave WEP. Após esse valor ser definido, ele deve então ser inserido no ponto de acesso. Para garantir que o cliente pode receber e decodificar a transmissão, o valor de semente ou a chave WEP deve ser indicado para cada cliente. Isso permitirá ocorrer uma conversa WEP criptografada.

Este valor não é usado apenas para criar um fluxo de dados WEP criptografado; uma técnica para embaralhar a chave é também aplicada. Esta técnica usa um vetor de inicialização (IV) de 24 bits que é criado quadro-a-quadro.

A técnica em que o IV é criado difere entre os fornecedores. O padrão WEP que é descrito dentro 802.11b define o tamanho do IV, e exige a mudança do IV sobre uma base quadro-a-quadro. Fora isso, não há requisitos da norma que definem como incrementar ou embaralhar a sequência IV. A falta da definição de uma sequência de IV é um ponto onde o protocolo WEP possui um grande problema de segurança. Uma vez que a chave WEP e IV estão juntas, elas podem ser usadas para criptografar o quadro. Quando os dados estão prontos para a transmissão, as chaves WEP e IV são combinadas, usando o RC4. O último passo é enviar o pacote. Uma vez que a outra extremidade recebe o quadro, o IV é retirado do cabeçalho do quadro e aplicado ao valor pré-semente para produzir a mesma sessão baseada em chave WEP que foi usado para criptografar o pacote. O mesmo processo de criptografia RC4 é realizado em sentido inverso, permitindo que o texto cifrado seja transformado para texto simples. Uma vez que esta operação seja concluída, o CRC é removido e aplicado aos dados para se certificar de que não foi corrompido em trânsito.

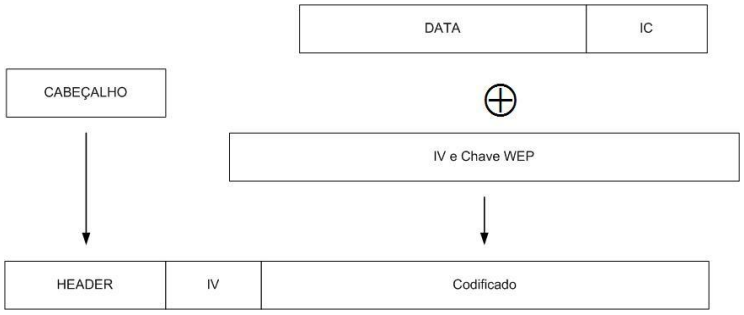


Figura 4.4-1 – Detalhes do processo WEP

A Figura 4.4.1-1 mostra como a criptografia é inserida no local. Como se pode ver, os dados e a verificação da integridade estão juntos de forma linear, bem como as chaves WEP e IV. As chaves WEP e IV são alimentadas com o gerador de números pseudo-aleatórios. A saída deste gera um fluxo de chave igual ao comprimento do *payload* do quadro mais o CRC. O remetente, em seguida, executa uma operação XOR no fluxo de chave e os dados, criando um fluxo de dados criptografado. O próximo passo envolve a colocação do IV dentro do cabeçalho do pacote e a transmissão do pacote para o destinatário.

4.5 802.1x

Ambas as organizações, IEEE e ANSI aprovaram o padrão 802.1x. Em 14 de junho de 2001, o IEEE aprovou as normas, quatro meses depois, em 25 de outubro de 2001, a *American National Standards Institute* (ANSI) aprovou também. O padrão 802.1x foi projetado para a autenticação de portas para todas as redes IEEE 802. Isso significa que ele irá trabalhar através de Ethernet, FDDI, *Token Ring*, *wireless* e muitos outros padrões de rede IEEE 802.

Uma coisa que as pessoas tendem a ficar confusas sobre IEEE 802.1x é que não é de modo algum um tipo de criptografia ou cifra. Toda criptografia tem lugar fora do padrão IEEE 802.1x. Por exemplo, em uma rede sem fio, o protocolo EAP poderia usar um de seus vários métodos de criptografia para autenticação. Após a

autenticação do usuário à rede sem fio, estes podem iniciar uma conversa usando WEP, TKIP, AES, ou um dos muitos outros esquemas de criptografia padrão *wireless*.

O padrão 802.1x é apenas um mecanismo que nega todo o tráfego, exceto os pacotes EAP, por exemplo, de acessar à rede. Uma vez que o EAP diz que o dispositivo está apto a acessar à rede, o protocolo 802.1x diz ao switch ou ponto de acesso para permitir o tráfego do usuário.

A Figura 4.5-1 revela as três principais designações definidas pela norma 802.1x. Cada uma delas tem regras e funções específicas. A norma foi escrita para integrar uma grande quantidade de equipamentos diferentes, os nomes dessas funções permanecem bastante genéricos. Como se pode ver na Figura 4.5-1, o protocolo 802.1x utiliza dois outros padrões. A partir do requerente ao autenticador, o padrão é EAP. Desde o autenticador para o servidor de autenticação, o protocolo é o RADIUS. O protocolo 802.1x EAP recebe as solicitações, as envia para um servidor RADIUS, e aguarda uma resposta. Uma vez que uma resposta é recebida, o acesso à rede poderá ser permitido ou negado.

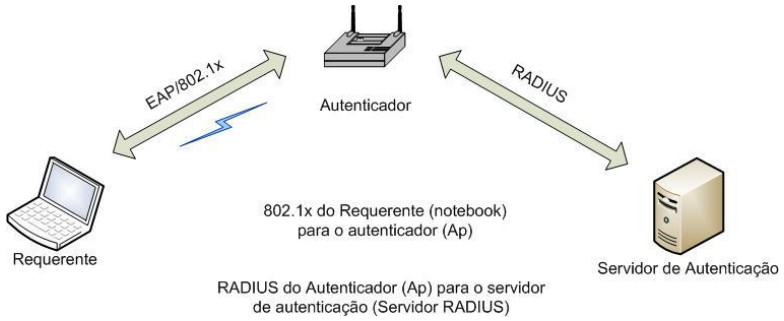


Figura 4.5-1 – Uma visão do 802.1x

4.5.1 O servidor de autenticação

O servidor de autenticação fornece o acesso à concessão ou rejeição dos recursos. Ele faz isso através da recepção de um pedido de acesso a partir do autenticador.

Quando o servidor de autenticação ouve um pedido, ele irá validá-lo e retornar uma mensagem de conceder ou rejeitar o acesso de volta para o autenticador.

Esta é a parte final da norma 802.1x pois o funcionamento deste servidor é definido em outro padrão (isto é, RADIUS).

4.5.2 Autenticador

O autenticador é a primeira parte da rede que um dispositivo 802.1x tentará conexão. Neste exemplo, é um ponto de acesso sem fio, embora possa ser qualquer coisa, proporcionando acesso à rede. O papel do dispositivo é permitir que apenas os pacotes EAP passem e esperem uma resposta do servidor de autenticação. Uma vez que o servidor de autenticação responde com um aceitar ou rejeitar a mensagem, o autenticador funcionará adequadamente. Se a mensagem retornada é uma mensagem de rejeição, ele continuará a bloquear o tráfego até que o resultado seja uma mensagem de aceitar. Quando a resposta de aceitar vem do servidor de autenticação, o autenticador então permite ao requerente o acesso à rede.

4.5.3 Requerente

O requerente é o dispositivo que pretende conectar-se à rede 802.1x. Isso pode ser um computador, um laptop, um PDA ou qualquer outro dispositivo com uma interface de rede. Quando o requerente se conecta à rede, deve passar pelo autenticador. Esse autenticador só permite ao requerente passar tráfego EAP ao servidor de autenticação. Este tráfego EAP são credenciais de autenticação do usuário ou do dispositivo. Uma vez que o servidor de autenticação determine que o usuário ou o dispositivo possa ser permitido na rede, ele enviará uma mensagem de acesso de concessão.

4.5.4 Extensive Authentication Protocol over LAN (EAPOL)

Extensive Authentication Protocol over Local Area Network (EAPOL) é parte do EAP, embora seja descrito dentro do padrão 802.1x. Isso ocorre porque o padrão 802.1x permite que certos tipos de mensagens EAP passem através do autenticador para o requerente. Para definir quais mensagens são autorizadas a passar, cada tipo de mensagem e formato de quadro teve de ser incluído dentro do padrão 802.1x.

O tráfego enviado pelo padrão EAPOL é descrito com seis tipos de quadros. Isso significa que somente esses seis tipos de quadro são autorizados a passar por um ponto de acesso para um cliente.

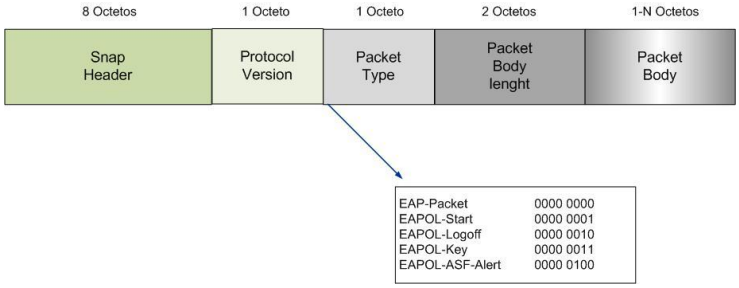


Figura 4.5-2 – Diagrama EAPOL

O IEEE criou espaço para mais, embora o padrão atual só descreva seis. A Figura 4.5-2 mostra cada tipo de quadro, juntamente com o valor que é usado para identificar o quadro.

O tipo EAPOL mais envolvido é o quadro EAPOL-*Key*. Este quadro é utilizado para enviar material contendo chaves, como chaves WEP dinâmicas. O único quadro de chave definido no padrão 802.1x é a chave RC4 WEP. Em 802.11i poderemos notar que algumas mudanças foram feitas no funcionamento do quadro EAPOL-*Key* para acomodar outros tipos de criptografia além do RC4.

4.6 REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

RADIUS é um acrônimo para *Remote Authentication Dial-In User Service*, um protocolo utilizado em ambientes de rede para a autenticação, autorização e

contabilidade. RADIUS pode ser executado através de vários tipos de dispositivos, como roteadores, servidores, switches, modems, concentradores VPN, ou qualquer outro tipo de dispositivo compatível com RADIUS. O protocolo trabalha através da criação de um túnel criptografado entre o dispositivo de rede e o servidor RADIUS. Este túnel é usado para enviar todas as informações de autenticação, de autorização e de contabilidade (AAA - *Authentication Authorization Accounting*) sobre quem é o usuário, onde o usuário é autorizado a ir, e onde o usuário realmente foi. Para iniciar este túnel criptografado, uma frase ou palavra chamado segredo compartilhado é necessário. O segredo compartilhado está localizado no dispositivo de rede que utiliza RADIUS e no servidor RADIUS. Uma vez que o segredo compartilhado é configurado corretamente, a comunicação segura pode ser estabelecida.

Um dos benefícios do RADIUS é o uso de uma base de dados comum dos usuários para prover estes serviços de AAA em vários tipos de dispositivos. Os bancos de dados que usam RADIUS para armazenar nomes de usuário e senhas podem ser configurados para apontar para muitos tipos diferentes de diretórios. Isto significa que RADIUS pode utilizar várias estruturas de diretório, como o *Microsoft Active Directory* (MS-AD), *Novell Network Directory System* (NDS), *Lightweight Directory Access Protocol* (LDAP), e muitos outros tipos de serviços de diretório em comum.

Este protocolo permite que os administradores centralizem o local e a administração do acesso do usuário e sua contabilização para todos os equipamentos de rede, bem como acesso remoto. RADIUS impede muitas das dores de cabeça associadas a remoção correta do acesso aos equipamentos de rede quando os empregados são dispensados. Uma vez que uma organização tenha implantado RADIUS, o acesso

do usuário pode ser facilmente removido em caso de uma rescisão, sem precisar alterar manualmente nomes de usuário e senhas de todos os equipamentos de rede.

As especificações do protocolo RADIUS estão atualmente definidas na RFC 2865 [22] e RFC 2866 [23]. RFC 2865 concentra-se na parte de acesso do RADIUS, permitindo o acesso do usuário em dispositivos ou para a própria rede. RFC 2866 concentra-se na parte de contabilidade do RADIUS, permitindo aos administradores monitorar as mudanças e acesso a dispositivos de rede, bem como o acesso geral à própria rede.

Agora que temos uma visão do uso primário e da história do RADIUS, podemos ver como RADIUS diz respeito a wireless. Primeiro, RADIUS pode ser usado como um método de acesso para administrar o ponto de acesso. Isto é semelhante à forma como ele seria usado para administrar roteadores e switches. O ponto de acesso e o servidor RADIUS teriam um segredo compartilhado e que seria usado para criar um canal criptografado que pode transportar o tráfego de autenticação do usuário.

Outra abordagem é usar o RADIUS, como explicado no padrão 802.1x, como um mecanismo de *back-end* de autenticação de usuário. RADIUS em si oferece esse recurso, de modo que o padrão 802.1x foi usado em vez de criar o seu próprio mecanismo de autenticação. Com este cenário, o ponto de acesso terá de ser configurado corretamente com o segredo compartilhado do servidor RADIUS e o ponto de acesso terá que manter o controle de solicitação do usuário para entrar na rede. Isso significa que o usuário só iria negociar a sua autenticação com o ponto de acesso, não com o servidor RADIUS. Isto é similar a como RADIUS deverá ser criado em um dispositivo de acesso remoto. Um usuário que quisesse permissão para entrar na rede seria solicitado pelo dispositivo de rede para fornecer algum tipo de autenticação. Depois de fornecida a autenticação, o equipamento de rede irá

verificá-la no banco de dados do servidor RADIUS do usuário. Se as credenciais estiverem corretas o usuário deve ser permitido na rede; se as credenciais não estiverem corretas, o usuário terá seu acesso negado.

RADIUS tem apenas quatro tipos de pacotes de autenticação, mas existem outros tipos de pacotes para a contabilidade. No entanto, esta seção só incide sobre os pacotes de autenticação. Os quatro tipos são:

1. *Access-Request* - Este pacote permite a sequência RADIUS ser estabelecida.

2. *Access-Accept* - Este pacote informa ao cliente RADIUS que a autenticação solicitada é correta.

3. *Access-Reject* - Este pacote informa o cliente RADIUS que a autenticação solicitada estava errada.

11. *Access-Challenge* - Este pacote é utilizado para enviar um desafio a um cliente RADIUS mostrar suas credenciais de autenticação.

Olhando para o pacote RADIUS na Figura 4.6-1 pode-se ver que todos os quatro tipos de pacotes consistem no mesmo formato de pacote. Eles são identificados pelo código de campo. Este campo tem números de código disponíveis que poderiam ser utilizados, porém os únicos abordados aqui são os *Access-Request* identificado pelo código 1, o *Access-Accept* identificado pelo código 2, o *Access-Reject* identificado pelo código 3, e o *Access-Challenge* identificado pelo código 11. O próximo campo (o identificador) é usado para combinar com os pedidos e respostas entre si. Isso garante que várias conversas RADIUS não sejam misturadas, alterando quais mensagens vão para quais dispositivos. O campo Comprimento é usado para identificar o tamanho do pacote; como o pacote RADIUS pode ter até 2000 atributos dentro dele, é necessário um mecanismo para medir o tamanho do pacote. O último campo, o campo autenticador, é o campo em que a senha está protegida; esta senha é protegida por um mecanismo de *hash*.

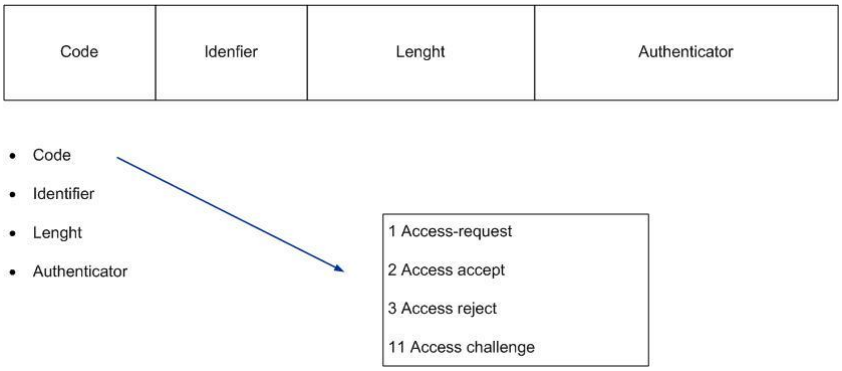


Figura 4.6-1 – Formato de um *frame* RADIUS

Ao olhar para o servidor RADIUS, bem como todos os servidores de autenticação que envolve este assunto, os detalhes que cercam a proteção do próprio servidor são muitas vezes esquecidas. Isto geralmente é proveniente das pessoas responsáveis pela construção e administração de redes - e não dos servidores. Isso acaba deixando o servidor RADIUS exposto. Por exemplo, a equipe responsável por construir e administrar redes na maioria das vezes não tem as habilidades necessárias para proteger os servidores. Pode-se ter a rede mais segura no mundo, no entanto se alguém tiver facilidades em invadir um servidor de autenticação, toda a rede será comprometida.

4.7 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Extensible Authentication Protocol (EAP) é um método padrão de autenticação para se obter acesso a uma rede. As modalidades de autenticação podem ser por certificados de segurança ou por senhas. Quando *Password Authentication Protocol* (PAP) surgiu pela primeira vez, questões de segurança logo o tornaram um método de autenticação dos menos desejáveis. Depois disso, o *Challenge Handshake Authentication Protocol* (CHAP) saiu e este também se viu rapidamente confrontado com questões de segurança. A indústria decidiu que era mais fácil fazer um protocolo de autenticação agir da mesma forma, não importando como ou que tipo

de validação de autenticação usaria. Isto significava que, pela primeira vez um protocolo poderia ser inserido em produtos e em softwares que permitiam senhas, *tokens* ou biometria, sem ter que escrever qualquer código extra para suportar os diferentes métodos. Trata-se de como e por que o EAP foi criado. Para usar o EAP, deve-se especificar dentro do campo tipo que espécie de autenticação será usada. EAP pode adaptar-se às questões de segurança e às mudanças, aproveitando os diferentes métodos de autenticação. EAP também é capaz de utilizar novas ou aperfeiçoar técnicas de autenticação sem ter de efetuar quaisquer alterações no equipamento EAP suportado.

Quando EAP foi criado, uma necessidade de compatibilidade com PPP foi exigido. Isso ajudou a garantir que uma grande base de equipamentos poderia suportar EAP sem grandes modificações. Para obter essa compatibilidade o EAP foi incluído como um tipo de *Point-to-Point Protocol* (PPP) dentro de um mesmo pacote PPP. Isto permitiu que qualquer dispositivo que suportasse PPP fosse capaz de suportar o EAP. O EAP permaneceu desta forma através da RFC 2284 [24]. Como EAP amadureceu e exigiu uma maior integração com o padrão 802.1x, seu posicionamento dentro de PPP foi avaliado. O resultado dessa avaliação foi a RFC 3748 [25]. O trecho da RFC 3748 citado abaixo é o raciocínio por trás das mudanças do EAP que eram necessárias para suportar o padrão 802.1x.

“O encapsulamento IEEE 802 do EAP não envolve PPP e IEEE 802.1x não inclui suporte para o link ou negociações na camada de rede. Como resultado, no IEEE 802.1x não é possível negociar mecanismos de autenticação não EAP, como o PAP ou CHAP [RFC1994]”.

Como se pode ver na Figura 4.7-1, o processo de EAP começa por dizer ao dispositivo que o método de autenticação PPP está sendo iniciado e que o método é EAP.

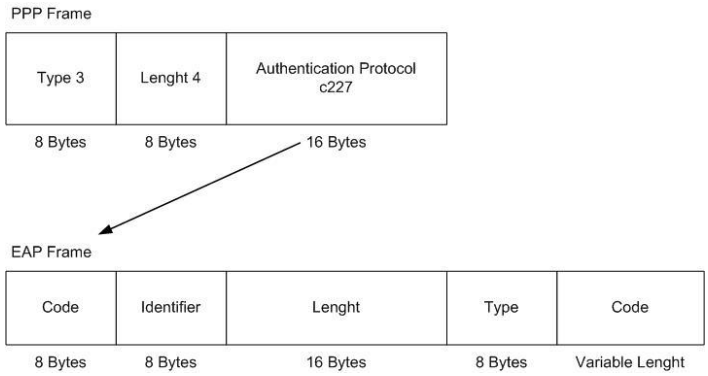


Figura 4.7-1 – Formato do *frame* PPP EAP

Olhando para a parte EAP do pacote em si, pode-se ver que é composta por quatro áreas principais: código, identificador, comprimento e dados. Estes campos são utilizados para identificar qual é a função do pacote, quanto tempo ele tem, e em quais negociações EAP o pacote pertence.

O EAP é capaz de suportar vários tipos de mecanismos de autenticação. Isto tem ajudado a EAP a não tornar-se obsoleto devido a vulnerabilidades de segurança ou fraquezas do protocolo. A capacidade de usar vários tipos de autenticação está localizada no campo Tipo de um pacote EAP. Hoje há vários tipos de EAP, alguns dos quais são específicos do fornecedor, alguns detalhados no padrão EAP, e algumas normas dentro de seus próprios documentos padrão. Outros são padrões da indústria por conta própria, detalhados por documentos IETF ou documentos RFC. Nas subseções abaixo os tipos EAP mais largamente utilizados por *wireless* são detalhados e analisados.

4.7.1 EAP-MD5

Extensible Authentication Protocol-Message Digest version 5 (EAP-MD5) é um dos tipos mais limitados de EAP incluídos na RFC EAP. Esta versão usa um algoritmo de *hash* MD para validar as credenciais do usuário. Alguns dos outros tipos de métodos EAP criam túneis criptografados e depois no interior desses túneis é que eles executam validação EAP-MD5. Uma das exigências do EAP MD5 é um segredo

compartilhado. Este segredo é usado para criptografar um desafio para verificar se a outra parte tem o mesmo segredo.

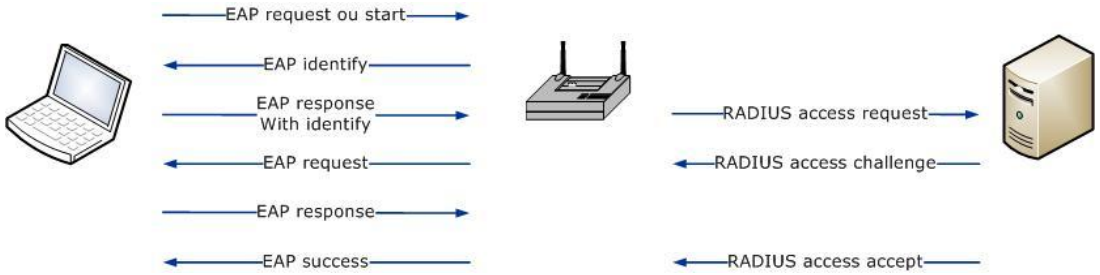


Figura 4.7-2 – Detalhe do EAP-MD5

Analisando a Figura 4.7-2 pode-se ver como EAP-MD5 funciona. O primeiro passo é o cliente enviar um pacote de solicitação ao ponto de acesso. Uma vez que o ponto de acesso ouve este pedido, ele irá responder, pedindo que o cliente forneça a sua identidade. A RFC 3748 para EAP permite que os itens de identificação sejam localizados na mensagem de identidade EAP, embora a principal função do campo identidade EAP seja informar ao servidor de autenticação que tipo de método EAP o cliente irá utilizar, e não para a identidade do usuário.

Continuando com o exemplo, o tipo de EAP dentro da seção de quadro de identidade EAP seria definido como MD5. Uma vez que o ponto de acesso receba esse código de identidade dentro do quadro da mensagem 2, ele irá enviá-lo para o servidor de autenticação. O servidor de autenticação então envia um desafio para o cliente. Este desafio é criptografado e enviado em formato de texto claro. Depois que o cliente recebe o desafio, ele usará o segredo compartilhado para criptografar o desafio e o enviará de volta para o servidor de autenticação. Uma vez que o servidor de autenticação recebe o desafio, ele irá executar a mesma operação que o cliente fez. Ele validará o *hash* comparando com o que o cliente enviou. Se isso for verdade, uma mensagem de sucesso EAP é enviada; se por algum motivo alguma coisa não estava correta, o servidor de autenticação envia uma mensagem de falha

com um código de razão. Esse código de razão ajudaria a compreender porque o quadro de EAP não foi aceito.

4.7.2 LEAP

Lightweight Extensible Authentication Protocol (LEAP) é um protocolo proprietário da Cisco Systems. O código do LEAP é ainda considerado de propriedade intelectual da Cisco Systems e está disponível para uso somente sob um acordo de não-divulgação (NDA - *non-disclosure agreement*).

LEAP funciona um pouco diferente dos principais tipos de EAP (Figura 4.7-3). O processo de EAP começa com o pedido do cliente voltado para o ponto de acesso. Quando o ponto de acesso ouve isso, ele irá enviar a resposta e pedir identidade. A maioria dos outros tipos de EAP só pede a identidade para o cliente EAP, LEAP irá responder com um nome de usuário no campo de identidade. Uma vez que o ponto de acesso ouve isso, ele irá encaminhar o pacote para o servidor de autenticação RADIUS na maioria dos casos. O servidor irá então enviar um desafio para o cliente através do ponto de acesso.

O desafio é composto de uma mensagem de 8 bytes. Quando o cliente ouve esta mensagem, ele irá realizar uma série de medidas para responder. Isso resultará em um número de operações DES, criando um texto cifrado, que é de 24 bytes. Este texto será enviado para o servidor de autenticação que irá fazer a mesma operação em sentido inverso e obter a senha original. Uma vez que ele tenha esta senha, ele vai se certificar de que as senhas combinam com a do usuário. Se uma correspondência for encontrada o servidor de autenticação envia uma mensagem *Access-Accept* ao ponto de acesso. Se não, o servidor de autenticação envia uma mensagem de rejeição ao ponto de acesso. O ponto de acesso, de acordo com a

mensagem, enviará uma mensagem de falha EAP ou de sucesso EAP para o cliente.

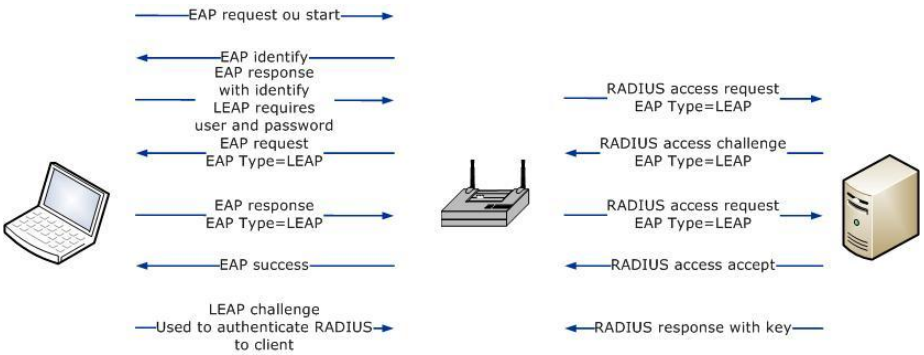


Figura 4.7-3 – Detalhes LEAP

4.7.3 EAP-TLS

O método *Extensible Authentication Protocol-Transport Layer Security* (EAP-TLS) é descrito no RFC 5216 e foi criado pela Microsoft em outubro de 1999. A RFC foi construída sobre os seguintes RFCs: RFC 2284 para PPP e RFC 2246 [26] para TLS. TLS surgiu a partir dos protocolos SSL mais velhos. A Netscape criou o *Secure Socket Layer* (SSL) e o utilizou para navegação segura na Web. Com o crescimento da Internet, atualizações para o SSL foram necessárias. Em 1996 o IEEE criou TLS baseado no SSL do Netscape e *Microsoft Private Communications Technology* (PCT). Este método EAP usa certificados para autenticar usuários e exigir certificados de servidor e de cliente final. Este método EAP específico é um dos mais fortes, embora ele não impeça o uso de quem está acessando a rede a partir de um computador com um certificado de cliente já instalado.

Configurar uma rede sem fio com 802.1x e EAP-TLS requer algum trabalho e planejamento. Primeiro, é preciso ter uma autoridade de certificação (CA), o servidor irá funcionar como distribuidor de certificados de cliente e servidor. Também seria necessário um servidor AAA que suporte o tipo EAP-TLS. Finalmente, será preciso um cliente que possa suportar este tipo de EAP. Uma vez que todas as peças

estejam no lugar, o próximo desafio será configurar corretamente cada peça para interagir.

Para compreender melhor o método EAP-TLS, apresentamos uma visão geral de alto nível do processo de autenticação com este método (Figura 4.7-4). Um pedido de pacote originário do cliente através do autenticador vinculado para o servidor de autenticação é feito. Uma vez que esta solicitação é recebida, o servidor de autenticação envia de volta uma resposta para o cliente e solicita a sua identidade. Em seguida, o cliente irá fornecer a identidade, solicitando o uso do EAP-TLS. Uma vez que esta é recebida, o servidor de autenticação irá enviar o respectivo certificado de chave pública para o cliente. Depois que o cliente recebe esta, ele irá responder com a sua chave pública e um canal seguro será criado. Isto é muito similar a como uma página da Web segura funciona, embora neste caso a validação do cliente é presente.

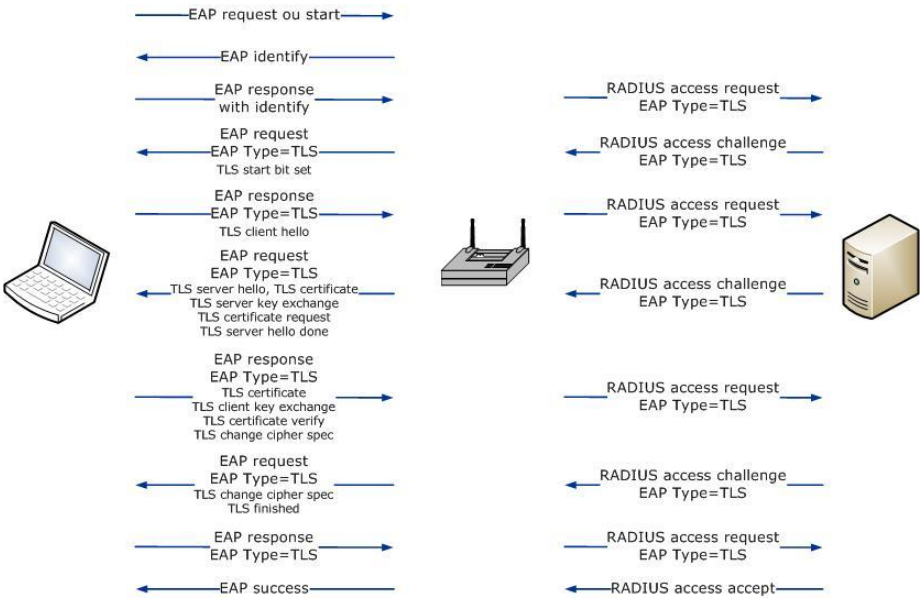


Figura 4.7-4 – Detalhes do EAP-TLS

Agora que ambos os lados foram autenticados uns pelos outros, outro processo EAP pode ter lugar dentro do túnel EAP-TLS para permitir que haja uma autenticação segura. Por exemplo, uma troca EAP-MD5 pode ter lugar dentro do túnel

criptografado, permitindo a autenticação mais fraca de segurança, porque está ocorrendo dentro de um túnel criptografado.

4.7.4 EAP-TTLS

O *Extensible Authentication Protocol-Tunnel Transport Layer Security* (EAP-TTLS) é um projeto de documento IETF criado por Funk Software Inc. A versão mais recente é chamada draft-ietf-pppext-EAP-TTLS-05.txt [27] e foi criada em julho de 2004. O raciocínio por trás da criação de um novo tipo EAP era baseado em uma oportunidade que a Funk Software viu no mercado. Esta oportunidade foi uma necessidade de oferecer suporte a dispositivos mais antigos que não foram capazes de realizar os novos tipos de autenticação. Este tipo de EAP ajudou a Funk Software oferecer soluções seguras para os equipamentos clientes sem fio mais antigos.

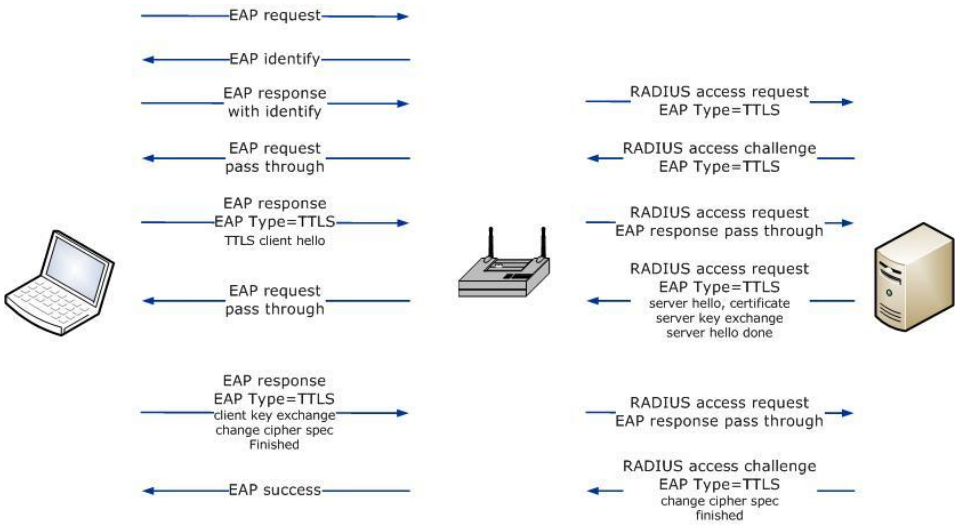


Figura 4.7-5 – Detalhes do EAP-TTLS

O método EAP-TTLS (Figura 4.7-5) funciona através da tomada de autenticação e protegendo-a dentro de um túnel TLS, no entanto, ao contrário do EAP-TLS, EAP-TTLS pode usar tipos de autenticação fora do EAP por parte de autenticação do cliente, como PAP, CHAP, MS-CHAP, MS-CHAP-V2, e muitos outros. O cliente

envia um pacote de solicitação. Esse pacote origina do cliente através do autenticador vinculado para o servidor de autenticação. Uma vez que este pedido é recebido, o servidor de autenticação envia de volta uma resposta para o cliente que solicita a sua identidade. Em seguida, o cliente irá fornecer identidade, solicitando o uso do EAP-TLS. Uma vez que esta é recebida, o servidor de autenticação irá enviar o respectivo certificado de chave pública para o cliente. Uma configuração opcional é o cliente enviar um certificado para validar que é o cliente correto.

É importante observar que o principal ponto do EAP-TTLS é aproveitar equipamentos antigos, que não podem usar métodos avançados de autenticação como o *Public Key Infrastructure* (PKI). Se alguém vai usar ou já tem PKI, EAP-TLS seria a melhor opção. Uma vez que o cliente recebe o certificado do servidor de autenticação, ele irá usar o EAP-TTLS para configurar um canal seguro através do autenticador entre ele e o servidor de autenticação. Isso é feito usando TLS e a chave pública do servidor de autenticação. Quando este processo estiver completo, vários outros tipos de autenticação padrão podem ter lugar dentro deste túnel TLS. Este é o momento onde o EAP-TLS e EAP-TTLS diferem, no EAP-TLS tudo o que poderia ser feito neste momento é a realização de outro tipo de EAP, como EAP-MD5 já dentro do canal EAP configurado. Com o EAP-TTLS pode-se usar outras formas de autenticação que não são possíveis no dispositivo que não suporte EAP.

4.7.5 PEAP

Protected Extensible Authentication Protocol (PEAP) foi criado como um esforço conjunto entre a RAS, a Microsoft e a Cisco Systems. Atualmente, o PEAP está em um projeto chamado IETF draft-josefsson-pppext-eap-tls-eap-10.txt [28], última atualização em outubro de 2004. Devido ao fato de que ele ainda existe em forma de projeto, as atualizações podem mudar seu número de versão ou o nome do

documento. PEAP foi uma jogada da indústria para fazer um único método EAP que múltiplos fornecedores poderiam compartilhar. Os três fabricantes que criaram o padrão implementaram, cada um a sua própria maneira, o que fez as versões PEAP da Microsoft e da Cisco diferentes e não interoperáveis. Este trabalho foi lentamente sendo alterado, embora não se espere uma fácil integração ao tentar usar os métodos PEAP da Microsoft e da Cisco alternadamente.

Uma das principais vantagens do PEAP é a capacidade de ter um tipo de EAP forte que não necessita de certificados de cliente, como o EAP-TLS. PEAP funciona semelhante ao EAP-TLS, criando um túnel criptografado com TLS e depois realiza outro método EAP dentro deste túnel criptografado. Ao contrário do EAP-TLS, PEAP quando executa este processo, não valida um certificado de cliente. Isto é onde a Cisco e Microsoft são diferentes, cada um deles utiliza um método diferente depois que a conexão TLS é criada.

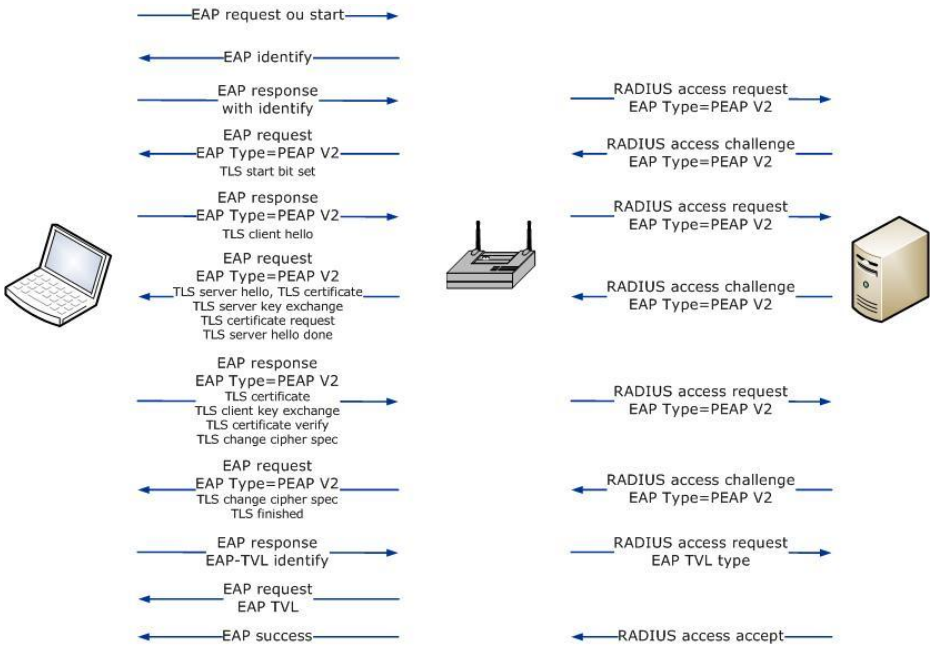


Figura 4.7-6 – Detalhes PEAP

O processo de PEAP (Figura 4.7-6) inicia semelhante ao de outros processos EAP com um pacote de solicitação enviada para o ponto de acesso. Uma vez que o ponto

de acesso ouve esta solicitação, ele irá responder com um pacote de resposta. Essa resposta também vai pedir ao cliente a sua identidade. A identidade será o tipo de EAP, neste caso, será mostrado um campo EAP-Type = PEAP no quadro. Isso irá instruir o servidor de autenticação EAP que o método a ser utilizado será o PEAP. Uma vez que o método EAP foi determinado, um túnel TLS é criado utilizando o certificado do servidor de autenticação para estabelecer o túnel TLS. Logo após, um novo processo de EAP acontece no interior do túnel para autenticar o cliente. Se alguém estiver usando a versão Microsoft PEAP, será utilizado MSCHAPv2 como um tipo de EAP. Este método EAP é definido no documento IETF chamado draft-Kamath-pppext-EAP-mschapv2-01.txt [29], que tem a sua versão mais recente publicada em dezembro de 2007.

4.7.6 EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) é um documento IETF criado pela Cisco Systems em fevereiro de 2004. O presente documento é chamado draft-cam-winget-eap-fast-00.txt, e hoje já se tornou uma RFC e está localizado no site do IETF. A Cisco teve algumas falhas de segurança publicadas sobre o seu método LEAP e em vez de corrigi-las, eles abandonaram o padrão proprietário e criaram este método EAP. Este método EAP suporta um tempo de *roaming* rápido comparado com outros padrões EAP. Este tempo era um requisito crítico para muitas empresas que têm telefones Wi-Fi ou alguma aplicação sensível a tempo. Isso fez a Cisco Systems necessitar de um método EAP rápido, seguro para autenticação sem fio.

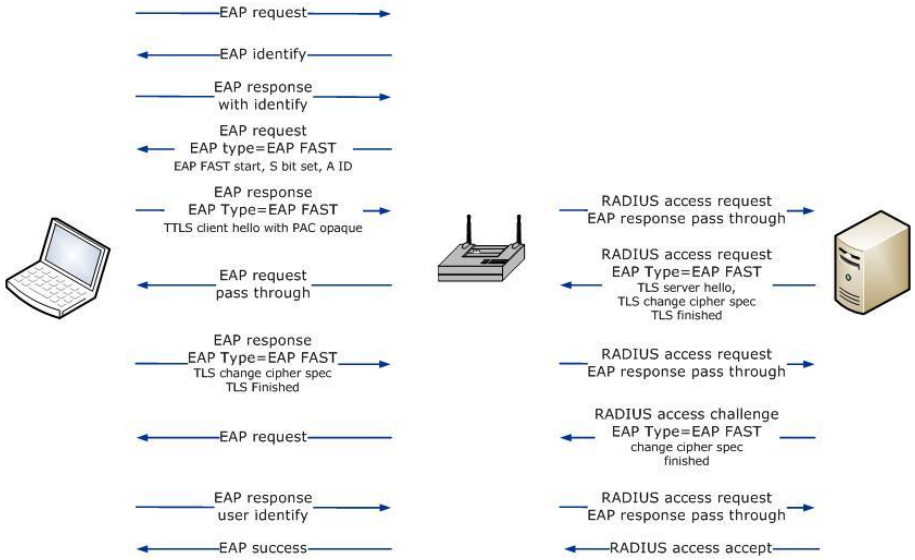


Figura 4.7-7 – Detalhes EAP-FAST

O método EAP-FAST (Figura 4.7-7) trabalha com o que se chama uma credencial de acesso protegido (PAC - *protected access credential*), que é semelhante a um certificado. O PAC é uma chave que é usada para criar um túnel criptografado entre o cliente e o servidor de autenticação. Essa chave tem a capacidade de ter as chaves dinamicamente alocadas. Este processo PAC de alocação dinâmica é chamado de auto-abastecimento. Ao se tomar a decisão de utilizá-lo, ele funcionará através da criação de uma conexão TLS e passará credenciais MSCHAP V2 para acessar a rede. É interessante observar que a sessão TLS só é autenticada pela chave pública do servidor. Após a conexão inicial à rede ser feita, um novo PAC pode ser enviado para este canal encriptado. Outra abordagem é usar troca de chaves em separado. Para fazer isto a mesma chave é validada tanto no usuário como no servidor final. Para contornar os problemas de gestão de chaves, o PAC tem a capacidade de mudar em intervalos específicos, uma vez que uma ligação segura tenha sido estabelecida.

Com o PAC criado ou introduzido, o processo EAP pode começar. Tal como acontece com os outros processos EAP, este começa da mesma forma com o

pacote de solicitação do cliente. O ponto de acesso responde à solicitação e uma resposta é enviada de volta pedindo identidade. O cliente então envia sua identidade. Este pedido de identidade apenas solicita o uso do EAP-FAST. Uma vez que o ponto de acesso ouve este pedido de identidade, ele vai responder com um pedido de EAP para enviar o PAC do cliente. Essa mensagem com o PAC vai ser passada para o servidor de autenticação. O servidor de autenticação, então, envia uma autoridade de identificação, que é um campo dentro do PAC. Este campo identifica o PAC correto de uma lista de clientes de PAC. Depois que o cliente ouve a autoridade ID e compara com o PAC correto, ele pode começar a criar um túnel TLS com base na chave principal para esse PAC. Isto irá criar um túnel que pode ser usado para executar a autenticação adicional.

4.8 WI-FI PROTECTED ACCESS (WPA)

Wi-Fi Protected Access (WPA) tem uma história interessante em relação à forma como ele se tornou um padrão. Quando a segurança do WEP foi quebrada, a indústria voltou-se para o IEEE para corrigi-lo. O IEEE disse que iria criar o padrão de segurança *wireless* 802.11i. Este padrão se arrastava e era muito lento o seu desenvolvimento. Com esta demora, as vendas dos dispositivos wireless despencaram. Este declínio foi devido à falta de um método padrão seguro para redes sem fio. Com isto, os fabricantes de redes sem fios começaram a pressionar o IEEE e outros órgãos responsáveis pelos padrões para ratificar algo e que eles pudessem produzir produtos seguros dentro destas normas. Com o adiamento da data de lançamento do 802.11i, a Wi-Fi Alliance decidiu que iria criar um subconjunto 802.11i chamado WPA. Isso significava que as grandes mudanças no padrão 802.11i influenciariam as futuras versões do WPA. Isto foi visto com o WPA e WPA2. Hoje, com 802.11i completo, o uso do WPA tem diminuído substancialmente.

O padrão WPA suporta dois métodos de autenticação e gerenciamento de chaves. O primeiro é autenticação EAP com o padrão 802.1x. Esse método funciona através da utilização do protocolo 802.1x e um servidor *back-end* de autenticação. Ele aproveita EAP para autenticação no ar e RADIUS para autenticação de *back-end*. Esse método é o mais seguro dos dois e gera um menor valor final de administração do cliente.

A outra opção disponível é usar chaves pré-compartilhadas. Esta opção requer que uma chave seja aplicada nos aparelhos e nos pontos de acesso sem fio. Isto significa também que tudo tem a mesma senha inserida. Para lutar contra alguém que use essa chave para escutar conversas dos outros, o WPA usa um método que cria uma chave de sessão única para cada dispositivo. Isto é feito com uma chave denominada de chave mestre de grupo (GMK) que contém um par de chaves transitório (PTK). Como isso funciona, será explicado na seção sobre 802.11i. Esta segunda solução foi adicionada ao WPA para suportar o uso em ambientes domésticos e pequenos escritórios, onde é pouco provável que exista um servidor de autenticação como o RADIUS.

WPA suporta TKIP e MIC para dispositivos mais antigos, assim como AES, embora o método que ele use seja um pouco diferente da definida no 802.11i. Ele tem a maioria das características abordadas na seção 802.11i. Algumas delas incluem a capacidade de negociar um conjunto de codificação ou um método de autenticação de elementos de informação com segurança de rede robusta (RSN).

Com o padrão WPA usando praticamente o que já tinha sido terminado para o IEEE 802.11i, algumas mudanças foram necessárias para poder criar esta norma provisória. Essas mudanças levaram a uma série de diferenças entre as duas normas.

A primeira grande diferença é que WPA suporta TKIP por padrão. Isso é diferente no 802.11i, que suporta AES CCMP por padrão. O WPA não suporta AES CCMP, no entanto, suporta AES, não apenas na variação que o 802.11i utiliza. O último ponto importante que diferencia WPA de 802.11i é o RSN IE. Este é usado para passar as configurações de codificação suportadas entre os pontos de acesso sem fio e os clientes. Em 802.11i, esta parte não foi bem definida para que o padrão WPA tivesse que criar algumas regras novas, sem afetar-lhes qualquer coisa que fosse feito para o IE RSN pelo grupo de trabalho 802.11i. Isto foi conseguido através da criação de um IE WPA e com valores diferentes para distingui-las umas das outras. Isso ajudou no fato de que, quando o IE RSN foi definido, não foi difícil colocá-lo em WPA.

4.9 802.11i

O padrão de segurança 802.11i surgiu em resposta a uma necessidade de melhorar a segurança das redes 802.11 para um nível suficiente, que justificasse as redes sem fio como um meio de transporte seguro e de aceitação geral. Nesse padrão, o IEEE definiu uma forma segura de acessar redes sem fio, tentando atenuar a enorme quantidade de ameaças que faziam a rede sem fio um risco real para as empresas.

Em julho de 1999 houve um grande interesse no reforço da camada MAC do 802.11 para a qualidade de serviço (QoS). Isto gerou gás suficiente para criar o grupo de trabalho TGe em março de 2000. Depois de um ano, foi determinado que esse grupo precisava ser dividido em um grupo de segurança e um grupo de QoS, devido à enorme carga de trabalho. Essa divisão de segurança criou o grupo de trabalho TGi. Este grupo criou o padrão 802.11i e o colocou para aprovação por votação. Esta aprovação tomou uma série de projetos ao longo de um período de três anos. Uma vez feito isso, conseguiu-se grupos de patrocinadores e, finalmente, o processo de

aprovação da norma padrão. Em 24 de junho de 2004 o corpo de normas finalmente aprovou o padrão 802.11i.

Observando o 802.11i, percebe-se que ele usa uma série de normas, protocolos e cifras que já foram definidos fora do 802.11i. Um certo número de normas também é definido no seu conjunto, como RADIUS, 802.1x, EAP, AES, RSN, TKIP e alguns outros padrões, que são parte do padrão 802.11i. Alguns deles são definidos dentro de seus próprios documentos e alguns deles são oficialmente criados dentro do documento do 802.11i.

Uma outra parte do padrão 802.11i é a habilidade para usar o EAP. Foi determinado que o padrão 802.11i não especificaria um método ou tipo de autenticação, mas permitiria um protocolo que poderia realizar vários tipos de autenticação dentro de si. Isto é exatamente o que faz EAP, que permite o uso de vários tipos diferentes de autenticação de senhas, smart cards, certificados e muitos outros, com base nos mesmos métodos de *request*, *accept* e *reject*.

Para o EAP funcionar corretamente com o padrão 802.11i, uma outra norma conhecida deve facilitar a transmissão de EAP entre entidades não confiáveis e de confiança. Isso é onde o 802.1x se encaixa no padrão, seu objetivo principal é fornecer um quadro de forte autenticação e gerenciamento de chaves. O protocolo 802.1x permite ao ponto de acesso permitir apenas um pedido de EAP para a rede. Este é o caso até que o cliente esteja devidamente autenticado. Uma vez autenticado, ocorre a negociação de chaves e, posteriormente, o acesso à rede pode ser alcançado.

Como incluído no WPA, o padrão 802.11i necessitava de uma opção para ambientes em que um servidor de autenticação não era financeiramente viável. Este servidor de autenticação foi uma exigência da norma 802.1x. Para tornar o 802.11i viável

tanto para grandes empresas como para usuários *small office*/*home office* (SOHO), um outro método era necessário. Esta foi a origem da criação do método de chave pré-compartilhada. Isto é muito semelhante ao WPA e seu método de chave pré-compartilhada. Quando uma chave pré-compartilhada é usada, cada cliente utiliza um segredo para criar um material de chaves subsequentes. Esta chave mestra é a mesma em toda a rede, como WEP, embora seja usada para criar uma sessão com chave para cada cliente.

As subseções abaixo descrevem as normas que estão localizadas dentro do padrão 802.11i.

4.9.1 Robust Secure Network (RSN)

Robust Secure Network (RSN) foi criado como parte do padrão de segurança 802.11i. RSN especifica a autenticação do usuário através de IEEE 802.1x e a criptografia de dados através do *Temporal Key Integrity Protocol* (TKIP) e *Counter Mode* com *CBC-MAC Protocol* (CCMP). RSN também tem a opção de usar TSN para permitir a utilização de métodos mais antigos de segurança, como WEP. TSN é explicado na Seção 4.9.1.1.

RSN usa TKIP e AES como métodos de criptografia para proteger a confidencialidade dos dados. TKIP é usado para compatibilidade com versões para dispositivos legados e AES é como um método de criptografia de longo prazo. AES está configurado no *Counter Mode* com o CCMP. 802.11i sugere que a AES deve ser utilizado em um método CCMP. O protocolo RSN também utiliza mensagens EAPOL-Key para o gerenciamento de chaves. A descrição abaixo revela como RSN trabalha com 802.11i visando ajudar a escolher métodos de autenticação disponíveis e esquemas de codificação de encriptação.

O anuncio dos conjuntos de codificação suportados em um ponto de acesso e no cliente é feita através de mensagens da *Robust Secure Network Association* (RSNA). Essas mensagens anunciam as cifras suportadas por cada parte e negociam que método será usado para conectar de forma segura. Estas mensagens estão localizadas dentro do que é chamado um RSN IE ou um elemento de informação RSN. O RSN IE pode ser enviado em um *beacon* de um ponto de acesso ou de um pedido de associação de um cliente. Após um pedido de associação, uma resposta será devolvida com um anúncio RSN IE listando que métodos correspondem ao método suportado pela outra parte.

O padrão permite RSN IE, opcionalmente, de estar dentro de cada um dos seguintes tipos gerenciamento de frames:

- Beacon
- Association Request
- Reassociation Request
- Probe Response

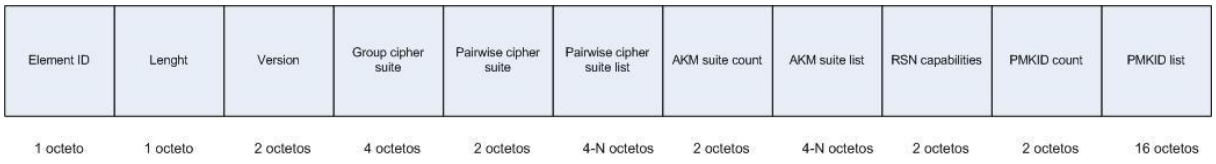


Figura 4.9-1 – Detalhes do frame RSN-IE

Observando a Figura 4.9-1, podem-se ver as muitas peças que compõem um quadro RSN IE. Das 11 seções desse quadro, apenas as três primeiras são exigidas em todas as transmissões RSN IE.

- *Element ID*
- *Lenght*
- *Version*

No RSN, a preocupação é apenas em informar à outra parte que conjuntos de codificação são suportados. Uma vez que tenha sido realizado, pode-se decidir se é

possível negociar um conjunto de codificação ou método comum entre ambas as partes. No *frame* RSN *Cipher Suite* existem seis conjuntos de codificação especificados e um número de reserva e conjuntos de codificação de fornecedores específicos que podem ser usados no futuro.

Tabela 4-3 – Detalhes do frame de conjunto de cifras

OUI	Suite Type	
3 octets	1 octet	
OUI	Suite Type	Meaning
00:0F:AC	0	Usa grupo de cifras
00:0F:AC	1	WEP 40
00:0F:AC	2	TKIP
00:0F:AC	3	Reservado
00:0F:AC	4	CCMP
00:0F:AC	5	WEP 104
00:0F:AC	6-255	Reservado
Vendor OUI	Other	Fabricante especifico
Other	Any	Reservado

Estes conjuntos de codificação permitem a utilização de qualquer combinação de métodos de segurança. Isto significa que pode ser posta em prática uma política que nega o uso de métodos mais fracos de segurança, como WEP e permite a escolha de TKIP ou AES.

4.9.1.1 Transition Secure Network (TSN)

A Rede de Transição Segura (*Transition Secure Network* - TSN) faz parte da porção RSN do 802.11i. É utilizado para manter a compatibilidade com versões anteriores de sistemas de redes sem fio. Foi esculpida em RSN para fornecer essa compatibilidade. Para certificar-se que alguns dos tipos mais fracos de autenticação e criptografia não foram configurados em RSN, eles foram retirados e considerados TSN. Isto faz RSN mais seguro e permite uma maneira fácil de desativar todos os métodos mais fracos. Com RSN, se não optar por suportar TSN, WEP não será incluído como uma opção para negociar entre o ponto de acesso e o cliente sem fio.

4.9.2 Temporal Key Integrity Protocol (TKIP)

O *Temporal Key Integrity Protocol* (TKIP) foi uma solução transitória desenvolvida para resolver o problema da reutilização da chave WEP. Ele mais tarde se tornou parte do 802.11i e, posteriormente, parte das normas WPA.

TKIP foi incluído no padrão 802.11i para manter compatibilidade com versões anteriores. O padrão 802.11i não queria usar uma cifra baseada em RC4, por isso foi escolhido AES (Seção 4.9.3). TKIP foi colocado em 802.11i pela simples razão de ajudar os dispositivos mais velhos na transição para o 802.11i. Uma das principais razões para usar o TKIP ao invés do WEP veio do aumento da segurança e do número crescente de ataques que assolaram o protocolo WEP. Usando TKIP aumenta-se a proteção contra estes ataques e reduz-se o risco global da exploração de uma rede sem fio.

A norma TKIP também teve valor na indústria, pois a migração de WEP para TKIP foi fácil. Na maioria dos casos, passar de WEP para TKIP envolvia apenas uma pequena mudança de firmware, o que significava que nenhum hardware precisaria ser trocado e também que a maioria dos dispositivos antigos, que já tinham sido comprados, seria capaz de atualizar para o TKIP.

A Cisco, assim como outros fornecedores, também criou soluções baseadas em TKIP antes que o padrão fosse ratificado.

A parte de criptografia TKIP funciona em um processo de duas fases. A primeira fase gera uma chave de sessão de uma chave temporária, um contador sequencial TKIP (TSC), e o endereço MAC do transmissor. A chave temporária é composta de um valor de 128 bits, semelhante ao da base de valor da chave WEP. O contador sequencial TKIP (TSC) é composto do endereço de origem (*Source Address* - SA), endereço de destino (*Destiny Address* - DA), prioridade, e o *payload* ou dados. Uma

vez concluída esta fase, um valor chamado de TKIP-*mixed transmit address and key* (ttak - transmissão mista de endereço e chave) é criado. Esse valor é usado como uma sessão baseada em chave WEP na segunda fase.

Na segunda fase o ttak e IV são utilizados para produzir uma chave que criptografa os dados. Isto é semelhante à forma como o WEP é processado. No WEP os primeiros 24 bits do IV são adicionados na frente da chave WEP e então usados para criar uma chave de encriptação que é aplicada nos dados. TKIP estendeu o espaço IV, adicionando 24 bits. Na segunda fase os primeiros 24 bits são preenchidos com os 24 bits do ttak. Os próximos 24 bits são preenchidos com a porção não utilizada da TSC. Isto é mais seguro que o WEP pois a chave está usando um valor diferente, dependendo com quem se está falando. No WEP cada cliente ou ponto de acesso cria o mesmo valor aleatório. Alguns produtos nem mesmo criaram um valor aleatório e apenas incrementaram o valor em um, tornando-o um alvo fácil para os hackers.

A base de TKIP veio do protocolo WEP. No padrão 802.11i, TKIP é referido como um conjunto de codificação de reforço do protocolo WEP em *hardwares* pré-RSNA. Isto é defendido porque RC4 ainda é usado como uma cifra, embora a técnica em que é utilizada tenha melhorado muito.

4.9.2.1 TKIP Message Integrity Check (MIC)

Parecido com o TKIP, o *Message Integrity Check* (MIC) também teve muitas versões antes do 802.11i o ter definido como um padrão único. O próprio protocolo foi criado para ajudar a lutar contra os muitos ataques de modificações de mensagem que eram predominantes no protocolo WEP. O padrão IEEE 802.11i descreve a necessidade do MIC na seguinte citação:

"Falhas no projeto IEEE 802.11 WEP fizeram com que ele deixasse de cumprir com seu objetivo de proteger o conteúdo do tráfego de dados de bisbilhoteiros casuais. Entre as falhas mais significativas do WEP está a falta de um mecanismo para derrotar mensagens falsificadas e outros ataques ativos. Para se defender contra ataques ativos, TKIP incluiu um MIC, chamado Michael".

O MIC foi criado como um método mais seguro de tratamento de verificação de integridade em relação ao IVC no WEP.

O MIC é um *hash* que é calculado sobre uma base por pacotes. Isto significa que um único MIC *hash* poderia abranger vários quadros e lidar com a fragmentação. O MIC é baseado no valor inicial (*seed value*), MAC de destino, MAC de origem, prioridade, e *payload*. Ao contrário do IC, MIC usa um algoritmo de *hash* para carimbar o pacote, dando a um atacante uma chance muito menor para modificar um pacote e que ele ainda consiga passar o MIC. O valor inicial é semelhante ao IV do protocolo WEP. TKIP e MIC utilizam o mesmo espaço IV, apesar de ter adicionado quatro octetos para ele. Isto foi feito para tornar a ameaça do uso do IV duas vezes em um curto período de tempo menos provável.

O MIC é criptografado também dentro da porção de dados, o que significa que não pode ser obtido através de um *sniffer wireless*. Para adicionar a isto, o TKIP também deixou o processo WEP IVC, que adiciona um segundo método menos seguro, de verificação de integridade de todo o quadro. Para combater os ataques de modificação de mensagens, TKIP e MIC foram um passo além e introduziram os procedimentos TKIP de contra-ataques. Este é um mecanismo destinado a proteger contra os ataques de modificação. Ele funciona da seguinte maneira: um ponto de acesso encerra suas comunicações se duas falhas MIC ocorrerem em 60 segundos. Neste caso, o ponto de acesso seria fechado por 60 segundos. Quando ele estiver de volta, seria necessário que todos os clientes que tentarem reconectar mudassem

suas chaves e passassem por uma *re-keying*. Alguns fornecedores permitem a definição desses limites, embora o padrão MIC anuncie estes valores.

Para evitar riscos de desencadear um processo de contra-ataques TKIP, o processo de validação MIC é realizado após uma série de outras validações. As validações realizadas antes dos contra-ataques de validação MIC são a soma de verificação de quadro (FCS), soma de verificação de integridade (ICV), e o contador de sequência TKIP (TSC). Se o ruído vier a interferir com o pacote e modificá-lo, um desses outros controles seria capaz de encontrá-lo primeiro, evitando assim o *frame* de incrementar o contador de contra-ataques MIC.

4.9.3 Advanced Encryption Standard (AES)

Pode-se aplicar AES de muitas maneiras diferentes. A maneira que o padrão 802.11i optou por aplicar a AES é com CCMP, que se baseia na CBC-MAC. CCMP foi escolhido para a integridade dos dados e autenticação, com o *Message Authentication Code* (MAC) fornecendo a mesma funcionalidade que o *Message Integrity Check* (MIC) tem para TKIP. Antes de nos aprofundar no CCMP, é preciso olhar para AES e alguns de seus modos. O primeiro termo é CTR, que é o AES no modo contador. Esta modalidade é usada para confidencialidade. Outro modo é chamado CBC-MAC, que está para o modo *Cipher Block Chaining Message Authentication*. Este modo é usado para integridade. AES também foi combinado com CTR e CBC-MAC para criar o CCM. CCM é a sigla para o modo CTR / CBC-MAC de AES, que incorpora tanto a confidencialidade do CTR quanto a integridade do CBC-MAC.

4.9.4 802.11i - Visão Geral do Sistema

Depois de consultar cada parte que compõe o padrão 802.11i, podemos agora olhar para ele como um todo. Veremos como o cliente se conecta ao ponto de acesso, autentica, e negocia chaves. Cada uma dessas etapas aproveita as normas descritas até agora.

O cliente em primeiro lugar precisa fazer uma conexão com o ponto de acesso. Isso aconteceria através do processo normal de autenticação de chave aberta (*open key*) (Seção 4.1). Contrariamente à maioria dos padrões 802.11, 802.11i apenas permite a autenticação de sistema aberto, em função da descoberta de uma falha de segurança na autenticação de chave compartilhada.

Após o pedido de requisição inicial, o cliente teria de ouvir um *broadcast* RSN IE ou enviar um pedido de teste com um RSN IE. Seja como for que este quadro RSN IE é enviado, os clientes e os pontos de acesso têm a necessidade de negociar um conjunto de codificação para uso. Após o envio dos quadros RSN IE e chegar a uma negociação, o processo EAP começa. Isto pode começar com o ponto de acesso enviando um pedido de identidade EAP ou um cliente enviando um EAPOL *Start frame*. Com o processo EAP iniciado, ele irá passar pelo processo de autenticação EAP associado a cada tipo de EAP em particular. Este processo é descrito na Seção 4.7. Ele termina quando o cliente recebe uma mensagem de sucesso EAP do ponto de acesso. Durante este processo, uma chave AAA é enviada do servidor de autenticação para o dispositivo sem fio final. Essa chave é usada como uma chave inicial para criar as chaves descritas a seguir.

O processo de troca de chaves usa o frame original 802.1x EAPOL-Key e faz algumas modificações, permitindo a utilização do WEP-40, o WEP-104, TKIP e suites de cifra CCMP. Da seção 802.1x, o quadro EAPOL-Key só suporta WEP-40 e

as chaves WEP-104. O padrão 802.11i modificou isto e adicionou a capacidade para o *frame* também levar as chaves TKIP e CCMP. Um processo conhecido como *four-way handshake* realiza esta troca de chaves. Esse processo usa duas chaves principais e cria um único grupo e chaves de sessão para cada cliente. Estas chaves de sessão e grupo são criadas a partir das duas chaves principais: (1) a chave de pares ou a chave mestra em pares (PMK) e (2) a chave de grupo ou a chave mestra do grupo (GMK).

Em uma configuração 802.1x 802.11i, o PMK vem do servidor de autenticação. Se a configuração 802.11i está usando chaves pré-compartilhadas, então o PMK é mapeado para uma senha. O PMK é dividido em três chaves. A primeira chave é a chave de confirmação EAPOL-Key (KCK), que é usada para fornecer dados de autenticidade de origem. A segunda chave criada a partir do PMK é o EAPOL-Key chave de criptografia (KEK), que é usada para garantir a confidencialidade. A última chave é chamada chave temporal emparelhada (*pairwise temporal keys* - PTK) que é usada também para a confidencialidade dos dados. Para criar a PTK, uma pseudo função randômica ocorre com o endereço MAC do ponto de acesso, o endereço MAC do cliente, e um de uso único enviado de cada lado. Isso permite que uma única chave mestre crie múltiplas chaves de sessões, sem ter que trocar uma nova chave mestre a cada vez.

A próxima chave no que diz respeito a chaves principais 802.11i é a chave de grupo ou chave mestra de grupo (GMK). Esta chave é semelhante ao PMK, exceto que é utilizada para o *beacon* e a gestão do tráfego de criptografia. O mesmo processo de *hashing* de endereços MAC de remetentes e receptores é usado para criar uma chave de grupo temporal (GTK) de uma chave mestra do grupo (GMK).

Tendo discutido as chaves e como elas são divididas para acomodar a criptografia de sessão, olharemos o *four-way handshake*. Este *handshake* inicia-se com o autenticador enviando ao requerente um *nonce* (*number used once*). Isso é muitas vezes entendido como um ANonce (*Ap nonce*) no padrão 802.11i. Este *nonce* é um valor aleatório utilizado para prevenir ataques de replay, descartando *nonces* antigos.

Depois que cada parte recebe uma mensagem, o primeiro passo antes de qualquer outro é o de verificar se o *nonce* foi alterado ou incorretamente reutilizado. Depois que o cliente recebe a primeira mensagem, ele irá verificar o *nonce,* e, em seguida, gerar um SNonce (*STATION nonce*). Este SNonce será utilizado na próxima etapa para calcular o par de chaves transitória (PTK). Após o PTK ser criado, o cliente irá enviar o SNonce, bem como os parâmetros de segurança descritas no quadro RSN IE ao ponto de acesso. Esta informação é a segunda mensagem no *four-way handshake*. Toda esta informação será criptografada usando a KCK, que irá protegê-la de qualquer alteração, enquanto ela estiver em trânsito. Uma vez que o ponto de acesso recebe esta, irá verificar que o *nonce* não é um valor antigo. Uma vez feito isso, ele também irá gerar o PTK da SNonce e ANonce e, em seguida, verificar a KCK para ter certeza que não foi modificada em trânsito. Após isto, a terceira mensagem do *four-way handshake* ocorrerá. Esta mensagem é usada para dizer ao cliente para instalar a chave PTK que foi criada e, se usada, esta mensagem vai enviar um GTK para o cliente instalar. Uma vez que o cliente recebe isso, ele irá verificar a KCK e, se estiver correto, instalar a chave ou as chaves. A última mensagem é uma confirmação usada para permitir ao autenticador saber que o cliente instalou com êxito as chaves e está pronto para se comunicar com eles. A figura 4.9-2 mostra como este *four-way handshake* ocorre.

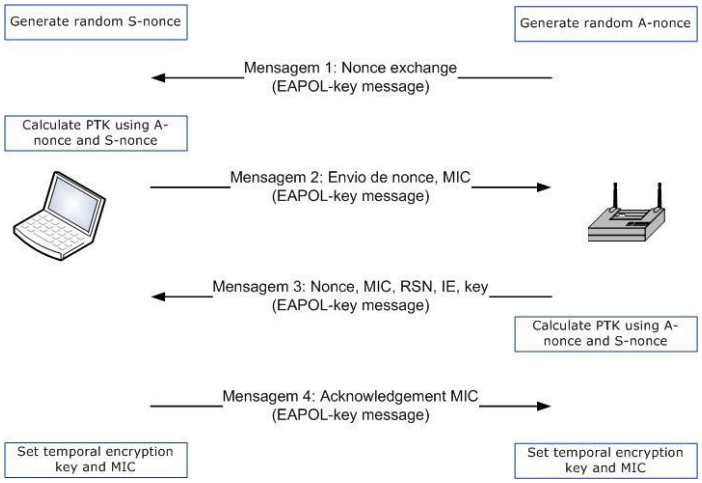


Figura 4.9-2 – 802.11 Four-way handshake

4.10 WI-FI PROTECTED ACCESS (WPA2)

Após o anuncio do 802.11i, o *Wi-Fi Alliance* queria continuar o investimento inicial feito em WPA. Isso criou um problema porque com o padrão 802.11i lançado, ter uma outra norma não era o que a indústria precisava. Para manter WPA em utilização, a *Wi-Fi Alliance* decidiu que iria voltar para o benefício central que a organização fornecia - padrão de testes de interoperabilidade e certificação. Ao criar WPA2, a *Wi-Fi Alliance* fez desta versão do WPA uma marca de interoperabilidade similar ao Wi-Fi. Esta marca garante que qualquer produto com ela tem um padrão 802.11i interoperável.

4.11 WLAN AUTHENTICATION AND PRIVACY INFRASTRUCTURE (WAPI)

A China decidiu que o 802.11i estava levando muito tempo e eles acharam melhor criar seu próprio padrão. Mesmo com 802.11i já lançado, a China ainda queria ter sua própria abordagem. Isto levou à criação do padrão WLAN *Authentication and Privacy Infrastructure* (WAPI). Esta norma tem muitas semelhanças com 802.11i, tais como RADIUS e 802.1x. Obter qualquer informação sobre esta norma é uma

violação de segurança nacional da China na Diretiva de Estado do Conselho Chinês 237, que regulamenta cifras de criptografia comerciais e exige tecnologia de criptografia para ser desenvolvida e vendida sob total sigilo.

Para vender produtos WLAN dentro da China, fornecedores de equipamentos estrangeiros precisam de licença WAPI através de um acordo com uma das 24 empresas chinesas com direitos concedidos pelo governo chinês. Esta tem sido uma dura tarefa em vendas para muitos líderes da indústria como Broadcom, Texas Instruments, Intersil, Atheros, e muitos outros. O governo chinês pediu-lhes para disponibilizar toda a propriedade intelectual envolvida em seus *chipsets*. Essa propriedade intelectual faz destas empresas serem líderes de mercado e para vender na China, eles poderiam perder isso. Como se poderia supor, muitas dessas empresas não estão correndo este risco.

5 CONCLUSÃO

Após analisar cada tipo de tecnologia, podemos concluir que existem vários métodos de se fornecer segurança em ambientes *wireless*. Cada método deve ser analisado e estudado para se ter certeza de que este atenderá ao seu tipo de ambiente. Não existe o método perfeito, e sim aquele que se adapta melhor ao seu tipo de necessidade.

Regras básicas devem ser seguidas em qualquer tipo de ambiente. Altas doses de proteção requerem altas doses de complexidade, o que pode acabar encarecendo a solução e também aumentando a sua dificuldade de implementação e manutenção.

Devido a sua praticidade, as redes sem fio deixaram de ocupar somente os perfis domésticos e passaram a fazer parte do cenário corporativo, o que requer um cuidado todo especial na parte de segurança.

Pudemos observar que o uso de somente uma tecnologia de proteção, acaba por deixar uma rede vulnerável a certos tipos de ataque, e que a combinação de mais de uma solução ao mesmo tempo seria um cenário bastante próximo do ideal.

Assim como aconteceu com o WEP, provavelmente outros tipos de criptografias consideradas seguras hoje deixarão de ser no futuro, principalmente devido ao avanço das novas tecnologias e do alto poder computacional existentes nos computadores atuais.

É certo também que a indústria não vai para por ai no desenvolvimento de novas técnicas de segurança, já que ela é a principal interessada neste assunto.

REFERÊNCIAS

[1] Ellison, Craig, Exploração e Proteger 802.11b Wireless Networks, 4 em setembro de 2001, página http://www.extremetech.com/article2/0,2845,9280,00.asp. Asp ExtremeTech.com, acessado em 20 de Maio de 2010.

[2] Leoutre, Marc, Edward Post, Mark Reigner, e Scott Lathrop, segurança sem fio: Wireless Antenas e Footprint Analysis, Unpublished Research Paper. Estados Unidos Academia Militar de West Point, NY, May 2002.

[3] Fratto, Mike, Mobile & Wireless Technology Tutorial: Wireless Segurança na Rede Informática, 22 de janeiro de 2001, a CMP United Business Media, em webpage http://www.networkcomputing.com/1202/1202f1d1.html#comments-open, acessado em 20 de Maio de 2010.

[4] Moioli, Fabio, da Segurança Pública de Acesso Wireless LAN Networks, Tese de Mestrado, Departamento de Teleinformática, Royal Institute of Technology, Estocolmo, Suécia. 12 de junho de 2000.

[5] Forouzan, Behrouz A., Comunicação de Dados e Redes de Computadores, 3ª Ed. Bookman, 2006, 840 p.

[6] Internet Security Systems, Wireless LAN Security: 802.11b e redes corporativas. ISS Technical White Paper. Webpage disponível online em http://documents.iss.net/whitepapers/wireless_LAN_security.pdf, acessado em 20 de Maio de 2010.

[7] Chickinsky, Alan, Ameaças Wireless LAN Security. Documento IEEE 802.11-01/258

[8] Colubris Networks, Inc. Comparando Colubris IPSEC Wireless Access Point com Wireless Solutions Middleware Gateways. 2002 Webpage online disponível em http://download.colubris.com/library/whitepapers/WP-020912-EN-02-00.pdf, acessado em 20 de Setembro de 2002.

[9] Colubris Networks, Inc. Comparando Colubris IPSEC Wireless Access Point Solutions com a Cisco Seguro para LANs sem fio. 2002 Webpage online disponível em http://download.colubris.com/library/whitepapers/WP-020912-EN-01-00.pdf, acessado em 20 de Setembro de 2002.

[10] Arbaugh, William, Narendar Shankar e YC Justin Wan, Your 802.11 Wireless Network não tem nenhuma roupa. Departamento de Ciência da Computação da Universidade de Maryland. On-line disponível na página da Web http://www.cs.umd.edu/ ~ waa / wireless.pdf, acessado em 5 de Abril de 2010.

[11] Earle, Aaron E., Wireless security handbook / Aaron E. Earle, Auerbach Publications, 2006, 353 p.

[12] Lynn, Mike e Robert Baird, Advanced 802,11 Attack, apresentação para conferência Black Hat 2002, em Las Vegas, NV 31 de julho de 2002. Disponível em

http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt, acessado em 14 de Setembro de 2009.

[13] Schwartz, Efraim, Pesquisador crack nova especificação de segurança sem fio. InfoWorld. 14 de fevereiro 02. Webpage disponível online em http://staging.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml, acessado em 1 de Outubro 2002.

[14] Mishra, Arunesh e William Arbaugh, An Initial Security Analysis of The IEEE 802.1X Standard. University of Maryland, Department of Computer Science e da Universidade de Maryland Institute for Advanced Computer Studies Techniacal Report CS-TR-4328 e UMIACS-TR-2002-10 6 de fevereiro de 2002.

[15] Potter, Bruce, 802.1x: O que é, como é quebrado, e como corrigi-lo. apresentação para conferência Black Hat 2002, em Las Vegas, NV 31 de julho de 2002. Disponível em http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-potter-802.1x.ppt, accessado em 19 Dezembro de 2009.

[16] Whalen, Sean, An Introduction to Arp Spoofing, April 2001 webpage online available at http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf, accessado em 7 Abril de 2010.

[17] Fleck, Bob and Jordan Dimov, Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network. http://digilander.libero.it/SNHYPER/files/arppoison.pdf, acessado em 26 de Novembro de 2009.

[18] Carey, Allan, Wireless Security Vulnerabilities continue to Surface: Cigital Identifies the Latest. White Paper by Cigital, Inc. http://www.cigital.com. October 2001.

[19] Skoudis, Ed, Counter Hack: A Step-by-Step Guide t Computer Attacks and Effective Defenses. Prentice Hall, Upper Saddle River, New Jersey, 2002. pp 351-358.

[20] Krishnamurthy, Prashnt, Joseph Kabara, Tanapat Anusas-amornkul, Security in Wireless Residential Networks, IEEE Transactions on Consumer Electronics, Vol 48, No 1, February 2002. pp 157- 166.

[21] Karygiannis, Tom and Les Owens, Wireless Network Security: 802.11, Bluetooth and Handheld Devices (Draft), National Institute of Standards and Technology Special Publication 800-48.

[22] RFC 2865 – Disponível em http://www.ietf.org/rfc/rfc2865.txt, acessado em Abril de 2010.

[23] RFC 2866 - Disponível em http://www.ietf.org/rfc/rfc2866.txt, acessado em Junho de 2010.

[24] RFC 2284 - Disponível em http://www.ietf.org/rfc/rfc2284.txt, acessado em Junho de 2010.

[25] RFC 3748 - Disponível em http://www.ietf.org/rfc/rfc3748.txt, acessado em Junho de 2010.

[26] RFC 2246 - Disponível em http://www.ietf.org/rfc/rfc2246.txt, acessado em Junho de 2010.

[27] http://tools.ietf.org/html/draft-ietf-pppext-eap-ttls-05, acessado em Junho de 2010.

[28] http://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-10.txt, acessado em Junho de 2010.

[29] http://aboba.drizzlehosting.com/EAP/draft-kamath-pppext-eap-mschapv2-01.txt, acessado em Junho de 2010.