Thiago Wasserberg Linhares

Redução do Atraso de Transição em Redes Sem-fio IEEE 802.11 para Usuários VoIP Móveis

São José – SC
Setembro/2010

Thiago Wasserberg Linhares

Redução do Atraso de Transição em Redes Sem-fio IEEE 802.11 para Usuários VoIP Móveis

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador:
Prof. Marcelo Sobral

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES
INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC
Setembro/2010

Monografia sob o título "Redução do Atraso de Transição em Redes Sem-fio IEEE 802.11 para Usuários VoIP Móveis", defendida por Thiago Wasserberg Linhares e aprovada em 3 de setembro de 2010, em São José, Santa Catarina, pela banca examinadora assim constituída:

Prof. Marcelo Sobral
Orientador

Prof. Odilson Tadeu Valle
CEFET / SC

Prof. Ederson
CEFET / SC

Agradecimentos

Presto meus sinceros agradecimentos a todos aqueles que ajudaram a lapidar meu caráter e tecer meu conhecimento, aos familiares que apoiaram durante minha trajetória até este momento, a todos aqueles que acreditaram em mim, aos amigos que foram e os que ainda estão presentes.

Dedico a conclusão desta etapa da minha vida principalmente aos meus pais, irmãos e minha namorada sempre presente, atenciosa e compreensiva, a qual amo.

Por ultimo ao meu orientador, que dedicou seu tempo e sua paciência na realização deste trabalho, sendo de fundamental importância.

Resumo

O objeto de estudo deste documento é o tempo de transição entre BSS e uma técnica efetiva para reduzi-lo, de forma a adequar a transmissão de VoIP sobre estruturas de rede sem-fios IEEE 802.11 compostas de múltiplos BSS.

Com a popularização das WLANs, as vantagens do VoIP e as facilidades agregadas a estas tecnologias, surgiu uma nova aplicação com grande potencial no âmbito corporativo, o VoWiFi ou voz sobre Wi-Fi. Muitas empresas adotam o VoIP como solução para a comunicação telefônica interna, substituindo a infraestrutura convencional baseada em PABX. O conceito de VoWiFi possibilita a mobilidade dos terminais telefônicos dentro do alcance da rede sem-fios da empresa, formando uma estrutura similar ao sistema celular, porém de domínio da empresa.

O problema com esta solução de comunicação é o balanceamento entre segurança e qualidade de serviço, uma vez que as atuais estruturas de rede apresentam elevado tempo de desconexão durante a transição (handover) do terminal móvel entre os pontos de acesso da rede. Como objetivo, este trabalho visa reduzir o tempo efetivo de desconexão entre o terminal móvel e a estrutura de rede durante o processo de transição de BSS. O meio empregado para tal realização consiste na realização de experimentos que utilizam a norma IEEE 802.11r, que propõe mecanismos para transição rápida de BSS, porém ainda não difundida comercialmente.

Palavras chave: IEEE 802.11, WiFi, VoIP, transição, BSS, IEEE 802.11r, handover

Abstract

The object of this paper is the transition time between BSS and an effective technique to reduce it in order to adjust the transmission facilities of VoIP over wireless network composed of multiple IEEE 802.11 BSS.

With the popularity of WLANs, the advantages of VoIP and facilities aggregated to these technologies, a new application with great potential in the enterprise, the VoWiFi or Voice over WiFi Many companies are adopting VoIP as a solution to the internal telephone communication by replacing the conventional infrastructure-based PBX. The concept of VoWiFi enables the mobility of telephone terminals within range of the wireless network of the company, forming a structure similar to cellular system, but the company's domain.

The problem with this solution of communication is the balance between security and service quality, since the current network structures have high disconnect time during the transition (handover) of the mobile terminal between network access points. The goal of this work is to reduce the effective time of disconnection between the mobile terminal and network infrastructure during the transition process from BSS. The means employed to such an achievement is the realization of experiments that use the IEEE 802.11r, proposing mechanisms for fast BSS transition, but not yet distributed commercially.

Key words: IEEE 802.11, WiFi, VoIP, transitions, BSS, IEEE 802.11r, handover

Sumário

Agradecimentos iv

Resumo v

Abstract vi

Sumário vii

Lista de Figuras x

Lista de Tabelas xiii

1 Introdução 14

Objetivos 16

Motivação 16

Organização do texto 16

2 Embasamento teórico 18

Requisitos para comunicações multimídia 18

Atraso 19

Jitter 20

Perda de pacotes 20

VoIP 21

Infra-estrutura de redes IEEE 802.11 23

Norma IEEE 802.11 e a arquitetura IEEE 802 23

Elementos de rede 802.11 infra-estruturada 24

Serviços de rede 26

Autenticação 27

Autenticação aberta 28

Autenticação por chave compartilhada 28

PSK (Pré-shared Key) 29

Autenticação 802.1x (EAP) 30

Associação 32

Transição de BSS (*Handover*) 32

3 Padrão 802.11r 35

Definição 35

Funcionamento 36

Processo de (re)associação com FT 37

Formato dos quadros 40

4 Experimentação 41

Ferramentas utilizadas 42

Softwares 42

Hardwares 42

Cenários de teste 43

Resultados dos testes 44

Experimentos e resultados obtidos sem aplicação da norma IEEE 802.11r 44

Jitter de cada teste VoIP realizado 50

Perda de pacotes 51

Resultados obtidos com a aplicação da norma IEEE 802.11r 52

Comparação e análise dos resultados 55

5 Conclusões 59

Anexo I 61

Anexo II 63

Anexo III 67

Anexo IV 69

Anexos V 70

Anexos VI 71

Anexo VII 72

Lista de Acrônimos 74

Referências Bibliográficas 76

Lista de Figuras

Figura 1: Cenário VoIP sobre rede 802.11 14

Figura 2: Topologia da estrutura VoIP 21

Figura 3: Crescimento de chamadas telefônicas internacionais 22

Figura 4: Pilha de protocolos TCP/IP da aplicação VoIP 23

Figura 5: Posicionamento da norma IEEE 802.11 dentro da família IEEE 802 24

Figura 6: Estruturas básicas de comunicação no padrão IEEE 802.11 25

Figura 7: Estrutura de uma ESS 26

Figura 8: Máquina de estados de associação 27

Figura 9: Troca de mensagens com autenticação abeta 28

Figura 10: Hierarquia de derivação de chaves na norma IEEE 802.11i 29

Figura 11: Troca de mensagens do protocolo 4-way handshake 29

Figura 12: Estrutura de autenticação IEEE 802.1x 30

Figura 13: Troca de mensagens durante autenticação EAP 31

Figura 14: Toca de mensagens durante uma associação 32

Figuras 15: Transição entre BSS's 33

Figura 16: Hierarquia de chaves da norma IEEE 802.11r 36

Figuras 17: Troca de mensagens durante associação inicial 38

Figura 18: Troca de mensagens de reassociação Over-the-air 39

Figura 19: Troca de mensagens de reassociação over-the-DS 39

Figura 20: Topologia utilizada nos testes 43

Figuras 21: Reassociação com autenticação aberta 45

Figura 22: Distribuição das reassociações com autenticação aberta 45

Figura 23: Tempo de reassociação de cada transição com autenticação abeta 46

Figura 24: Reassociação com autenticação WPA-PSK 46

Figura 25: Distribuição das reassociações com autenticação WPA-PSK.....47

Figura 26: Tempo de reassociação de cada transição com autenticação WPA-PSK.....47

Figura 27: Reassociação com autenticação WPA-EAP 48

Figura 28: Distribuição das reassociações com autenticação WPA-EAP.....49

Figura 29: Tempo de reassociação de cada transição com autenticação WPA-EAP.....50

Figura 30: Jitter dos testes VoIP 50

Figura 31: Média e projeção de perda de pacotes durante as transições.....51

Figura 32: Reassociação com autenticação FT-PSK 52

Figura 33: Distribuição das reassociações com autenticação FT-PSK 53

Figura 34: Tempo de reassociação de cada transição com autenticação FT-PSK 53

Figuras 35: Reassociação com autenticação FT-EAP.....54

Figura 36: Distribuição das reassociações com autenticação FT-EAP 54

Figura 37: Tempo de reassociação de cada transição com autenticação FT-EAP 55

Figura 38: Histograma comparativo entre WPA-PSK e FT-PSK.....56

Figura 39: Histograma comparativo entre autenticação WPA-EAP e FT-EAP 56

Figura 40: Comparativo entre todos métodos de autenticação 57

Figura 41: Comparativo entre tempo de transição de métodos de autenticação 58

Figura 42: Detalhamento de quadro de rede 802.11 61

Figura 43: Quadro Beacon com adaptação para FT.....63

Figura 44: Quadro Association request com adaptação para FT 63

Figura 45: Quadro Association response com adaptação para FT.....63

Figura 46: Quadro Reassociation request com adaptação para FT 63

Figura 47: Quadro reassociation response com adaptação para FT 63

Figura 48: Quadros Authenticaton com adaptação para FT.....63

Figura 49: Detalhamento do campo MDIE 64

Figura 50: Detalhamento do campo FTIE.....64

Figura 51: Detalhamento do campo GTK 65

Figura 52: Detalhamento do campo TIE 65

Figura 53: Detalhamento do campo RDIE.....65

Figura 54: Detalhamento do campo RIC 65

Figura 55: Detalhamento do quadro FT genérico 66

Figura 56: Detalhamento dos quadros FT request e response.....66

Figura 57: Detalhamento do quadro FT Confirm 66

Figura 58: Detalhamento do quadro FT Ack 66

Lista de Tabelas

Tabela 1: Parâmetros para qualidade de comunicação de voz 18

Tabela 2: Atraso de serialização 19

Tabela 3: Atraso de propagação 19

Tabela 4: Lista de serviços de redes IEEE 802.11 utilizados no trabalho 26

Tabela 5: Métodos de autenticação suportados por redes 802.11 30

Tabela 6: Softwares utilizados nos testes 42

Tabela 7: Hardwares utilizados nos testes 42

Tabela 8: Tipos de quadro de controle 61

Tabela 9: Tabela dos parâmetros opcionais do campo FTIE 64

Tabela 10: Tipos de intervalo de tempo 65

Tabela 11: Tipos de ação de protocolo FT 66

1 Introdução

As redes IEEE 802.11 se tornaram o padrão de fato para WLAN (redes locais sem-fio), sendo amplamente usadas para prover conectividade. Além da facilidade evidente de atender usuários em qualquer localização dentro da região coberta pelo serviço, sem necessidade de cabeamento prévio, essas redes sem-fio abrem novas possibilidades de serviços e aplicações que exploram a ubiqüidade e mobilidade[GAST, 2005]. Dentre essas, o uso de telefones VoIP (Voice over IP) sem-fio tem o atrativo de prover um serviço de telefonia IP similar ao da telefonia celular, pois um usuário móvel pode manter conversações em qualquer ponto da área de cobertura [WARD, 2003]. No entanto, o serviço VoIP possui requisitos de tempo-real brando (soft real-time) para que o áudio transmitido seja inteligível, porém as redes IEEE 802.11 não foram inicialmente concebidas para atender esse tipo de exigência. Em particular, a transição entre BSS (Basic Station Set, similar na rede IEEE 802.11 a células), conhecida como handover, apresenta um atraso significativo que pode causar uma interrupção momentânea de uma conversação em andamento. A figura 1 mostra uma topologia genérica de uma aplicação de telefonia IP sobre uma rede 802.11.

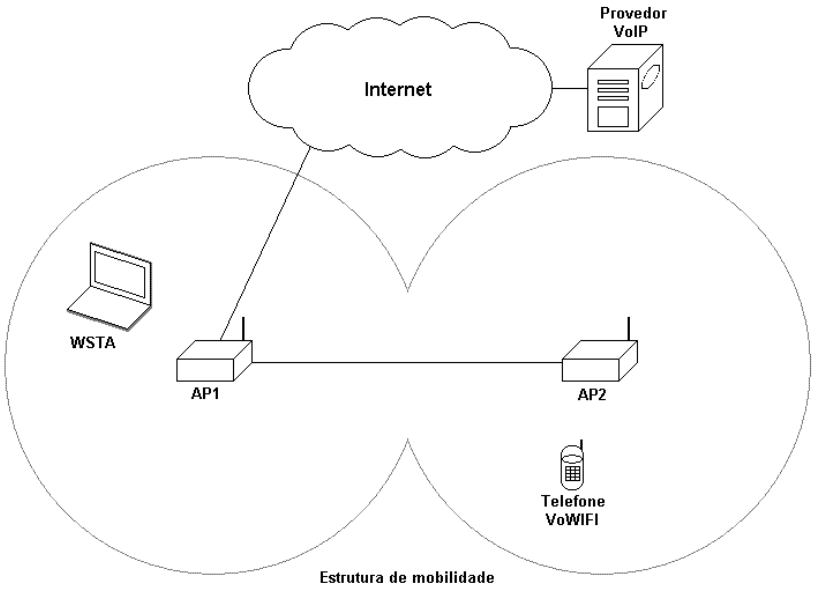


Figura 1: Cenário VoIP sobre rede 802.11

Uma conversação VoIP possui requisitos de qualidade de serviço para que se obtenha uma boa reprodução do áudio transmitido. A perda de mensagens não deve exceder 1%, para evitar estalos e palavras cortadas. Como a amostragem típica para digitalização e encapsulamento em mensagens é de 20 ms, e codecs não conseguem atenuar perdas mais longas que esse valor, a perda de duas ou mais mensagens consecutivas causa degradação de qualidade perceptível. Outro requisito limita a 150 ms a latência, ou atraso entre a captura do som no transmissor e sua reprodução no receptor. O padrão de telefonia ITU-T G.114 definiu esse valor como adequado para conversação confortável e satisfatória, porém experimentos de laboratório mostraram que um valor de 200 ms é aceitável. Finalmente, o jitter (variação de atraso entre mensagens consecutivas) não deve exceder 30 ms, para evitar que o som recebido seja intermeado por chiados. Assim, o uso de um serviço VoIP sobre uma rede sem-fio IEEE 802.11 implica uma verificação quanto ao atendimento desses requisitos de qualidade.

Em uma rede sem-fios IEEE 802.11 composta por múltiplos BSS, sendo cada BSS coordenado por um AP (Access Point), uma WSTA (Wireless Station) móvel eventualmente migra de BSS. Isto acontece automaticamente, quando a intensidade do sinal do BSS atual estiver abaixo de um certo valor predefinido. Neste caso, desencadeia-se uma operação de transição (handover), que demanda um certo tempo para se completar. O atraso para efetuação da transição depende do tempo necessário para realizar a associação com o novo BSS, além da varredura dos canais de transmissão em busca dos BSS existentes na vizinhança. Originalmente a associação implicava a troca de quatro mensagens, porém com a adoção de novos e mais sofisticados métodos de autenticação um número crescente de mensagens passou a ser necessário para completar a associação. Assim, a associação com o novo BSS pode apresentar uma contribuição significativa para esse atraso de transição, uma vez que, dependendo do método de autenticação, muitas mensagens podem ser trocadas entre a WSTA e o AP. No caso de a rede sem-fio ser usada por usuários VoIP móveis, esse atraso de transição pode causar principalmente a perda de mensagens e um incremento momentâneo da latência. Em vista disto, surgiu a necessidade de um novo mecanismo de transição entre BSS, de forma a torná-lo mais rápido.

A extensão IEEE 802.11r foi proposta em julho de 2008 e tem como objetivo reduzir o atraso de transição entre BSS's [IEEE, 2008]. Para a redução no tempo de reassociação que ocorre durante uma transição, a norma propõe uma redução drástica no número de mensagens trocadas durante o processo de autenticação. Essa redução é mais evidente em autenticações que utilizam métodos EAP, e só é possível graças a um mecanismo chamado FT (fast

transition), que modifica alguns quadros de controle do padrão 802.11 assim como o método de gerenciamento e hierarquia de chaves, possibilitando a troca de material criptográfico entre os pontos de acesso após a primeira autenticação de um WSTA [BANGOLAE,]. Com isto, espera-se que, em condições ideais, uma reassociação ocorra em até 50ms. Assim, um atraso de transição dessa magnitude poderia satisfazer os requisitos de qualidade para um serviço VoIP usado por usuários móveis.

Objetivos

O objetivo geral do trabalho é reduzir o atraso de transição em redes sem-fio IEEE 802.11, de forma a atender os requisitos de qualidade para o serviço VoIP para usuários móveis. Para atingir esse objetivo, o trabalho propõe identificar os parâmetros de comunicação presentes em interfaces de rede e Access Points IEEE 802.11 que influenciam na duração desse atraso, e usar a norma IEEE 802.11r, que define um mecanismo para a transição rápida de BSS.

Motivação

A motivação para este trabalho é viabilizar o uso de redes sem-fio IEEE 802.11 por usuários VoIP móveis. Desta forma, seria possível criar uma rede de telefonia sem-fio privativa, com funcionalidade semelhante a uma rede celular.

Organização do texto

O texto esta organizado da seguinte forma:

- **Capitulo 2**: Descreve as referencias bibliográficas para embasamento teórico do projeto, os requisitos mínimos de atraso e perdas de pacotes para comunicações de voz, um overview do funcionamento de redes 802.11 e os serviços utilizados que serão utilizados

- **Capitulo 3**: Apresenta a norma IEEE 802.11r, seu funcionamento e como ocorre a redução no tempo de transição.
- **Capitulo 4**: Neste capitulo é apresentado a metodologia, os cenários de teste e os resultados obtidos no cenário atual de redes 802.11, sem transição rápida, confrontados com a aplicação da transição rápida (IEEE 802.11r) utilizados para mensurar o tempo de transição em redes 802.11 e as melhorias.
- **Capitulo 5**: Apresenta as conclusões do documento.

2 Embasamento teórico

Requisitos para comunicações multimídia

As aplicações com *streams*[1] que geram tráfego de tempo-real tem características mais restritivas que as demais aplicações de dados. Além da transmissão correta das mensagens há necessidade de sincronização entre fonte e destino para apresentar uma qualidade satisfatória no serviço [JESZENSKY, 2004]. Desta forma, tais aplicações possuem pouca tolerância a atrasos, *jitter*[2] e perda de pacotes. No caso específico de telefonia IP (VoIP), para atender os requisitos de qualidade e padronização nos sistemas telefônicos o ITU-T[3] elaborou uma série de documentos normativos (G.110 a 119 - General Recommendations on the transmission quality for an entire international telephone connection). Essa recomendação estipula valores limites para parâmetros que influenciam a qualidade da comunicação, conforme mostrados na tabela 1.

Tabela 1: Parâmetros para qualidade de comunicação de voz

Atraso	<150ms
Jitter	< 30ms
Perda de pacotes	<1% (dependendo do CODEC[4])

Fonte: (GOLENIEWSKY, 2002)

As próximas subseções detalham a influência desses parâmetros na qualidade das comunicações de voz.

---

1 Fluxo de dados em sistemas computacionais

2 Médida de variação do atraso entre os pacotes sucessivos de dados

3 Seção de Padronização da área de Telecomunicações do ITU - União Internacional de Telecomunicações ("International Telecommunication Union")

4 Técnica de codificação e decodificação de sinais

Atraso

O atraso é o tempo que a voz leva desde a origem até seu destino, do momento que é pronunciada e codificada até ser decodificada do outro lado da linha para que possa ser ouvida. O principal efeito causado por este atraso é um retardo na comunicação que pode ser percebido como um incômodo pelo usuário [JESZENSKY, 2004]. Esse atraso é comumente chamado de atraso fim-a-fim e corresponde ao somatório de todos atrasos ocorridos do inicio ao fim do percurso trafegado pela voz, podendo ser dividido em dois tipos: atrasos fixos e variáveis, sendo o segundo exclusivo de sistemas por comutação de pacotes. O atraso possui três componentes, sendo eles atraso algorítmico, de serialização e de propagação, que dependem basicamente da tecnologia empregada e limitações físicas dos meios de transmissão.

- Atraso algorítmico – gerado pelos CODECs
- Atraso de serialização – tempo que a interface de rede leva para colocar os dados no meio de transmissão. Depende da taxa de transmissão do enlace de dados e o tamanho do quadro transmitido. A tabela 2 lista o atraso em *ms* para enlaces de dados e quadros de transmissão variados.

Tabela 2: Atraso de serialização

Velocidade do *link*	*Atraso (ms)*					
	64 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	1500 Bytes
56 kbps	9	18	36	72	144	214
64 kbps	8	16	32	64	128	187
128 Kbps	4	8	16	32	64	93
256 kbps	2	4	8	16	32	46
512 kbps	1	2	4	8	16	23
768 kbps	0,640	1,28	2,56	5,12	10,4	15

FONTE: (GUIMARÃES, 1999)

- Atraso de propagação – atraso característico do meio físico onde o sinal será transportado e o tipo de sistema de transmissão utilizado. A tabela 3 mostra alguns sistemas de transmissão e seus respectivos atrasos. [ITU-T, 2003]

Tabela 3: Atraso de propagação

Sistema de transmissão ou de processamento	**Atraso em sentido único**	**Comentários**
Sistema terrestre de cabo coaxial ou radio: FDM e transmissão digital	4µs/km	Permite o atraso em repetidores e regeneradores
Sistema de fibra óptica, transmissão digital	5µs/km	
Sistema de cabo coaxial submarino	6µs/km	
- transmissor - receptor	13ms 10ms	Pior caso
Sistemas via satélite: - 400 Km de altitude - 14000 Km de altitude - 36000 Km de altitude	 12ms 110ms 260ms	Propagação através do espaço (entre estações terrestres)

Fonte: (ITU-T, G.114, 2003)

Jitter

Variação do atraso fim-a-fim, a qual resulta da diferença entre o atraso máximo e o atraso mínimo durante uma comunicação. O jitter acarreta um tempo variável na chegada dos pacotes, que quando muito elevado causa uma sensação de desconforto na comunicação. Para minimizar o efeito que o jitter causa em comunicações em tempo real é adicionado um buffer[5] de jitter no receptor para que a informação na saída seja constante e com tempo fixo [JESZENSKY, 2004]. Essa técnica incrementa o atraso fim-a-fim, portanto o tamanho do buffer deve ser calculado com prudência para não reduzir a qualidade da comunicação.

As redes do tipo IP são caracterizadas por serem best-effort (melhor esforço), pois seus principais protocolos (IP, TCP e UDP) não provêem mecanismos para atender requisitos de qualidade de serviço. Assim, as PDUs de diferentes fluxos de dados que chegam a um roteador são usualmente encaminhadas por ordem de chegada (enfileiramento do tipo FIFO – First In First Out). Devido a esse enfileiramento, que causa a multiplexação dos datagramas vindos de diferentes enlaces, os atrasos de entrega sofridos por PDUs subsequentes de um mesmo fluxo podem variar ao longo do tempo. No caso de aplicações VoIP, a variação do atraso pode comprometer a sincronização entre fonte e destino, tornando parte da conversação ininteligível.

Perda de pacotes

A perda de pacotes é caracterizada pelo numero de pacotes que não chegam ao seu destino, e o maior causador dessas perdas é o congestionamento nos links de transmissão,

mas podem ser causados por problemas de hardware e quedas no link de comunicação [FOROUZAN, 2007]. Os congestionamentos aumentam o atraso nos pacotes, e quando esse se torna muito elevado o pacote é descartado. O efeito das perdas de pacote durante uma comunicação é caracterizado por oscilações na comunicação, pequenas falhas durante a conversação. Isto ocorre quando as perdas atingem um determinado limite que varia de acordo com o CODEC utilizado o entendimento durante a chamada pode ser comprometido.

VoIP

O serviço telefônico convencional vem sofrendo um processo de integração de serviços e convergência entre os dois tipos fundamentalmente diferentes de tecnologia: voz e dados. O cenário atual esta caracterizado pela busca do mercado por novas aplicações e tecnologias assim como custo para ampliação da rede convencional para as operadoras, somando estes fatos ao crescimento explosivo da internet, e o grande número de aplicações disponíveis sobre ela, o protocolo IP se apresentou como forte candidato para a convergência entre as redes de dados e voz, abrindo espaço para uma nova aplicação denominada VoIP (voz sobre IP). A figura 2 mostra uma visão geral da topologia VoIP utilizada hoje. [JESZENSKY, 2004].

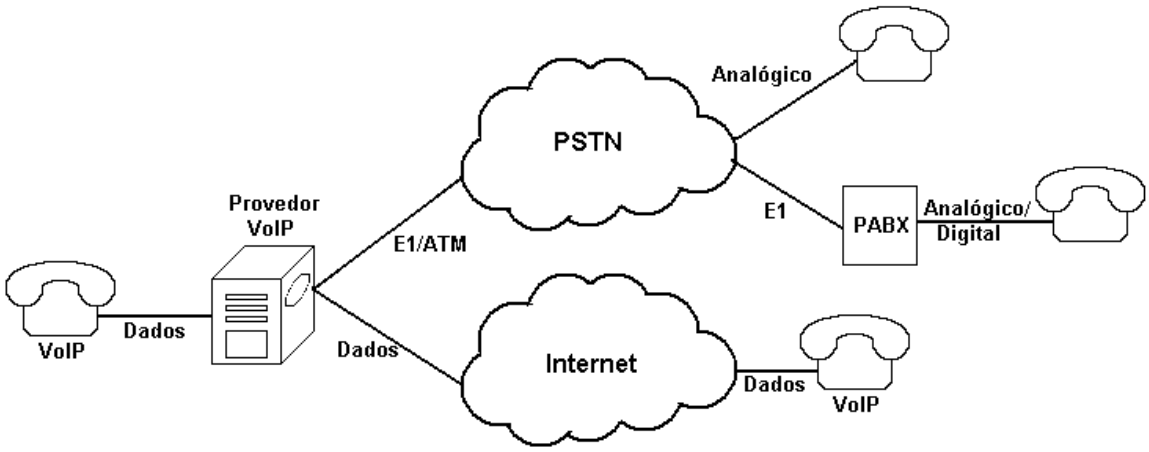


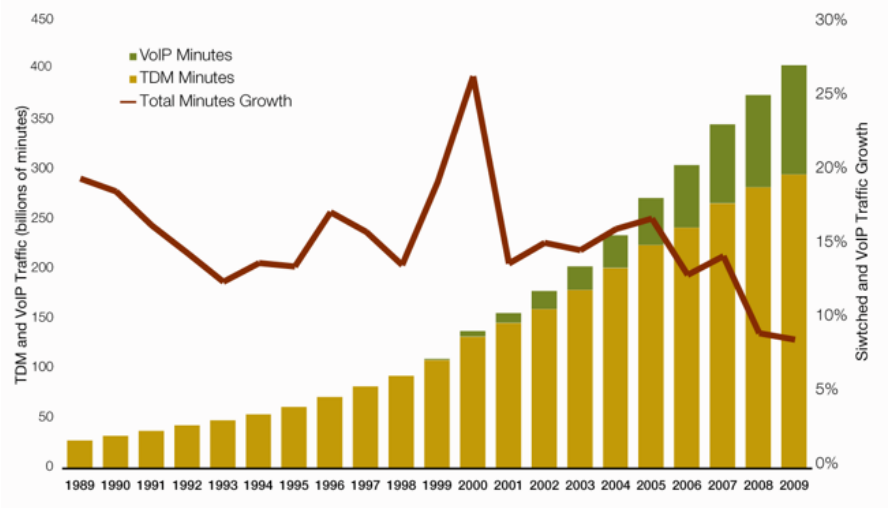
Figura 2: Topologia da estrutura VoIP

O VoIP ainda não possui uma padronização ou regulamentação definida, assim muitas instituições internacionais como ITU-T e IEEE, trabalham para desenvolver um padrão para está tecnologia. Mesmo sem um padrão definido e uma legislação especifica em vigor, essa

---

5 Memória temporária utilizada para escrita e leitura de dados

nova aplicação vem ganhando espaço no cenário da telefonia mundial [JESZENSKY, 2004]. O gráfico representado pela figura 3 apresenta o crescimento das chamadas telefônicas internacionais VoIP e convencional mostrada como TDM.



Fonte: (www.telegeography.com)

Figura 3: Crescimento de chamadas telefônicas internacionais

Atualmente a maior parte das soluções VoIP aplicadas no mundo utilizam os protocolos H.323, desenvolvido pelo ITU-T, ou o SIP, proposto pelo IETF, ambos para sinalização. Alem desses, a transmissão de streams de áudio se faz com o RTP (Real Time Protocol), protocolo proposto pelo IETF na RFC 3550 para transporte fim-a-fim de mídia em tempo real brando (*soft real-time*).

O RTP não oferece qualidade de serviço e não aborda aspectos de reserva de recurso ao longo do trajeto de uma comunicação, e funciona de forma transparente tanto em conexões unicast quanto multicast. Apesar do RTP ter sido projetado para ser independente da rede de transporte e camadas, é comumente utilizado sobre o UDP, adicionando funcionalidades como verificação de atraso fim-a-fim, sequencialização e sincronismo de sessão [IETF, 2003]. O RTP também possibilita o monitoramento e controle dos fluxos de transmissão de uma comunicação, sendo utilizado para isso um protocolo adicional chamado RTCP[6], que informa aos terminais as características do meio de transmissão como jitter, perda de pacotes e atraso [FOROUZAN, 2007].

O RTP usa o protocolo UDP para transmissão de suas PDUs, uma vez que esse protocolo não faz controle de erros nem de fluxo, o que adicionaria atrasos indesejáveis à comunicação. A figura 4 mostras uma pilha de protocolos TCP/IP utilizadas hoje para aplicações VoIP.

---

[6] Real Time Control Protocol, RFC 3550

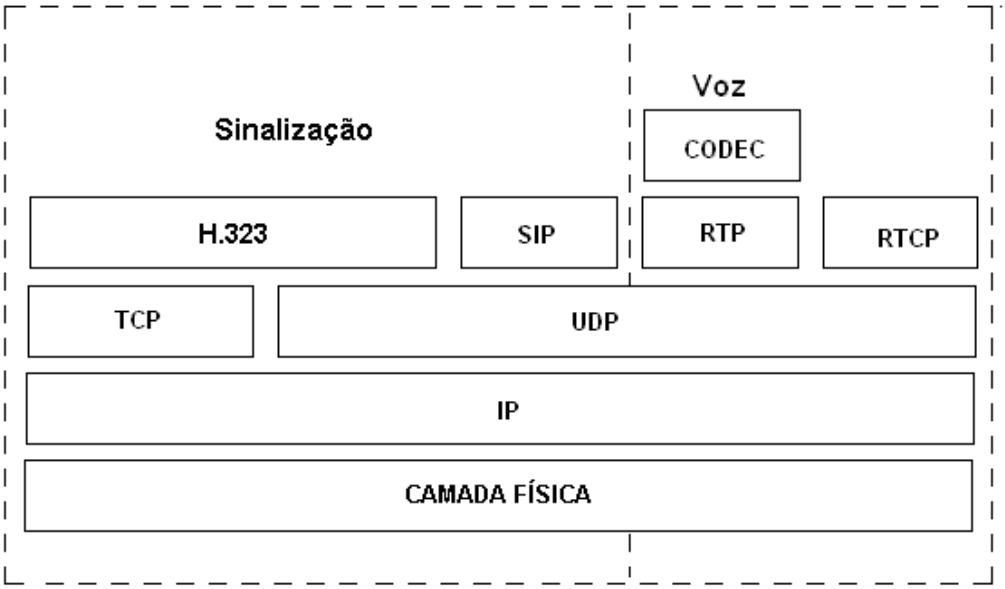


Figura 4: Pilha de protocolos TCP/IP da aplicação VoIP

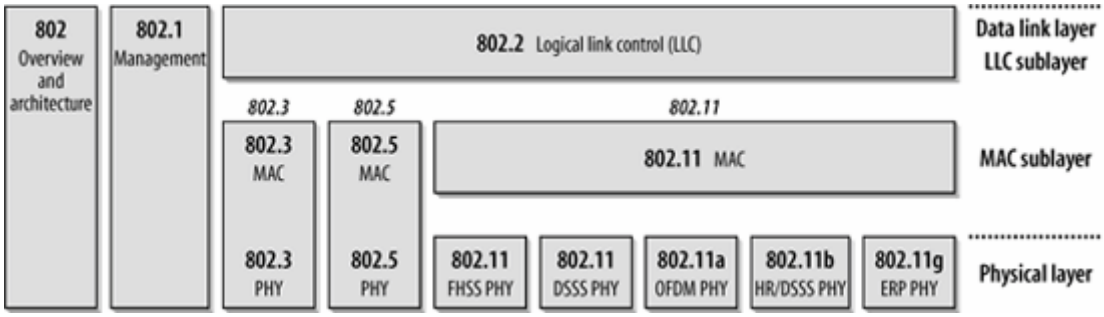
A abordagem VoIP utilizada no projeto utiliza como protocolo de sinalização o SIP (Session Initiation Protocol), proposto pelo IETF na RFC2543 em 1999, desenvolvido para criar e controlar sessões multimídia interativas na internet entre dois participantes ou mais. É um protocolo do tipo cliente servidor baseado em texto, assim como HTTP e o SMTP, o que o torna mais simples, flexível e escalável.

Infra-estrutura de redes IEEE 802.11

Nos últimos anos, devido ao cotidiano e dinâmica da população, principalmente do mercado em busca de agilidade e produção, as redes sem fio tornaram-se algo indispensável, capazes de prover a mobilidade aos usuários antes limitadas por cabos. Já estão presentes em quase todos os lugares, desde escritórios e shoppings até áreas comuns de lazer como no calçadão de Copacabana, e a cada dia que passa aumenta o numero de dispositivos com suporte a este tipo de comunicação, assim como a demanda por essa tecnologia.

Norma IEEE 802.11 e a arquitetura IEEE 802

O padrão 802.11 faz parte da família de normas IEEE 802, que tem como objetivo especificar tecnologias para redes locais (LANs). A figura 5 mostra a relação do padrão 802.11 com outros padrões descritos pelo IEEE [GAST, 2005].



Fonte: (GAST, 2005)

Figura 5: Posicionamento da norma IEEE 802.11 dentro da família IEEE 802

Como mostrado na figura, a norma IEEE 802.11 Cobre a camada física e subcamada MAC da arquitetura IEEE 802:

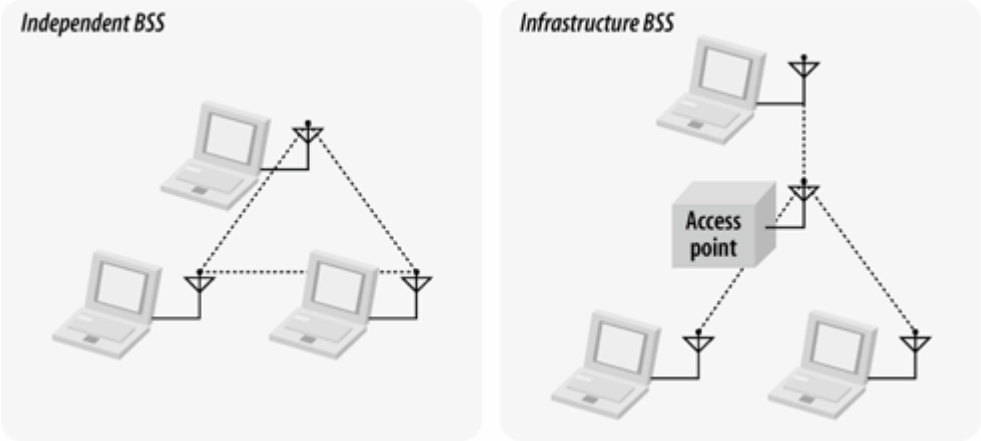
- Camada física (PHY): corresponde ao meio de transmissão e as técnicas utilizadas para transmitir a informação. As técnicas de modulação utilizadas pelo padrão 802.11 são FHSS[7], DSSS[8] e OFDM[9]
- Subcamada MAC: nessa camada se implementa o controle de acesso ao meio de transmissão, além dos formatos de quadros de dados e controle usados para as transmissões de dados. O acesso ao meio é feito por um protocolo conhecido por CSMA/CA (*Carrier Sense Multiple Access network with Collision Avoidance*).

Elementos de rede 802.11 infra-estruturada

As redes WLAN IEEE 802.11 podem ser configuradas em dois modos de operação distintos: infra-estruturado e Ad-hoc. No modo infra-estruturado, as redes possuem uma estação base, chamada de ponto de acesso (AP, ou Access Point), responsável pela autenticação e associação de estações, além de servir de intermediador para comunicação entre estações sem-fio e possivelmente estações na rede cabeada [IEEE, 2007]. No modo de operação Ad-hoc, as redes não possuem estação base, e assim as WSTAs podem se comunicar diretamente com qualquer outra WSTA em seu alcance. A figura 6 mostra esses dois tipos de redes sem-fio 802.11. [GAST, 2005]

---

7 Técnica de espalhamento espectral denominada Frequency Hopping Spread Spectrum
8 Técnica de espalhamento espectral denominada Direct Sequence Spread Spectrum
9 Técnica de modulação denominada Orthogonal Frequency-Division Multiplexing



Fonte: (GAST, 2005)

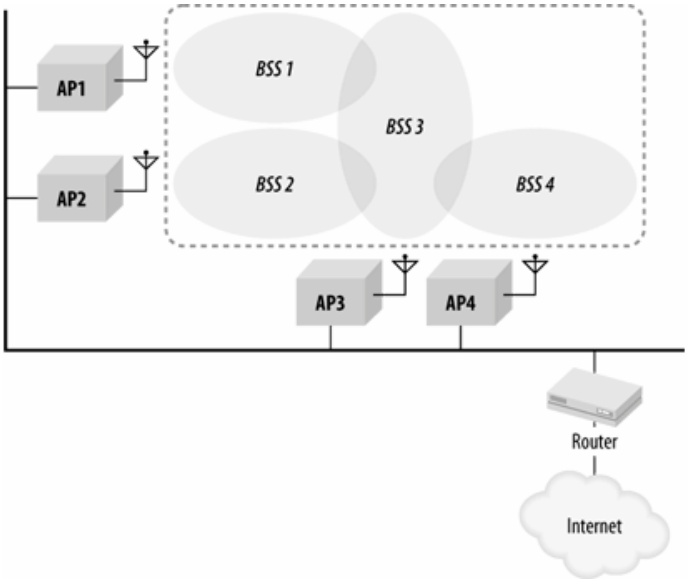
Figura 6: Estruturas básicas de comunicação no padrão IEEE 802.11

A estrutura básica de organização nas redes IEEE 802.11 é chamada de BSS[10] quando em modo infra-estruturado (i.e, quando possui um ponto de acesso), ou IBSS[11] em redes Ad-hoc. Em ambos os casos, são composta de estações sem fio que tanto podem ser móveis ou fixas, e possuem uma cobertura limitada cujo alcance depende da taxa de dados, da potência de transmissão e os ganhos das antenas, além das características físicas do ambiente onde está implantada a rede [ERGEN, 2002]. Os limites de alcance em campo aberto podem variar de aproximadamente 20 m (para taxa de dados de 54 Mbps) a quase 100 m (para taxa de 1 Mbps). No caso de redes infra-estruturadas, o padrão 802.11 possibilita combinar vários BSS para ampliar a área de cobertura de uma rede WLAN. Esses BSS devem possuir a mesma identidade de rede (SSID) e seus AP devem ser interligados por um sistema de distribuição (DS), que pode ser via rede cabeada ou sem-fio (quando então se chama WDS). Essa nova estrutura, chamada de ESS (Extended Station Set) e exemplificada na figura 7, possibilita que as estações móveis possam se deslocar de um BSS para outro, porém permanecendo conectadas à mesma rede local. Essa transição entre BSS é conhecida por handover ou roaming [GAST, 2005].

---

10 Basic Service Set

11 Independent Basic Service Set



Fonte: (GAST, 2005)

Figura 7: Estrutura de uma ESS

Em transições entre BSSs da mesma ESS, a comunicação não é perdida. Assim, qualquer fluxo de dados iniciado antes da transição é continuado após o restabelecimento da comunicação no novo ponto de acesso. Por exemplo, uma chamada VoIP iniciada em um BSS é continuada após a transição, porém sofrendo uma possível degradação na qualidade durante o processo.

Serviços de rede

Uma maneira de definir uma tecnologia de rede é definindo os serviços que ela oferece e permitindo que fornecedores de equipamentos possam programar esses serviços da forma que acharem melhor. O 802.11 oferece nove serviços. Apenas três dos serviços são utilizados para transferência de dados, os seis restantes são operações de gestão que permitem à rede acompanhar de nós móveis e entregar frames em conformidade. A tabela a 2.4 lista os serviços que serão utilizados no decorrer do trabalho. [GAST, 2005].

Tabela 4: Lista de serviços de redes IEEE 802.11 utilizados no trabalho

Serviço	Descrição
Associação	Usado para estabelecer conexão com um AP
Reassociação	Usada mudar o ponto de conexão de um AP para o outro
Desassociação	Desconectar a estação móvel da rede
Autenticação	Estabelece a identidade da estação (MAC address) antes de

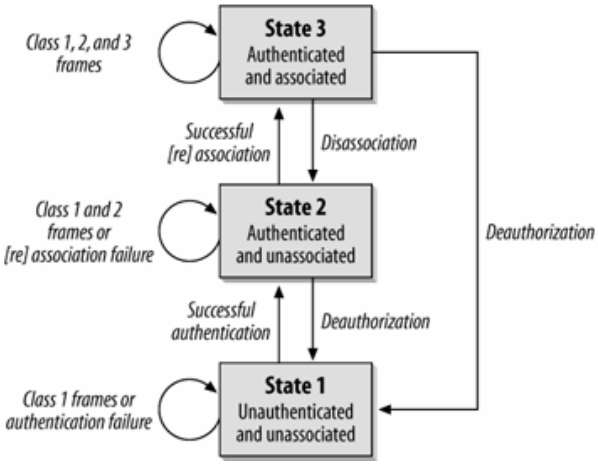
	estabelecer associação
Desautenticação	Usado para terminar a autenticação

Fonte: (GAST, 2005)

Os serviços que têm influência direta no atraso de transição são associação, autenticação e reassociação. A atuação desses serviços pode ser exemplificada em três estados.

- Estado 1 – não associado e não autenticado
- Estado 2 – não associado e autenticado
- Estado 3 – associado e autenticado

Quando a estação móvel está se conectando a rede, possui estado inicial 1, e quando chega ao estado 3 está apta a transferir dados e informação pela WLAN. No processo de reassociação o usuário sai do estado 3 para o estado 1, reiniciando o processo. A figura 8 ilustra uma máquina de estados e o papel dos serviços nas transições de estados [GAST, 2005].



Fonte: (GAST, 2005)

Figura 8: Máquina de estados de associação

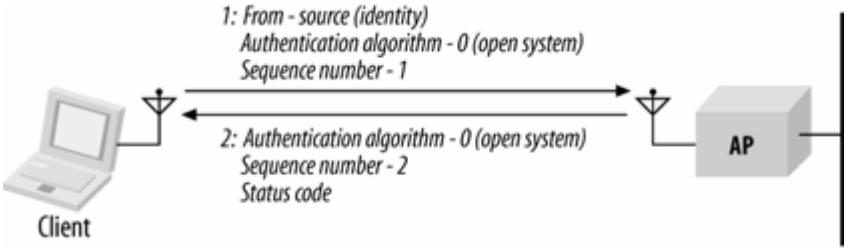
Autenticação

Autenticação é o processo de identificar um usuário que solicita acesso a uma determinada área, função ou funcionalidade. Durante o processo de autenticação a entidade autenticadora solicita a identificação do usuário e a compara com seu banco de dados, liberando ou não o acesso [GEIER, 2008]. Só após esta etapa o cliente esta autorizado a desfrutar dos serviços providos pela rede. Em uma rede sem fio o usuário deve se identificar antes de ter acesso pleno a rede e a seus recursos.

O IEEE 802.11 definiu originalmente dois métodos de autenticação de usuários, sendo eles sistema aberto (Open-system) e autenticação por chave compartilhada (*shared key authentication*). O método de autenticação e segurança inicialmente proposto para o padrão 802.11, conhecido como WEP (*wired equivalente privacy*), é vulnerável e assim não provê uma segurança adequada a transmissão. Por esse motivo o IEEE desenvolveu o padrão 802.11i, que descreve novas técnicas de autenticação e criptografia para redes sem fio, aumentando a privacidade e segurança da rede.

Autenticação aberta

Este é o método de autenticação mais simples em arquiteturas 802.11. Nele não há uma autenticação propriamente dita, pois qualquer usuário que detenha um dispositivo com tecnologia compatível pode conectar-se a rede sem restrições. Alem deste fato, nesta abordagem a comunicação não é criptografada ficando exposta a interceptação por indivíduos mal intencionados, porem o tempo de associação e reassociação gasto neste sistema é mínimo, não implicando em problemas significativos para aplicações em tempo real como é o caso do VoIP. A figura 9, exemplifica a troca de mensagens durante a autenticação por sistema aberto [GAST, 2005].



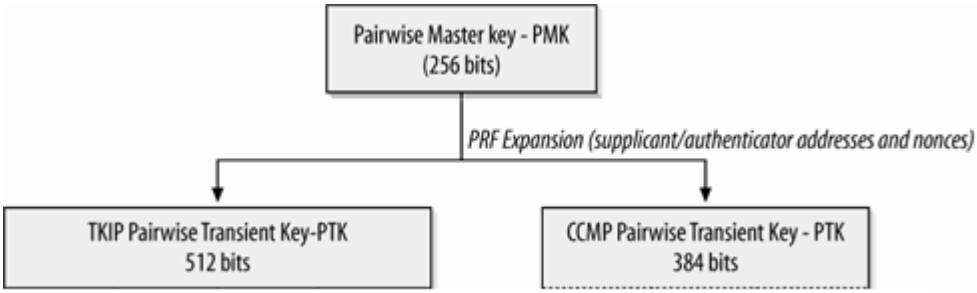
Fonte: (GAST, 2005)

Figura 9: Troca de mensagens com autenticação abeta

Autenticação por chave compartilhada

A autenticação por chave compartilhada é proposta na norma 802.11i, conhecida como WPA2 (Wi-Fi Protected Access) e descrita para corrigir as falhas de segurança do WEP. Este padrão define novos mecanismos de segurança para garantir a confidencialidade e integridade da rede e da informação trafegada sobre ela. Esta norma descreve dois métodos de autenticação e gerenciamento de chave, sendo eles PSK e EAP, assim como uma hierarquia de chave com a finalidade de proteger a chave mestra de criptografia. A chave mestra é conhecida por PMK e não é trocada em momento algum da transmissão, sendo utilizada para gerar chaves temporárias (PTK) que são instaladas nas WSTa e AP para criptografar os dados

durante a transmissão. No método de autenticação PSK a chave PMK é previamente configurada no ponto de acesso, já no EAP a chave mestra é calculada pelo servidor Radius. A figura 10 apresenta a hierarquia de chaves do WPA [GAST, 2005].

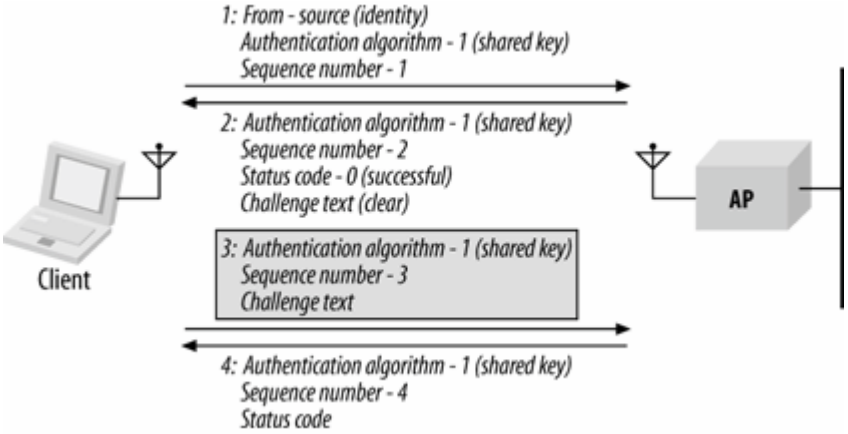


Fonte: (GAST, 2005)

Figura 10: Hierarquia de derivação de chaves na norma IEEE 802.11i

PSK (Pré-shared Key)

Em sistemas com autenticação por chave pré-compartilhadas o ponto de acesso é previamente configurado com uma chave de acesso, que o usuário deve conhecer para se conectar a WLAN. Após a associação, a estação móvel troca suas credenciais com o ponto de acesso respondendo a um desafio em um processo conhecido por 4-way handshake, este utiliza o protocolo EAPOL para transmitir as mensagens [NIST, 2007]. Está técnica de autenticação protege a integridade da rede e da informação, porém adiciona um atraso no processo de associação e reassociação durante a transição entre BSS's. Este atraso é de pequena magnitude e não implica em impacto significativo para aplicações em tempo real. A figura 11, mostra a troca de mensagens do protocolo 4-way handshake ocorridas durante o processo de autenticação [GAST, 2005].

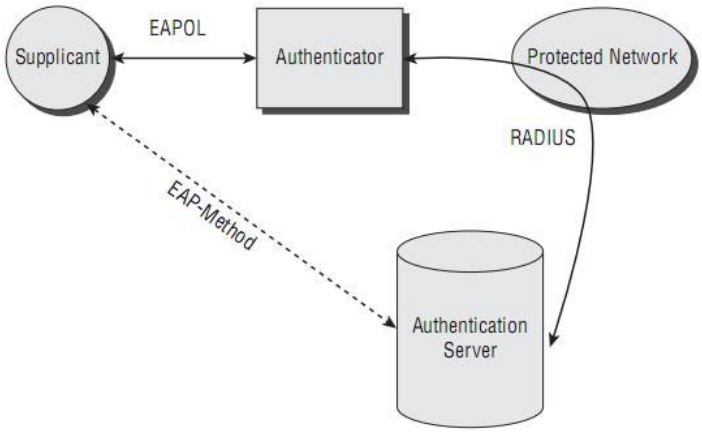


Fonte: (GAST, 2005)

Figura 11: Troca de mensagens do protocolo 4-way handshake

Autenticação 802.1x (EAP)

O protocolo EAP, descrito na norma IEEE 802.1x, permite métodos de autenticação arbitrários possibilitando trocas de informação e credenciais de forma segura entre o cliente e um servidor. O protocolo EAP provê um tunelamento criptografado entre o cliente e o servidor de autenticação, possibilitando a troca de credenciais preservando a integridade e a segurança da rede. A figura 12 mostra a arquitetura do controle de acesso proposto na norma IEEE 802.1x, com seus elementos envolvidos e protocolos [GEIER, 2008].



Fonte: (GEIER, 2008)

Figura 12: Estrutura de autenticação IEEE 802.1x

Como mostrado na figura 12 o método EAP faz uma ligação lógica entre o WSTA (supplicant) e o servidor de autenticação, e sobre este link lógico as credenciais são fornecidas para que ocorra a autenticação. As PDUs EAP, que transportam os dados do método EAP selecionado, são transportadas por protocolos distintos durante o trajeto. No percurso entre WSTA e autenticador (no caso, o AP o transporte das PDUs EAP se faz sobre o protocolo EAPOL. A norma não especifica um protocolo para comunicação entre autenticador e servidor de autenticação, porém comumente se usa o protocolo RADIUS[12]. [GEIER, 2008]

O protocolo EAP suporta uma ampla variedade de mecanismos de autenticação, implementados em métodos EAP, e é projetado para funcionar sobre qualquer tecnologia referente a camada de link. A tabela 5 lista todos os métodos de autenticação suportados em redes IEEE 802.11 [GAST,2005].

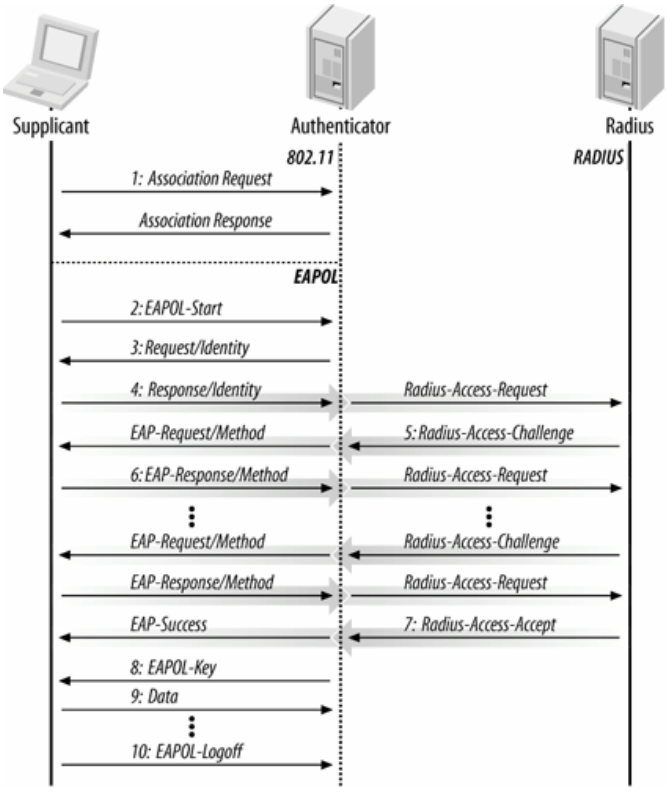
Tabela 5: Métodos de autenticação suportados por redes 802.11

[12] Remote Authentication Dial In User Service, RFC 2138

Type code	Authentication protocol	Description
4	MD5 Challenge	CHAP-like authentication in EAP
6	GTC	Originally intended for use with token cards such as RSA SecurID
13	EAP-TLS	Mutual authentication with digital certificates
21	TTLS	Tunneled TLS; protects weaker authentication methods with TLS encryption
25	PEAP	Protected EAP; protects weaker EAP methods with TLS encryption
18	EAP-SIM	Authentication by mobile phone Subscriber Identity Module (SIM)
29	MS-CHAP-V2	Microsoft encrypted password authentication; compatible with Windows domains

Fonte: (GAST, 2005)

Dependendo do método EAP selecionado, há um atraso para conclusão da autenticação o qual pode ser significativo. Esse atraso ocorre devido à quantidade de mensagens trocadas entre o cliente e o servidor de autenticação durante a autenticação. Outros fatores devem ser levados em consideração para mensurar o atraso proveniente do processo de autenticação, sendo o numero de saltos na rede do autenticador até o servidor de autenticação Radius, assim como o tráfego na rede durante o processo de autenticação. A figura 13 apresenta um exemplo de estabelecimento de conexão em redes 802.11 com autenticação utilizando protocolo EAP [GAST, 2005].



Fonte: (GAST, 2005)

Figura 13: Troca de mensagens durante autenticação EAP

Associação

Uma estação móvel só pode transmitir e receber dados para a WLAN se estiver conectada a um ponto de acesso. O processo para estabelecimento de conexão entre o ponto de acesso e o usuário é a associação, que só pode ser efetivada após a identificação do usuário por algum método de autenticação. O processo de associação tem inicio com a estação fazendo uma varredura em todos os canais de transmissão em busca de pontos de acesso disponíveis em sua cobertura [ERGEN, 2002]. Todos os AP enviam um quadro de anúncio, chamado de *beacon*, a cada 100ms (tempo padrão da especificação 802.11). Esse quadro contém informações necessárias para o estabelecimento da conexão, como o tipo de autenticação requerida e o nome da rede (SSID). Após localizar o quadro de anúncio do ponto de acesso alvo é iniciada a associação. A figura 14 mostra a troca de mensagens genérica durante uma associação entre uma WSTA e um ponto de acesso.

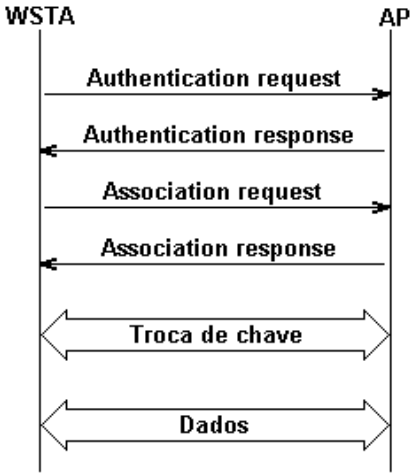


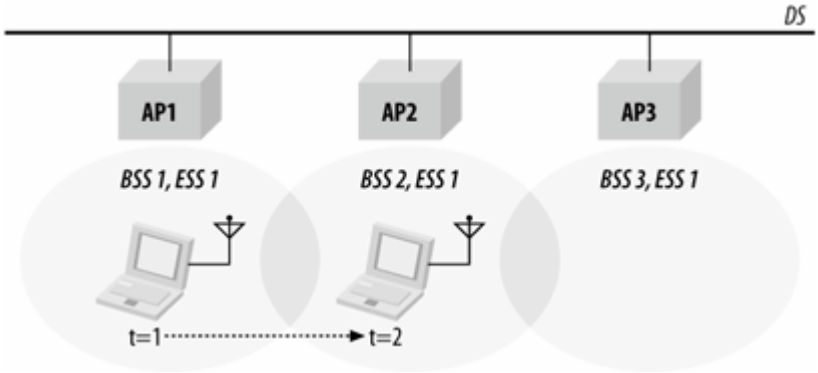
Figura 14: Toca de mensagens durante uma associação

Transição de BSS (*Handover*)

Um dos problemas para atender os requisitos de qualidade em chamadas VoIP e outras aplicações de tempo real sobre redes 802.11 se refere à mobilidade. Em estruturas de rede mais complexas com mais de um ponto de acesso para prover conectividade entre os usuários, um WSTA tem a possibilidade de fazer transição de BSS durante a comunicação, mudando sua associação de um ponto de acesso para outro que esteja dentro de sua área de cobertura. Um problema no processo de transição de BSS é o tempo em que a estação fica incomunicável, podendo chegar a alguns segundos dependendo do método de autenticação utilizado e a localização do servidor de autenticação na rede, em casos que utilizem o EAP como método de autenticação [IEEE, 2007]. Por definição o padrão 802.11 não suporta

associação a mais de um ponto de acesso simultaneamente, e essa característica resulta na incapacidade dessas redes WLAN realizarem soft-handover (transição de BSS sem necessidade de prévia dissociação). Sendo assim, para que ocorra uma transição a WSTA deve primeiramente se dissociar do ponto de acesso atual para em seguida iniciar o processo de associação em outro ponto de acesso. Esse procedimento força uma parada na comunicação das aplicações que utilizam a rede, sendo um ponto sensível para algumas delas, em particular as que geram tráfego de tempo-real como no caso de VoIP.

O processo de transição de BSS é deflagrado quando o nível do sinal na WSTA atinge um limite mínimo para uma comunicação estável e com nível de erro aceitável (nível de sinal pré-estabelecido). Nesse instante a WSTA inicia o processo de varredura em busca de outros pontos de acesso com melhor nível de sinal e mesmo SSID dentro da ESS, e após localizar um AP que atenda aos critérios citados, o processo de reassociação é iniciado. Durante este processo o cliente deve ser autenticado novamente, assim como a cada reassociação. Em métodos de autenticação mais simples essas autenticações repetidas a cada transição de BSS não apresentam reduções significativas de qualidade da comunicação. Porém os métodos que utilizam o protocolo EAP para autenticação, por serem mais complexos e trocarem um número maior de mensagens, podem levar um tempo significativo para conclusão da transição de BSS, o qual pode chegar a alguns segundos. Esse fator pode inviabilizar as comunicações VoIP e multimídia para usuários móveis em cenários que combinam múltiplos BSS's e autenticação por meio do protocolo EAP. A figura 15 a seguir exemplifica a transição de BSS e o processo de reassociação [GAST, 2005].



Fonte: (GAST, 2005)

Figuras 15: Transição entre BSS's

A figura 15 apresenta um cenário com três BSS interligados por um sistema de distribuição formando um ESS. A estação móvel no instante t=1 está na região de cobertura do AP1 e em deslocamento para a direita em direção ao AP2. No momento t=2 a estação

móvel não esta mais sob a área de cobertura do AP1, assim inicia o processo de reassociação com o AP2.

3 Padrão 802.11r

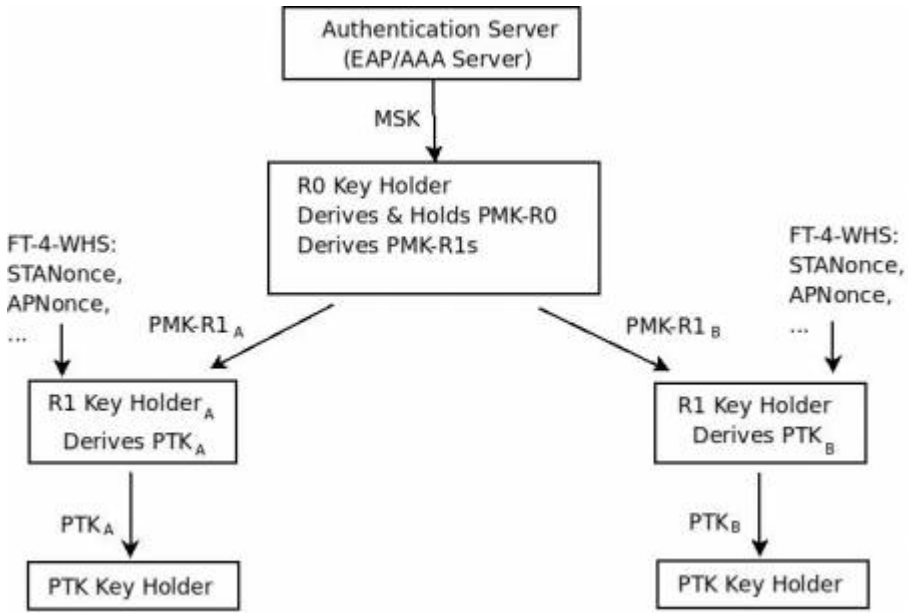
O IEEE 802.11r é um padrão proposto em junho de 2008 para fazer transição rápida de BSS. A principal modificação proposta trata tornar válido em um conjunto de BSS o resultado de uma autenticação de uma WSTA em um dos BSS desse conjunto. Para isso define-se um novo mecanismo de troca de chaves e uma nova hierarquia de derivação de chaves. O resultado esperado é agilizar o processo de autenticação dos mecanismos 802.11i, reduzindo o tempo em que a WSTA móvel fica desconectada da rede durante as transições de BSS [IEEE, 2008]

Definição

A redução no tempo de transição é possível devido a modificações no método de gerenciamento de chaves e na hierarquia de chaves propostos anteriormente no padrão 802.11i. No padrão 802.11r o conjunto de BSS onde se podem fazer transições rápidas de BSS se chama domínio de mobilidade (MD – Mobility Domain). Dentro do MD, o elemento onde se faz a primeira autenticação se chama R0KH (R0 Key Holder), e os elementos onde se fazem associações subsequentes são denominados R1KH (R1 Key Holder). Tanto R0KH quanto R1KH são na realidade funcionalidades existentes em cada AP. A transição rápida, chamada de Fast BSS Transition (FT BSS), faz com que, após a associação inicial com a primeira autenticação no domínio de mobilidade, as demais reassociações trocam as credenciais em apenas quatro mensagens, como será mostrado nas figuras 32 e 35. Para isso, FT BSS define um mecanismo para que a partir da PMK inicial, mantida no R0KH e denominada PMK-R0, sejam derivadas PMK-R1 para cada R1KH. Essas PMK-R1 são transferidas para os R1KH correspondentes, residentes nos AP do domínio de mobilidade.

Funcionamento

O padrão IEEE 802.11r divide a rede em domínios de mobilidade, que são conjuntos de AP em que as estações móveis podem efetuar transições rápidas com o mecanismo FT. Essa estrutura de mobilidade tem como objetivo reduzir o numero de mensagens trocadas no processo de autenticação entre o usuário móvel, o autenticador e o servidor de autenticação. Dentro de um domínio de mobilidade o WSTA faz sua primeira autenticação com um AP por meio do método WPA-PSK ou WPA-EAP. Depois de conferida a identidade do usuário móvel, o R0KH residente no AP onde se fez essa associação inicial calcula a chave PMK-R0 (primeira derivação da chave PMK). As chaves PMK-R0 são utilizadas pelo R0KH para gerar chaves PMK-R1 (segunda derivação da chave PMK), que serão distribuídas aos R1KH, residentes nos demais AP do domínio de mobilidade. Nos pontos de acesso as chaves PMK-R1 são utilizadas para derivar as chaves temporárias PTK, que serão utilizadas encriptar os quadros de dados entre WSTA e AP. Ainda durante a primeira autenticação com o domínio de mobilidade a estação móvel recebe informações como identificação do domínio de mobilidade (MDIE), identificação do R0KH (R0KH-ID) e R1KH (R1KH-ID) e tempo de duração da chave temporária (informações contidas no campo FTIE no quadro de confirmação de autenticação). A figura 16 mostra a hierarquia de chaves utilizadas pelo padrão 802.11r.[IEEE, 2008]



Fonte: (IEEE 802.11r – Fast Transition, 2008)

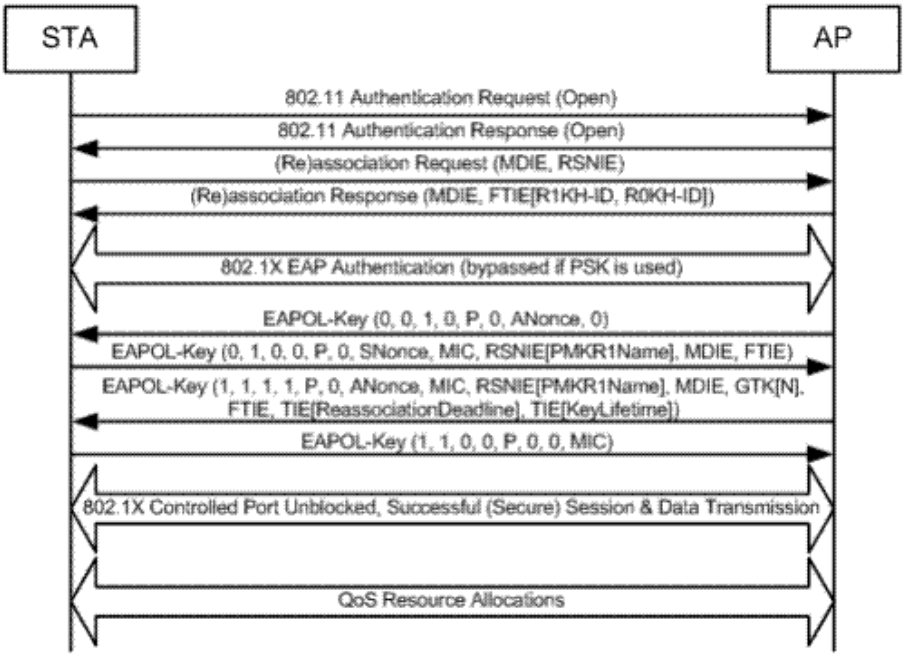
Figura 16: Hierarquia de chaves da norma IEEE 802.11r

A figura 16 exemplifica a hierarquia de derivação de chaves com a norma IEEE 802.11r. No primeiro nível esta o servidor de autenticação, logo abaixo o controlador do domínio de mobilidade que deriva as chaves PMK distribuindo para os pontos de acesso em nível inferior, este deriva as chaves temporárias PTK e distribuem para os WSTA's.

Para as próximas reassociações e autenticações o usuário móvel envia ao ponto de acesso alvo as informações obtidas durante o processo de associação inicial, que contém dados derivados de sua autenticação, identificação do ponto de acesso de origem e informações do domínio de mobilidade. Todas estas informações são trocadas nos quatro quadros de controle (autenthication request, authentication response, reassociation request e reassociation response) durante as transições, eliminado a fase de tunelamento (na autenticação com EAP) e o protocolo 4-way handshake, isto reduz o overhead de mensagens durante as transições.

Processo de (re)associação com FT

O primeiro acesso ao domínio de mobilidade é chamado de FT de acesso inicial ao domínio de mobilidade (FT initial mobility domain association), e é durante esse processo que ocorre a troca das chaves do protocolo EAP e PSK, assim como a derivação das chaves PMK-R0 e PMK-R1. O inicio da associação é idêntico à associação com suporte a 802.1x. Após a confirmação de identidade é iniciado o processo FT 4-way handshake, responsável por distribuir as chaves geradas a partir da autenticação EAP. A figura 17 exemplifica o processo de associação inicial [IEEE, 2008].

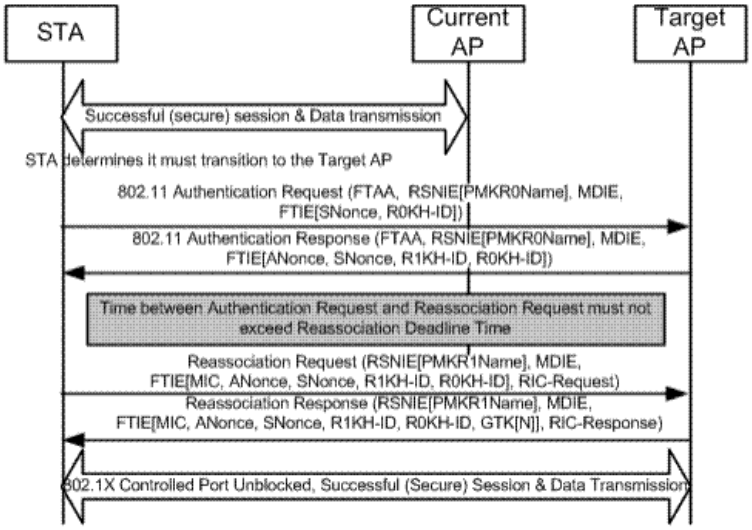


Fonte: (IEEE 802.11r – Fast Transition, 2008)

Figuras 17: Troca de mensagens durante associação inicial

Após a primeira associação com o domínio de mobilidade, o processo de reassociação utilizando o protocolo FT pode ser realizado de duas formas distintas:

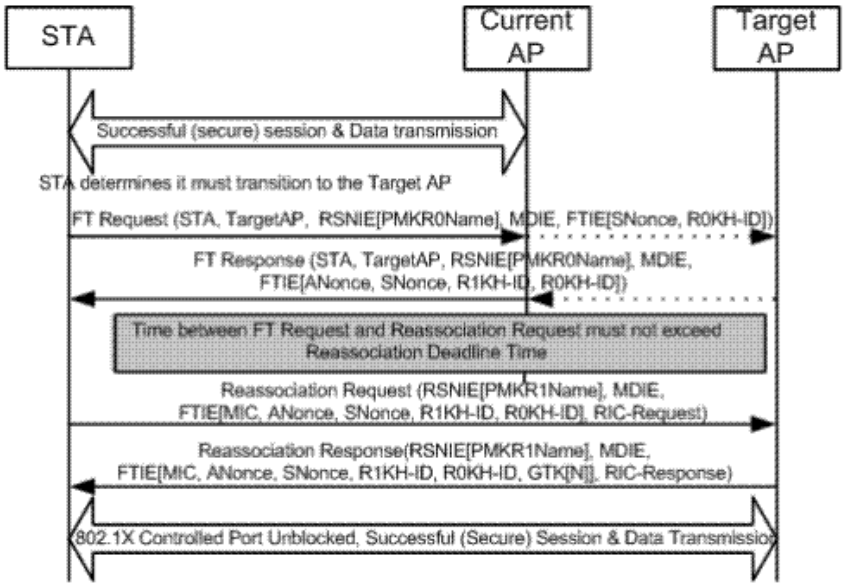
- Over-the-air FT – a qual a estação móvel comunica-se diretamente com o ponto de acesso alvo através de interface sem fio, trocando as informações necessárias para o sucesso da reassociação sem intermediários. Este processo utiliza os quadros de autenticação e reassociação para trocar as credenciais. A figura 18 detalha a troca de mensagens do método over-the-air FT [IEEE, 2008].



Fonte: (IEEE 802.11r – Fast Transition, 2008)

Figura 18: Troca de mensagens de reassociação Over-the-air

- Over-the-DS – A estação móvel utiliza o ponto de acesso corrente para trocar informação com o ponto de acesso alvo através do sistema de distribuição comum entre eles, ao contrario do método anterior que utiliza os quadros 802.11 adaptados esta técnica utiliza os quadros FT. A figura 19 mostra detalhadamente a troca de mensagens FT entre os elementos envolvidos [IEEE, 2008].



Fonte: (IEEE 802.11r – Fast Transition, 2008)

Figura 19: Troca de mensagens de reassociação over-the-DS

Formato dos quadros

O padrão IEEE 802.11r fez algumas adaptações nos quadros de gerenciamento já existentes nos padrões anteriores. Ocorreram mudanças nos quadros beacon, association request e response, reassociation request e response e authentication. Foram acrescentados alguns campos nestes quadros que serão descritos no anexo II [IEEE, 2008].

4 Experimentação

Os testes consistem na realização de chamadas VoIP e captura do trafego RTP gerado com auxilio de um analisador de protocolo. O objetivo dos testes é colher informações necessárias para uma análise detalhada do impacto negativo que a autenticação proporciona sobre a qualidade de cada chamada VoIP durante a transição de BSS.

A duração média de uma chamada telefônica é de 3 a 4 minutos, e durante cada chamada uma parte do tempo a linha esta ociosa, com um ou ambos os interlocutores quietos [LEONEL, 2003]. Com base nestas informações e para evidenciar o impacto na comunicação assim como uma boa qualidade durante as chamadas ao invés de conversação entre dois interlocutores foi transmitida uma musica com sonoridade constante, garantindo uma ocupação de linha de aproximadamente 100%.

Na aplicação da técnica de testes, foi configurado um ramal automático que atende a chamada e toca uma musica, e ao fim encerra a chamada. Cada chamada tem uma duração com tempo fixo de 2 minutos e 45 segundos, e foram realizadas 20 chamadas em cada cenário de testes, totalizando um tempo de 55 minutos por cenário. Durante cada chamada foram transmitidos exatos 8500 pacotes RTP.

Todos os testes foram realizados em condições ideais, ou seja, eliminando as variáveis que pudessem influenciar nos valores dos resultados obtidos e prejudicar a analise dos dados. Como condições ideais compreendem-se uma única estação móvel utilizando o meio sem fio, o mais próximo possível do ponto de acesso e estática sendo que as transições foram realizadas de forma manual, através de comandos digitados no pronpt cliente do supplicant no Linux.

Para reprodução dos testes, os anexos III ao VII contêm as informações e os arquivos de configuração do hostapd utilizados na realização dos testes. Para informações da configuração do cliente basta dar o comando *man wpa_cli* no *prompt* do linux.

Ferramentas utilizadas

Para realização dos testes e comprovação pratica dos resultados foram utilizados alguns equipamentos e softwares citados a seguir:

Softwares

Todos os testes foram realizados no Linux, usando-se a distribuição Ubuntu 10.4 LTS. A tabela 3.1 apresenta uma lista dos softwares utilizados nos testes, a plataforma de funcionamento e uma breve descrição.

Tabela 6: Softwares utilizados nos testes

Softwares	**Plataforma**	**Descrição**
Wireshark 1.2.7	multiplataforma	Software de captura de pacotes e análise de protocolos
Hostapd 0.7.2	Linux	Emula ponto de acesso
Twinkle 1.4.2	Linux	Softphone VoIP
Asterisk 1.6.2	Linux	Servidor SIP
Supplicant 0.7.2	Linux	Software com atuação na camada MAC

Hardwares

A tabela 3.2 apresenta uma lista dos equipamentos utilizados, modelo dos equipamentos e informações de hardware relevantes.

Tabela 7: Hardwares utilizados nos testes

Equipamento	**Modelo**	**Hardware**
Notebook	Acer aspire 3690	Celeron M 1.73Ghz, 512 DDR2, FSB 433 Mhz,
Adaptador 802.11	Atheros	Chipset Atheros AR5005G
Desktop	Asus	AMD Athlon(tm) 64 Processor 3000+, 1G DDR2, FSB 400 MHz, Placa mãe A8V-VM ULTRA
Adaptador 802.11	Pacific	Chipset Atheros AR2413

Cenários de teste

O objetivo geral dos testes é coletar informações e características da transição de uma estação móvel entre BSSs durante chamadas VoIP. A partir das informações adquiridas avaliar o desempenho individual de cada teste realizado.

Para realização dos testes foi utilizado um notebook e um PC Desktop com adaptado de rede IEEE 802.11. A topologia da rede assim como os elementos presentes nos testes é representado na figura 20.

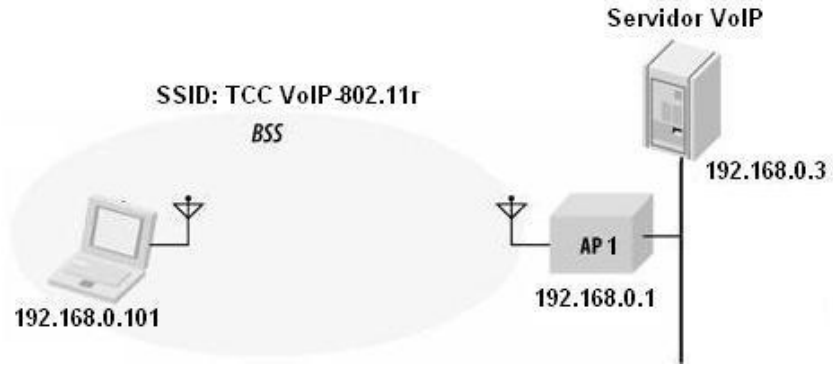


Figura 20: Topologia utilizada nos testes

Na figura 20 o ponto de acesso e o servidor VoIP foram identificados como elementos distintos para melhor compreensão da topologia utilizada, porem no cenário real, o Desktop emulava um ponto de acesso utilizando o software hostapd e a placa sem fio, e em background estava rodando o servidor asterisk.

Como pode ser visualizado na figura 20, o cenário de teste tem um único BSS, por este motivo, o processo de transição foi simulado, resultando em um maior controle sobre o experimento. O efeito de transição pode ser obtido enviando um pedido de reassociação no suplicante, assim o WSTA fez reassociações no próprio ponto de acesso sem a necessidade de mais de um AP. Este processo é equivalente a transição espontânea entre BSSs distintas.

Uma vez que as reassociações foram forçadas, não foi necessário que o WSTA estivesse em movimento para que ocorressem as transições. Por este motivo, os testes foram realizados com o notebook estático e o mais próximo possível do ponto de acesso. Diminuindo assim o impacto que um canal de comunicação móvel implica sobre uma comunicação de dados, fato este que garantiu uma maior precisão nos resultados obtidos.

Com exceção ao primeiro teste em que não foi realizado nenhuma transição, a única diferença entre os demais é o método de autenticação utilizado.

Resultados dos testes

A distribuição dos resultados foi dividida em três subseções. Na primeira estão os resultados obtidos nos testes antes da aplicação da norma 802.11r, na segunda parte os resultados obtidos nos testes com a aplicação da norma, por último é apresentado uma comparação entre os resultados sem e com aplicação da norma, assim como a análise dos resultados com os parâmetros de qualidade propostos pelo ITU-T, e citados na sessão 2.1.

Na prática o tempo de transição é o intervalo de tempo entre a desautenticação com o ponto de acesso corrente até o fim da toca de credenciais do WSTA com o ponto de acesso alvo, e corresponde ao somatório entre o tempo de varredura e o tempo de (re) associação. Seguindo o mesmo raciocínio, o tempo de varredura é o intervalo que corresponde ao quadro de desautenticação até o primeiro quadro de autenticação. O tempo de (re) associação é o intervalo entre o primeiro quando de autenticação até o quadro de resposta de reassociação, isto em sistemas de autenticação aberto ou com FT, em sistemas de autenticação WPA-PSK e WPA-EAP o tempo se estende até o ultimo quadro da troca de chaves com protocolo *4-way handshake*.

A proposta do projeto é reduzir o tempo de reassociação, uma vez que o padrão IEEE 802.11r não trata a questão da varredura. Por tanto os resultados apresentados a seguir não levam em consideração a varredura.

Experimentos e resultados obtidos sem aplicação da norma IEEE 802.11r

Como citado na sessão 2.3, em sistemas de comunicação que utilizam o sistema aberto como forma de autenticação, o numero de mensagens trocadas entre o WSTA e o ponto de acesso durante uma transição é o menor possível. Após a deautenticação do ponto de acesso corrente, ocorre à troca de quatro quadros de controle até que o WSTA esteja novamente autenticado e pronto para transmitir. A figura 21 foi obtida durante os testes com auxilio do analisador de protocolo, e demonstra a troca de quadros entre o ponto de acesso e o WSTA durante uma transição com autenticação aberta. O instante de recepção de cada quadro é mostrado na primeira coluna à esquerda, e o tipo de cada quadro é informado na última coluna à direita.

```
12:19:40.472559              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
12:19:40.472566 HonHaiPr_7c D-Link_a9:c0: IEEE 80 Deauthentication, SN=2255
12:19:40.473452              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
12:19:40.473462 HonHaiPr_7c D-Link_a9:c0: IEEE 80 Authentication, SN=2256,
12:19:40.474086 D-Link_a9:c HonHaiPr_7c:a IEEE 80 Authentication, SN=607, F
12:19:40.475574              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
12:19:40.475579 HonHaiPr_7c D-Link_a9:c0: IEEE 80 Reassociation Request, SN
12:19:40.476405 D-Link_a9:c HonHaiPr_7c:a IEEE 80 Reassociation Response, S
12:19:40.478156              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
12:19:40.507412 D-Link_a9:c Broadcast     IEEE 80 Beacon frame, SN=598, FN=
12:19:40.609786 D-Link_a9:c Broadcast     IEEE 80 Beacon frame, SN=599, FN=
```

Figuras 21: Reassociação com autenticação aberta

Após a realização dos testes pôde ser levantado uma estatística em relação ao tempo de associação utilizando o sistema de autenticação aberto. Nesta figura o tempo de reassociação foi de 3ms. O gráfico representado pela figura 22 apresenta a distribuição das reassociações em função do tempo.

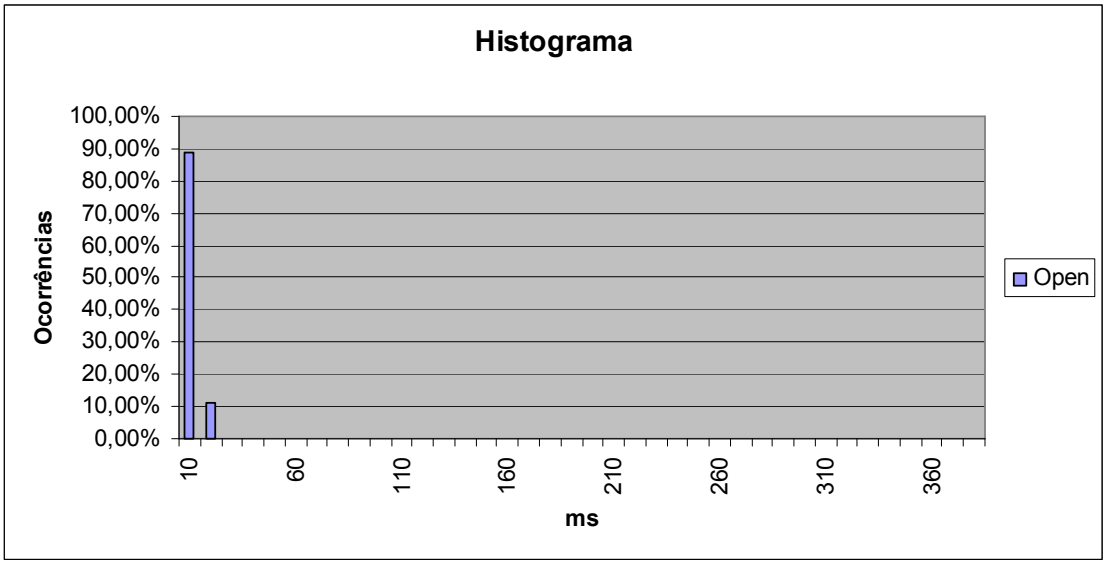


Figura 22: Distribuição das reassociações com autenticação aberta

Nos resultados obtidos, em 88,67% as reassociações ocorreram abaixo de 10ms e todas em menos de 20ms. O tempo médio de duração das reassociações foi de 4,75ms e o desvio padrão foi de 2,68ms, sendo assim 99,7% das reassociações com sistema aberto de autenticação ocorreram em até 12,79ms. Isto pode ser visualizado no gráfico representado pela figura 23, que apresenta o tempo de duração de cada reassociação obtida durante o teste com autenticação aberta. Nesse gráfico fica evidente que as durações de todas as reassociações se situaram entre 2 ms e 14 ms.

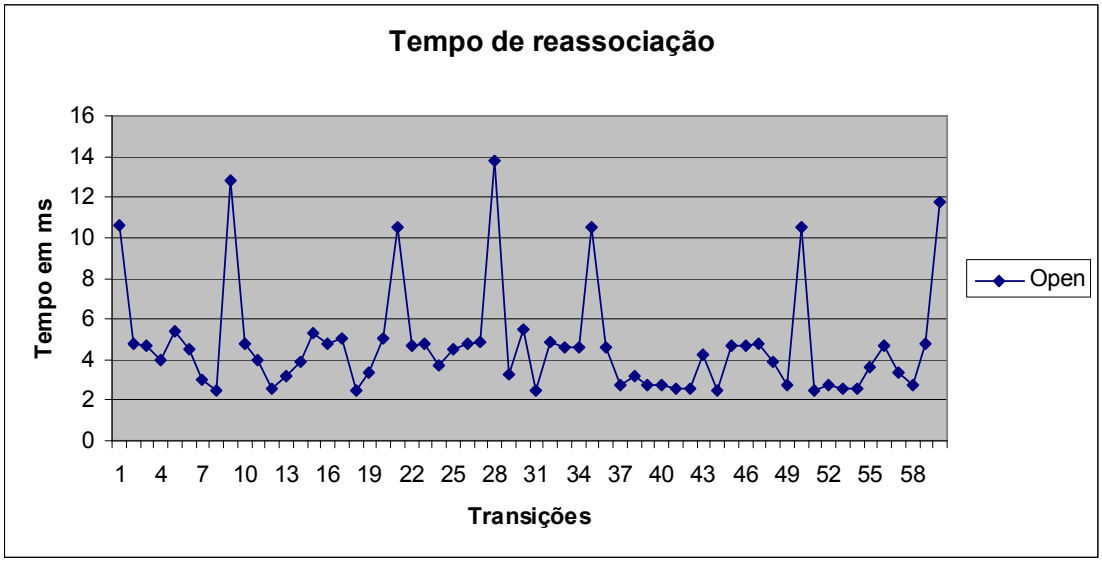


Figura 23: Tempo de reassociação de cada transição com autenticação abeta

O método de autenticação com WPA-PSK adiciona algumas trocas de quadros, e assim seu tempo de reassociação deve ser maior em comparação com sistemas com autenticação aberta. A figura 24 mostra todos os quadros trocados entre o ponto de acesso e o WSTA, inclusive a troca da chave de acesso, o que pode ser comparado com a seqüência de quadros apresentada na seção 2.3.

```
14:37:36.741299             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.741322 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Deauthentication, SN=1877
14:37:36.742131             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.742135 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Authentication, SN=1878,
14:37:36.742663 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Authentication, SN=2389,
14:37:36.744172             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.744183 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Reassociation Request, SN
14:37:36.744884 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Reassociation Response, S
14:37:36.747326 Tp-LinkT_c5 HonHaiPr_7c:a EAPOL   Key
14:37:36.757949             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.757956 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Null function (No data),
14:37:36.759727             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.759739 HonHaiPr_7c Tp-LinkT_c5:d EAPOL   Key
14:37:36.762903 Tp-LinkT_c5 HonHaiPr_7c:a EAPOL   Key
14:37:36.775501             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
14:37:36.775508 HonHaiPr_7c Tp-LinkT_c5:d EAPOL   Key
14:37:48.426776             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
```

Figura 24: Reassociação com autenticação WPA-PSK

O tempo de reassociação com este método de autenticação corresponde ao intervalo entre o primeiro quadro de autenticação e o ultimo quadro EAPOL de chave, ambos marcados na figura 24. Neste exemplo o tempo de reassociação foi de 33,4 *ms*.

Com base nos resultados obtidos nos testes com autenticação WPA-PSK, pôde ser avaliado o tempo de reassociação com este método de autenticação. O gráfico representado pela figura 25 mostra a concentração das ocorrências de reassociação em função do tempo.

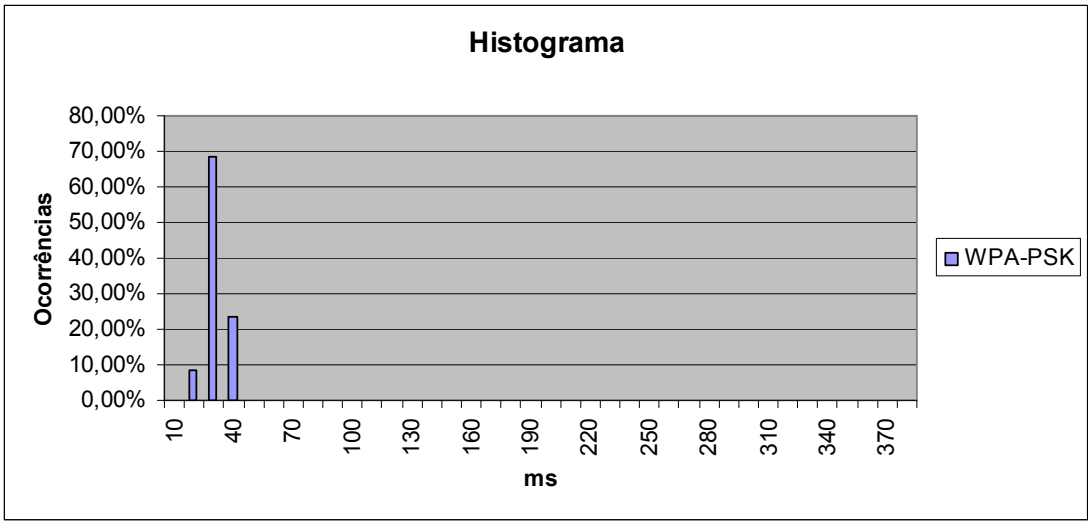


Figura 25: Distribuição das reassociações com autenticação WPA-PSK

Analisando o gráfico e os resultados obtidos, foi constatado que 8,33% das reassociações ocorreram em menos de 20 *ms*, 76,66% em menos de 30 *ms* e todas em menos de 40 *ms*. Com base nos mesmos resultados, médio de reassociação foi de 24,6 *ms* e o desvio padrão obtido foi de 5ms, a partir destas informações obteve-se que 99,7% das reassociações ocorrem em até 39,6 *ms*. O gráfico representado pela figura 26 apresenta detalhadamente o tempo de reassociação em cada transição.

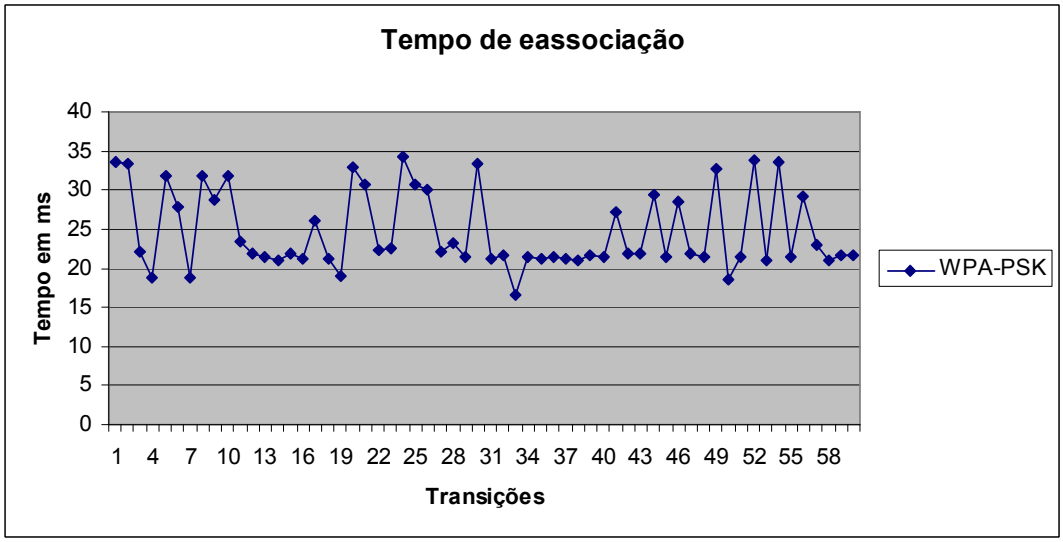


Figura 26: Tempo de reassociação de cada transição com autenticação WPA-PSK

Analisando o gráfico da figura 25, pode ser visualizado que todas as transições ocorreram no intervalo entre 15 a 35 *ms*.

Alem do método de autenticação WPA-PSK, o padrão IEEE 802.11i define o método de autenticação WPA-EAP, citado na sessão 2.3. A figura 27 mostra a troca de mensagens da autenticação EAP obtida em um experimento, contendo o início da associação, o processo de tunelamento e a troca de credenciais entre o WSTA e o servidor de autenticação.

```
15:14:56.748802 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Deauthentication, SN=1602
15:14:59.747717             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.747722 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Authentication, SN=1603,
15:14:59.748320 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Authentication, SN=2561,
15:14:59.750561             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.750566 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Association Request, SN=1
15:14:59.751298 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Association Response, SN=
15:14:59.753186 Tp-LinkT_c5 HonHaiPr_7c:a EAP     Request, Identity [RFC374
15:14:59.754746             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.754754 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Null function (No data),
15:14:59.764740             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.764746 HonHaiPr_7c Tp-LinkT_c5:d EAP     Response, Identity [RFC37
15:14:59.765326 Tp-LinkT_c5 HonHaiPr_7c:a EAP     Request, EAP-TTLS [RFC528
15:14:59.766981             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.766985 HonHaiPr_7c Tp-LinkT_c5:d EAP     Response, Legacy Nak (Res
15:14:59.767678 Tp-LinkT_c5 HonHaiPr_7c:a EAP     Request, PEAP [Palekar]
15:14:59.769640             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.769647 HonHaiPr_7c Tp-LinkT_c5:d TLSv1   Client Hello
15:14:59.775202 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Server Hello, Certificate
15:14:59.782971             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.782978 HonHaiPr_7c Tp-LinkT_c5:d TLSv1   Client Key Exchange, Char
15:14:59.793783 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Encrypted Handshake Messa
15:14:59.798066             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.798073 HonHaiPr_7c Tp-LinkT_c5:d EAP     Response, PEAP [Palekar]
15:14:59.799453 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Application Data, Applica
15:14:59.801444             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.801449 HonHaiPr_7c Tp-LinkT_c5:d TLSv1   Application Data, Applica
15:14:59.803998 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Application Data, Applica
15:14:59.815908             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.815915 HonHaiPr_7c Tp-LinkT_c5:d TLSv1   Application Data, Applica
15:14:59.817813 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Application Data, Applica
15:14:59.822424             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.822430 HonHaiPr_7c Tp-LinkT_c5:d TLSv1   Application Data, Applica
15:14:59.823648 Tp-LinkT_c5 HonHaiPr_7c:a TLSv1   Application Data, Applica
15:14:59.830753             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.830758 HonHaiPr_7c Tp-LinkT_c5:d EAP     Response, PEAP [Palekar]
15:14:59.831946 Tp-LinkT_c5 HonHaiPr_7c:a EAP     Success
15:14:59.833508 Tp-LinkT_c5 HonHaiPr_7c:a EAPOL   Key
15:14:59.839281             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.839292 HonHaiPr_7c Tp-LinkT_c5:d EAPOL   Key
15:14:59.842388 Tp-LinkT_c5 HonHaiPr_7c:a EAPOL   Key
15:14:59.848843             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
15:14:59.848849 HonHaiPr_7c Tp-LinkT_c5:d EAPOL   Key
15:14:59.950135             HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
```

Figura 27: Reassociação com autenticação WPA-EAP

Na figura 27, os cinco primeiros quadros sublinhados estão presentes entre todos os métodos de autenticação, na seqüência os quadros dentro do quadrado destacado correspondem à primeira fase da autenticação EAP, onde ocorre o tunelamento para a troca

de credenciais da segunda fase deste método de autenticação, por fim os últimos quatro quadros sublinhados, estes presentes também na autenticação PSK, corresponde a troca de credenciais, neste caso ente o WSTA e o servidor de autenticação. Neste exemplo o tempo de reassociação foi de 101,1 *ms*.

Com base nos resultados obtidos durante os testes com autenticação WPA-EAP, foi realizada uma análise estatística do tempo de associação com autenticação WPA-EAP. O gráfico representado pela figura 28 mostra os resultados dos testes usando um histograma com a duração das reassociações.

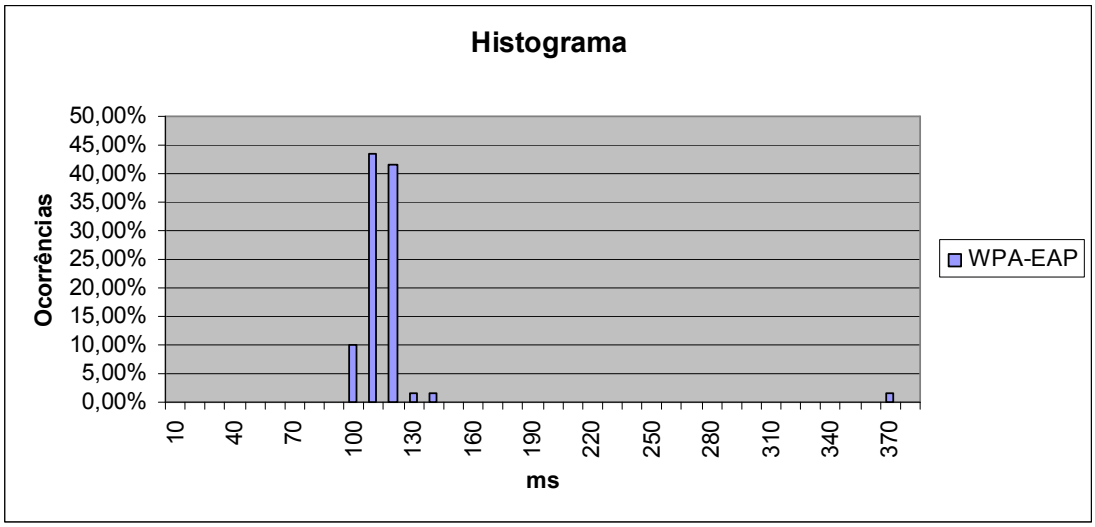


Figura 28: Distribuição das reassociações com autenticação WPA-EAP

De acordo com o gráfico da figura 28, pode ser afirmado que 53,33% das reassociações ocorreram abaixo de 110 *ms*, 98,33% das reassociações ocorreram abaixo de 140 *ms* e todas as reassociações ocorreram abaixo de 370 *ms*. Ainda com base nos resultados obtidos nos testes, foi calculado a duração média de reassociação de 112,4 *ms* e o desvio padrão de 34,58 *ms*, e assumindo esses resultados pode-se afirmar que 99,7% das reassociações ocorreram em até 216,14 *ms*. O gráfico representado pela figura 29 mostra de forma detalhada o tempo de cada reassociação.

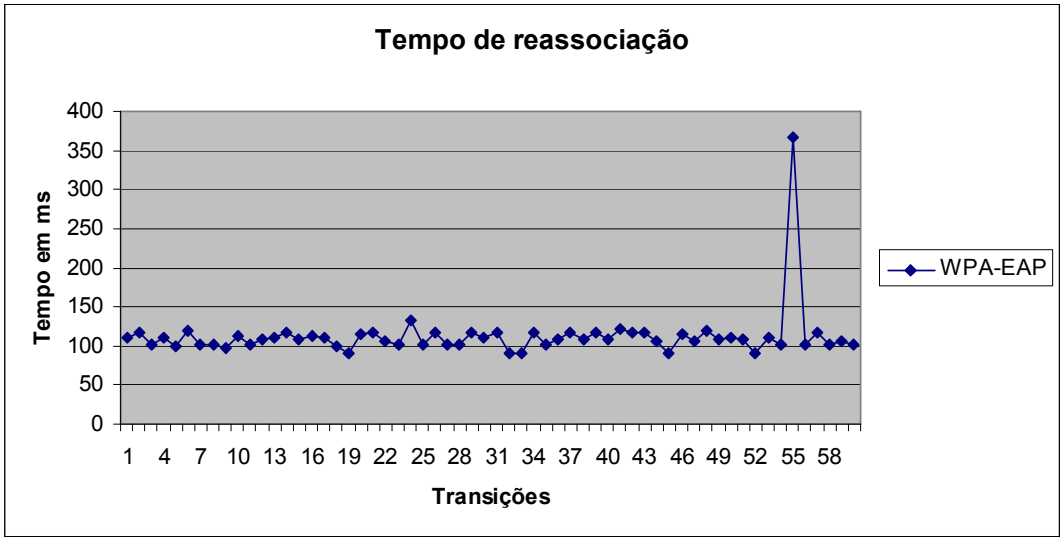


Figura 29: Tempo de reassociação de cada transição com autenticação WPA-EAP

Analisando o gráfico 3.6, pode se afirmar que as reassociações durante o teste ocorreram dentro do intervalo entre 90 e 150 *ms*, com uma ocorrência destoante de 370 *ms*.

Jitter de cada teste VoIP realizado

Durante os testes de chamada, foi possível dimensionar o jitter em cada cenário realizado, e traçado uma projeção estatística com base no desvio padrão de cada um deles. O gráfico representado pela figura 30 apresenta os resultados obtidos em relação ao jitter em cada teste realizado.

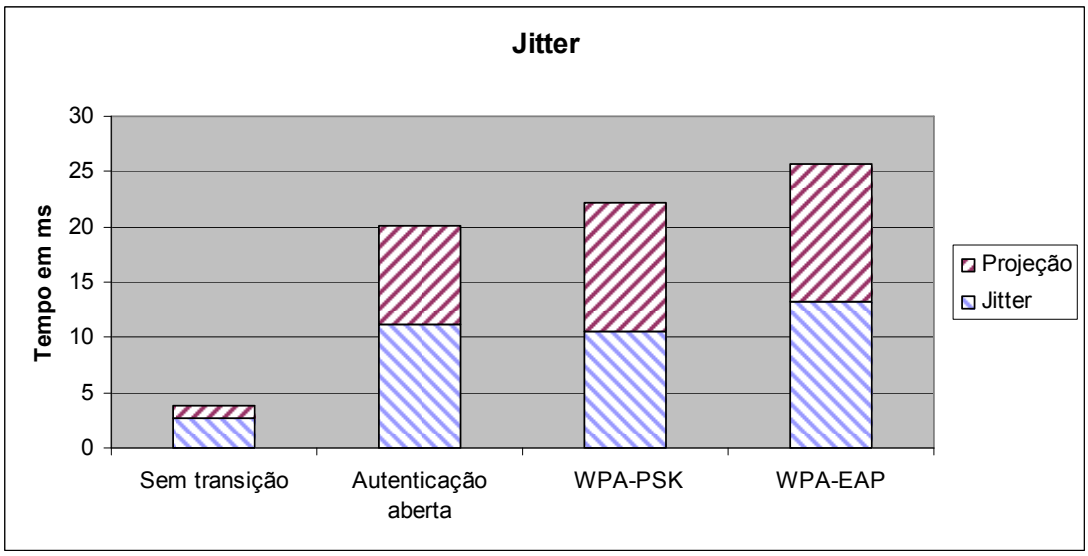


Figura 30: Jitter dos testes VoIP

Com bases nos resultados dos testes assim como no gráfico mostrado, o cenário com o melhor desempenho em relação ao *jitter* é aquele em que não foi realizado transição, a qual

apresentou um *jitter* de 3,87 *ms*. A diferença entre os resultados dos demais cenários de testes é de 5,55 *ms*, com *jitter* de 20,13 *ms* e 25,68 *ms* nos cenários com autenticação aberta e WPA-EAP, respectivamente.

O *jitter* não teve impacto sobre a qualidade da comunicação durante os testes, pois foi utilizado um *buffer* de recepção (*buffer de jitter*) de 50 *ms*. Porém quando este *buffer* foi reduzido para valores inferior a 20 *ms* a qualidade começou a ser degradada.

Perda de pacotes

Com base nos testes realizados e nos resultado obtidos, foi possível obter uma estimativa de perdas de pacote RTP das chamadas VoIP ocasionadas pelas transições. O gráfico representado pela figura 31 traça um paralelo entre a média de perda de pacotes durante as transições com uma projeção estatística de perdas calculada a partir de três vezes o desvio padrão de cada teste, considerando uma distribuição gaussiana que abrange estatisticamente 99,7% das perdas que ocorrem durante uma transição em uma comunicação ativa em caso de uma reprodução dos testes.

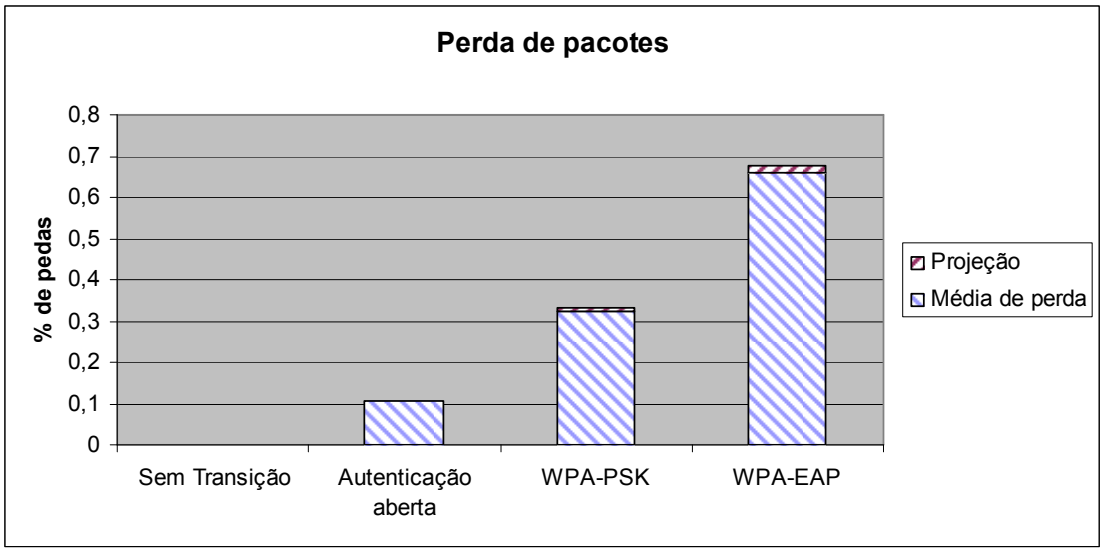


Figura 31: Média e projeção de perda de pacotes durante as transições

De acordo com o gráfico e com os resultados obtidos, o sistema de comunicação VoIP sem transição obteve 0% de perdas, e as perdas ocasionadas pelas transições cresceram gradativamente em função do método de autenticação utilizado. Nos testes em que foi realizado transição durante as chamadas, a melhor performance ocorreu no sistema de autenticação aberta, que apresentou 0,11% de perdas, o sistema com autenticação WPA-PSK apresentou 0,33% de perdas contra os 0,68% obtidos no WPA-EAP. Em todos os caso, foi levado em consideração a projeção calculada.

Durante as transições com autenticação EAP a qual o tempo de desconexão é elevado, após o restabelecimento da comunicação ocorreu oscilações de alguns *milisegundos* durante a comunicação, estabilizada em seguida.

Resultados obtidos com a aplicação da norma IEEE 802.11r

O método de autenticação utilizado no teste e proposto na norma IEEE 802.11r é equivalente ao método de autenticação IEEE 802.11i, porém mais rápido. Após a aplicação da norma, ficou evidente a redução de mensagens trocadas durante uma reassociação tanto em aplicações com autenticação FT-PSK quanto a aplicação com autenticação FT-EAP. Ambos os métodos resultaram em um mesmo número de quadros durante as transições que o sistema de autenticação abeto. Vale ressaltar que mesmo os quadros de controle obtidos durante as transições (mostrados nas figuras seguintes) serem aparentemente os mesmos que dos testes antes da aplicação da norma IEEE 802.11r, estes quadros contêm campos adicionais pertencentes ao mecanismo FT. A figura 32 mostra a troca de quadros entre o WSTA e o ponto de acesso durante uma transição rápida com autenticação PSK (FT-PSK).

```
01:12:35.946867              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:12:35.946874 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Deauthentication, SN=982,
01:12:35.948827              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:12:35.948841 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Authentication, SN=983, F
01:12:35.951683 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Authentication, SN=2976,
01:12:35.959713              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:12:35.959719 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Reassociation Request, SN
01:12:35.961834 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Reassociation Response, S
01:12:35.964487              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:13:06.359237              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:13:06.359244 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Probe Request, SN=986, FN
01:13:06.360338 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Probe Response, SN=3275,
```

Figura 32: Reassociação com autenticação FT-PSK

Na figura 3.5 todos os quadros trocados durante a transição estão sublinhados. A transição tem inicio com a deautenticação do WSTA com o ponto de acesso corrente, após o quando de deautenticação são trocados apenas quatro quadros na seqüência até que o WSTA esteja associado ao ponto de acesso alvo. No exemplo da figura 32, o tempo de reassociação foi de 13ms.

Durante os testes foram obtido informações relevantes quanto ao tempo de reassociação. Os tempos de reassociação estão expressos através do gráfico representado pela figura 33, que mostra a distribuição das reassociações em função do tempo.

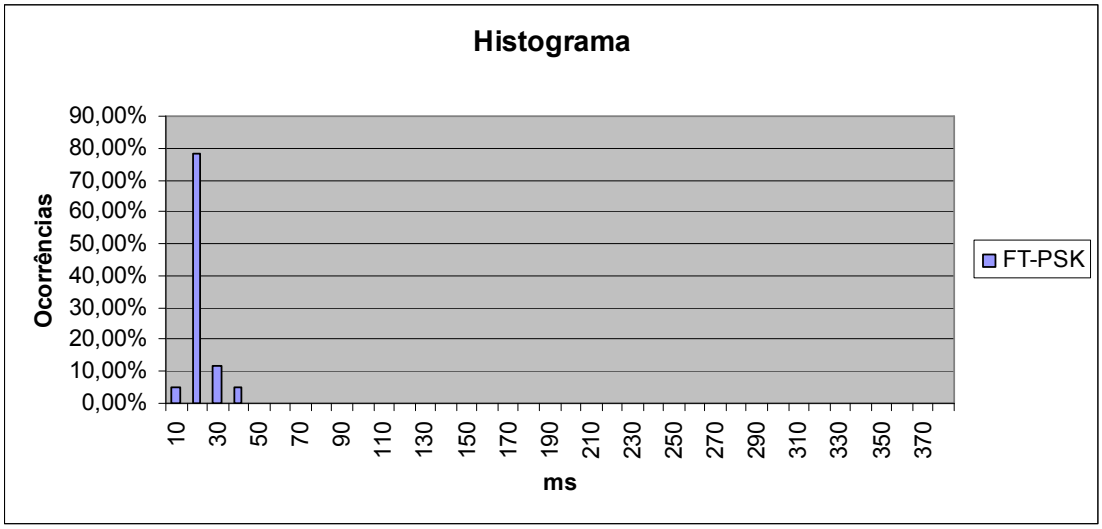


Figura 33: Distribuição das reassociações com autenticação FT-PSK

De acordo com o gráfico da figura 33, 83,33% das reassociações durante os testes ocorreram em menos de 20 *ms*, e todas em menos de 40 *ms*. Uma outra abordagem na análise é mostrada no gráfico representado pela figura 34, que apresenta detalhadamente o tempo em cada transição durante os testes com autenticação FT-PSK.

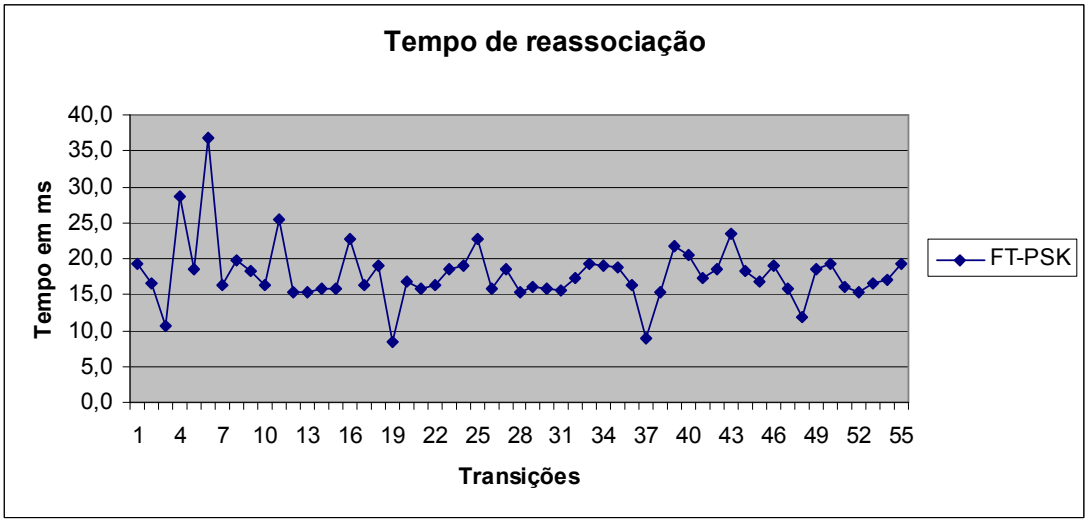


Figura 34: Tempo de reassociação de cada transição com autenticação FT-PSK

Como pode se visto no gráfico da figura 34, todas as reassociações sucedidas durante o teste com FT-PSK ocorreram no intervalo de tempo entre 7 a 39 *ms*.

Assim como na autenticação com FT-PSK, o método FT-EAP troca exatamente a mesma quantidade de quadros. Apesar da figura 35 ser muito semelhante a apresentada anteriormente, esta foi obtida dos resultados dos testes com autenticação FT-EAP.

```
01:44:27.402202              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:44:27.402212 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Deauthentication, SN=338,
01:44:27.406894              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:44:27.406901 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Authentication, SN=339, F
01:44:27.409920 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Authentication, SN=1528,
01:44:27.420803              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:44:27.420811 HonHaiPr_7c Tp-LinkT_c5:d IEEE 80 Reassociation Request, SN
01:44:27.423027 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Reassociation Response, S
01:44:27.425667              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
01:44:27.427918 Tp-LinkT_c5 HonHaiPr_7c:a IEEE 80 Data, SN=1531, FN=0, Flag
01:44:27.434916              HonHaiPr_7c:a IEEE 80 Acknowledgement, Flags=..
```

Figuras 35: Reassociação com autenticação FT-EAP

As considerações sobre a figura 35 são as mesmas da figura 32, porém neste exemplo o tempo de reassociação foi de 16,1 *ms*.

Com base nos testes realizados foi possível traçar uma estimativa em relação ao tempo de reassociação utilizando autenticação FT-EAP. O gráfico representado pela figura 36 mostra a distribuição estatísticas do tempo de reassociação.

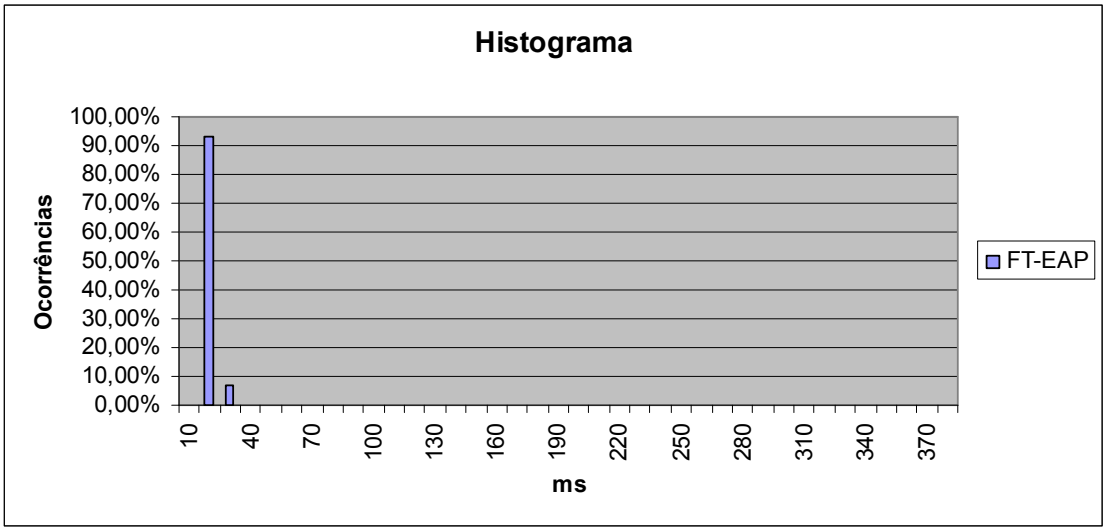


Figura 36: Distribuição das reassociações com autenticação FT-EAP

Com base nas informações mostrada no gráfico da figura 36, pode se afirmado que 93,33% das reassociações ocorreram em menos de 20ms e todas ocorreram a baixo de 30 *ms*. O gráfico representado pela figura 37 mostra o tempo de reassociação em cada transição durante o teste com autenticação FT-EAP.

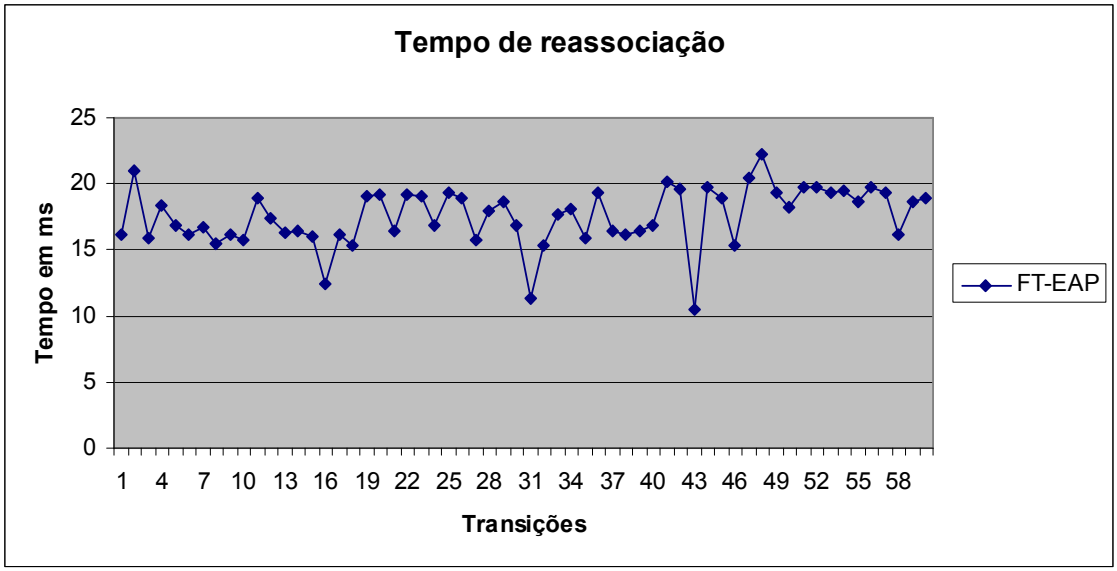


Figura 37: Tempo de reassociação de cada transição com autenticação FT-EAP

Analisando o gráfico da figura 37, é visível que todas as reassociações durantes os testes com autenticação FT-EAP ficaram no intervalo de tempo entre 10 *ms* a 23 *ms*.

Comparação e análise dos resultados

Baseado nos testes realizados foi possível constatar a dimensão do atraso de transição em estruturas de rede IEEE 802.11 e a melhora deste tempo com a aplicação da norma 802.11r. Também foi possível verificar a perda de pacotes ocasionada pelo tempo de desconexão e a degradação da qualidade em transmissões VoIP.

Para apresentação dos resultados foi utilizado gráficos que facilitam a visualização e compreensão da otimização obtida com a norma de transições rápidas. O gráfico representado pela figura 38 apresenta um histograma comparativo entre a autenticação PSK sem e com a aplicação da norma IEEE 802.11r.

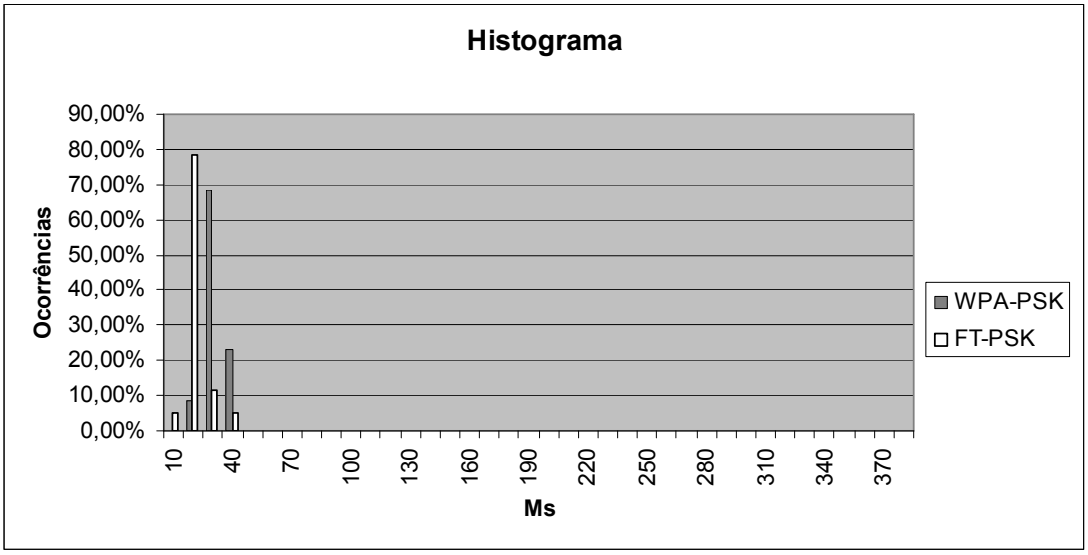


Figura 38: Histograma comparativo entre WPA-PSK e FT-PSK

A autenticação FT-PSK não correspondeu as expectativas de redução no tempo de transição, tanto na autenticação WPA-PSK quanto na FT-PSK o as autenticações ocorreram até 40 *ms*. Os resultados obtidos nos testes com autenticação EAP, com e sem a aplicação da norma, podem ser visualizados no histograma representado pela figura 39.

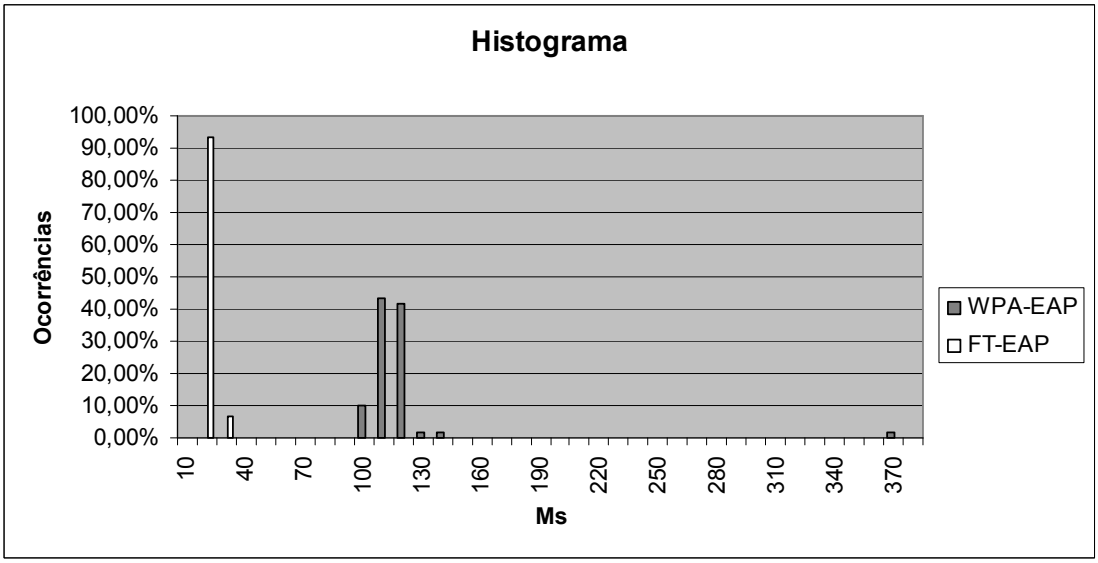


Figura 39: Histograma comparativo entre autenticação WPA-EAP e FT-EAP

De acordo com o histograma da figura 39, a aplicação da norma de transição rápida reduziu drasticamente o tempo de transição com autenticação EAP, a qual todas as transições ocorreram em até 30 *ms*.

O gráfico representado pela figura 40 apresenta o comparativo entre o tempo médio de transição em todos os métodos de autenticação testados, e traça uma projeção estatística calculada a partir de três vezes o desvio padrão com os resultados obtidos em cada teste, considerando uma distribuição gaussiana.

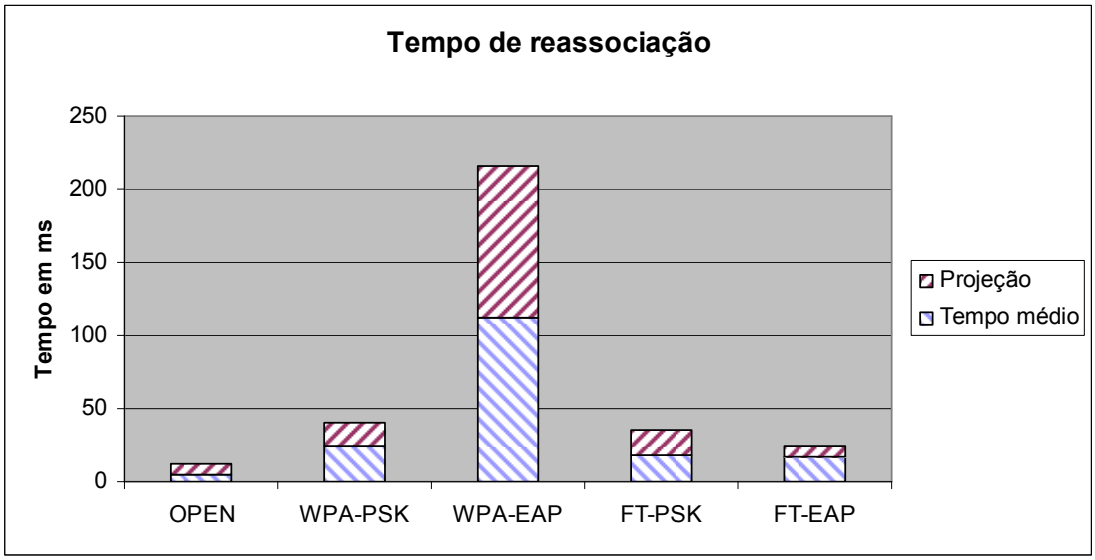


Figura 40: Comparativo entre todos métodos de autenticação

Analisando os resultados mostrados no gráfico da figura 40, é visível o ganho no tempo de reassociação com a utilização da norma IEEE 802.11r. Na aplicação FT-PSK, a redução no tempo de reassociação não é tão evidente, reduziu de 39,72ms para 35,34ms. Entretanto na aplicação com FT-EAP o tempo de reassociação reduziu de 216,15ms para 24,14ms, um tempo quase nove vezes inferior. Ambos os resultados levaram em consideração a projeção estatística.

Comparando os resultados obtidos durante os testes com todos os métodos de autenticação abordados no trabalho, o único que apresenta problemas para atender a todos os requisitos mínimos para comunicações de voz normatizados pela ITU-T, durante as transições foi o método de autenticação WPA-EAP, que apresentou um atraso de reassociação de 216,15ms, que por si só é maior que o atraso máximo proposto pelo órgão regulamentador.

Para tacar uma comparação paralela e real entre todos os métodos de autenticação utilizados durante o projeto, o gráfico representado pela figura 41 apresenta o tempo de reassociação em escala logarítmica de cada transição realizada durante os testes.

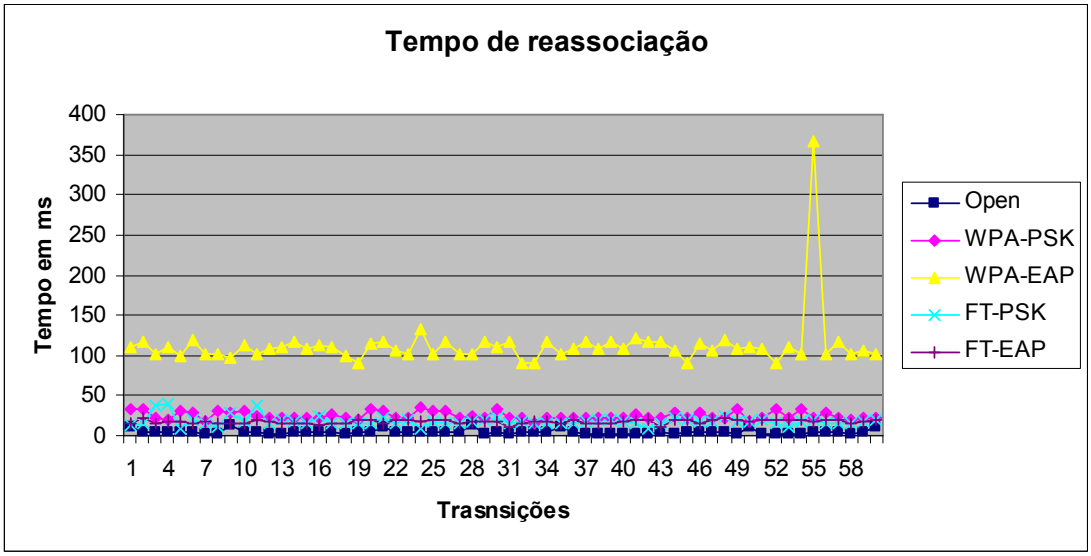


Figura 41: Comparativo entre tempo de transição de métodos de autenticação

Analisando o gráfico da figura 41, é possível ter uma idéia qualitativa em relação ao tempo de reassociação e a melhora obtida com a aplicação da norma IEEE 802.11.

5 Conclusões

As aplicações WLAN (IEEE 802.11) amplamente difundidas em empresas, residências e lugares públicos, atendem as necessidades de comunicação de aplicações em estações fixas. Porém no caso de estruturas de rede com mais de um BSS e estações móveis, o atraso de transição de BSS pode comprometer a qualidade de comunicação ou mesmo inviabilizar o funcionamento de uma aplicação. Isso é particularmente sensível em aplicações com características de tempo-real, como VoIP. Este trabalho investigou o problema de transição de BSS e o uso de técnicas propostas na norma IEEE 802.11r para sua redução. Em cenários de teste compostos por dois AP com suporte à norma IEEE 802.11r, obteve-se melhora no tempo de transição de BSS. Os atrasos de transição obtidos se situaram abaixo de 40 ms, sendo assim compatíveis com valores para atraso fim-a-fim estipulados nas recomendações ITU-T G.110 a G.119. Para fins de comparação, os atrasos de transição, *jitter* e perda de pacotes sem uso da norma IEEE 802.11r variaram entre 16,5 e 34,3 *ms*, 6,08 e 17,83 *ms* e 0,1 e 0,6 % respectivamente,no caso de uso de WPA-PSK, e 91,2 a 367,3 ms, 7,14 a 23,36 ms e 0,4 a 3 % no caso do uso de WPA-EAP. Os resultados obtidos com a aplicação da norma proposta, dão subsídios ao uso de redes IEEE 802.11 com múltiplos BSS por usuários VoIP móveis. Entretanto foi levantado outro fator que pode influenciar na degradação da qualidade de comunicação de aplicações sobre este tipo de rede, sendo ele o tempo de varredura, uma vez que a norma aplicada reduz apenas o tempo de reassociação.

Alem dos resultados positivos alcançados, o trabalho trouxe duas contribuições acadêmicas. Primeiro o estudo e o teste de desempenho da norma IEEE 802,11r como solução para redução no tempo de transição de BSS. Em segundo o estudo e aplicação do *hostapd*, um software para implantação de um ponto de acesso em um computador baseado em Linux. Esse software proporciona uma plataforma que pode ser usada como protótipo para estudo e desenvolvimento de técnicas relacionadas com redes IEEE 802.11.

Por fim, fica como proposta para trabalhos futuros a investigação do problema da descoberta de novos BSS, conhecida como varredura. A varredura se faz necessária para que uma estação móvel descubra que outros BSS existem, quando se dissocia do BSS atual. O

tempo que uma estação demora para descobrir um novo BSS contribui para o atraso de transição, e durante os experimentos se mostrou significativo, com valores entre 0,2 e 34,5 *ms*. Assim, a redução no tempo de transição de BSS implica também a melhoria no procedimento de varredura e descoberta de novos BSS.

Anexo I

Tipos de quadros 802.11

Esta subseção descreve o formato e os tipos de quadro 802.11 necessários para o entendimento do trabalho, porem não compreende o detalhamento de cada campo dos mesmos. A figura 42 representa detalhadamente um quadro 802.11.

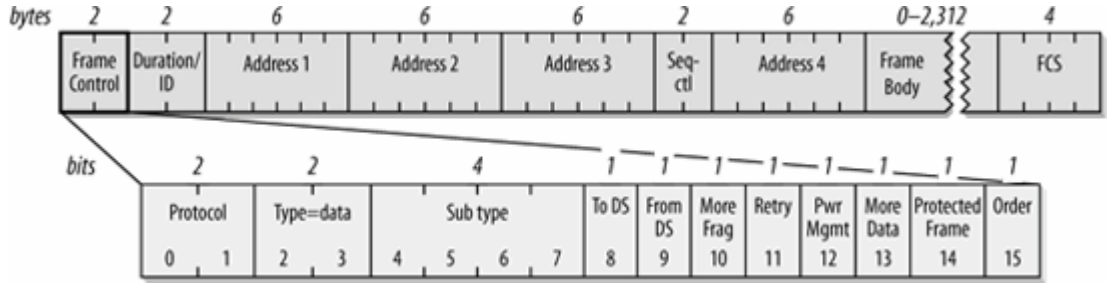


Figura 42: Detalhamento de quadro de rede 802.11

O padrão 802.11 define três categorias de quadro: quadros de gerenciamento, quadros de controle e quadros de dados.

- **Gerenciamento** – quadros utilizados para iniciar a comunicação entre a estação móvel e o ponto de acesso.
- **Controle** – são utilizados para acessar a canal e reconhecimento de quadro.
- **Dados** – transporta a informação transmitida pelas estações moveis. [Forouzan]

Os quadros de rede que serão utilizados no decorrer do trabalho compreendem apenas quadros de gerenciamento, são mostrados na tabela 8 e explicados nas sessões seguintes.

Tabela 8: Tipos de quadro de controle

Subtype (hexadecimal)	Tipo de quadro
0	Association request
1	Association response
2	Reassociation request
3	Reassociation response
4	Probe request

5	Probe response
8	Beacon
A	Disassociation
B	Authentication
C	DeAuthentication

Anexo II

Formato dos quadros de gerenciamento 802.11r

- Quadro beacon

Beacon	MDIE

Figura 43: Quadro Beacon com adaptação para FT

- Quadro association request

Association Request	MDIE

Figura 44: Quadro Association request com adaptação para FT

- Quadro association response

Association Response	MDIE	FTIE

Figura 45: Quadro Association response com adaptação para FT

- Quadro reassociation request

Reassociation Request	MDIE	FTIE	RIC

Figura 46: Quadro Reassociation request com adaptação para FT

- Quadro reassociation response

Reassociation Response	RSNIE	MDIE	FTIE	RIC

Figura 47: Quadro reassociation response com adaptação para FT

- Quadros authentication

Authentication	RSNIE	MDIE	FTIE	TIE	RIC

Figura 48: Quadros Authenticaton com adaptação para FT

- **Detalhamento dos campos adicionais**

  - **MDIE**

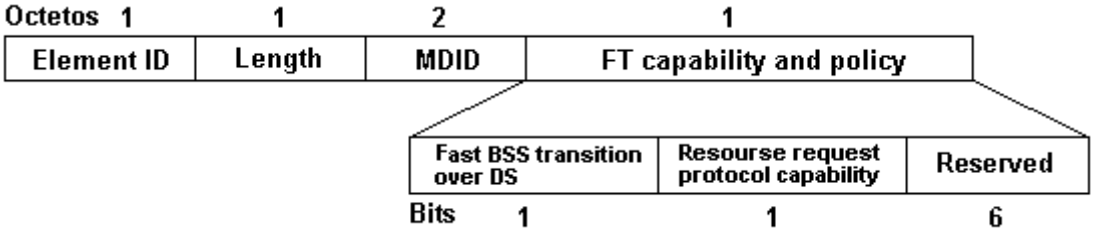


Figura 49: Detalhamento do campo MDIE

  - **FTIE**

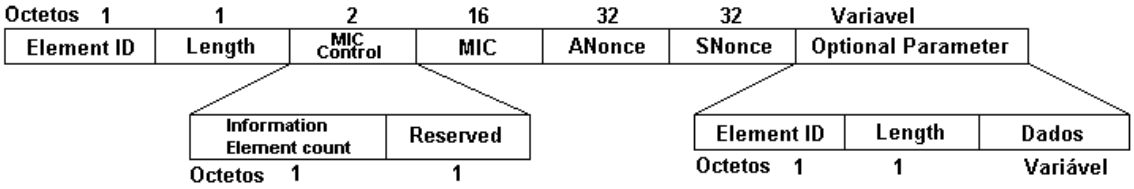


Figura 50: Detalhamento do campo FTIE

    - ANonce transporta o R1KH codificado
    - SNonce transporta o S1KH codificado

Os parâmetros opcionais do quadro FTIE são listados na tabela 2.x.

Tabela 9: Tabela dos parâmetros opcionais do campo FTIE

Subelement ID	Campo de dados	Comprimento (octetos)
0	Reservado	
1	Transporta o identificador R1KH-ID	6
2	Transporta o quadro GTK	15-42
3	Transporta o identificador R0KH-ID	1-48
4-255	Reservado	

    - **GTK**

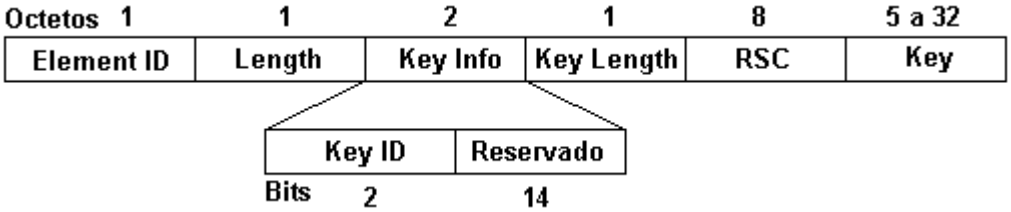


Figura 51: Detalhamento do campo GTK

- **TIE**

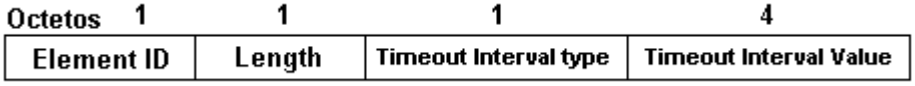


Figura 52: Detalhamento do campo TIE

Os tipos de intervalo de tempo estão expressos na tabela 2.x

Tabela 10: Tipos de intervalo de tempo

Timeout interval type	Significado	Unidade
0	Reservado	
1	Intervalo limite de reassociação	Time Units (TUs)
2	Intervalo de duração de chave	Segundos
3-255	Reservado	

- **RIC Data information Element (RDIE)**

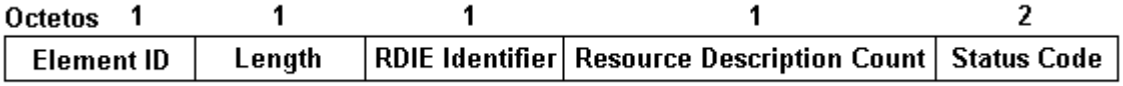


Figura 53: Detalhamento do campo RDIE

- **RIC Descriptor Information Element**

Figura 54: Detalhamento do campo RIC

- **Quadros FT**

As ações da FT são definidos em quatro formatos, que são utilizados em transições sobre o sistema de distribuição (DS). A tabela 2.x lista as ações possíveis no FT.

Tabela 11: Tipos de ação de protocolo FT

Valor do campo ação	Descrção
0	Reservado
1	FT Request frame
2	FT Response frame
3	FT Confirm frame
4	FT Ack frame
5-255	Reservado

- Quadro FT genérico

Octetos 1	1	6	6	Variavel
Category	Action	STA Address	Target AP Address	Variable

Figura 55: Detalhamento do quadro FT genérico

- FT Request frame e response

Octetos 14	Variavel		
Header	RSNIE	MDIE	FTIE

Figura 56: Detalhamento dos quadros FT request e response

- FT Confirm frame

Octetos 14	Variavel			
Header	RSNIE	MDIE	FTIE	RIC

Figura 57: Detalhamento do quadro FT Confirm

- FT Ack frame

Octetos 14	Variavel				
Header	RSNIE	MDIE	FTIE	TIE	RIC

Figura 58: Detalhamento do quadro FT Ack

Anexo III

Configuração do arquivo hostapd.conf

As configurações na seqüência não correspondem ao arquivo na integra, contém as principais configurações do arquivo e devem ser adequadas a cada caso para reprodução dos experimentos.

```
interface=wlan0
bridge=br0
driver=nl80211
ctrl_interface_group=0
ssid=teste
hw_mode=g
channel=11
auth_algs=1
ieee8021x=1
eapol_version=2
eap_message=hello
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/tcc/hostapd-0.6.10/hostapd/hostapd.eap_user
ca_cert=/tcc/ca/CA.pem
server_cert=/tcc/ca/server.pem
private_key=/tcc/ca/key-server.pem
private_key_passwd=thiago
own_ip_addr=192.168.0.3
nas_identifier=TCC
auth_server_addr=192.168.0.3
auth_server_port=1812
```

```
auth_server_shared_secret=radius
radius_server_clients=/etc/hostapd.radius_clients
radius_server_auth_port=1812
wpa=3
wpa_passphrase=senha_de_acesso_PSK
wpa_pairwise=CCMP TKIP
rsn_pairwise=CCMP TKIP
mobility_domain=a1b2
r0_key_lifetime=10000
r1_key_holder=000102030405
reassociation_deadline=1000
r0kh=02:01:02:03:04:05 TCC 000102030405060708090a0b0c0d0e0f
```

Anexo IV

Instalação do hostapd e bibliotecas necessárias

Instalação de dependências de softwares no Ubuntu Linux
apt-get install build-essential libssl-dev bridge-utils brctl

Obtenção do software hostapd no site oficial. Deve-se usar versão 0.7.2 ou superior
wget http://hostap.epitest.fi/releases/hostapd-0.7.2.tar.gz

Compilação e instalação do hostapd
tar -zxf hostapd-0.6.10.tar.gz
cd hostapd-0.7.2/hostap
cp defconfig .config
make clean
make
make install

Criação da interface bridge necessária para integrar as interfaces ethernet e sem-fio no AP
brctl addbr br0
brctl addif wlan0
brctl addif eth0
ifconfig br0 IP_da_eth0

Anexos V

Criar certificado SSL para utilização de servidor RADIUS

Os comandos na seqüência devem ser utilizados no terminal de comandos para gerar os certificados que serão utilizados pelo servidor RADIUS.

```
openssl req -newkey rsa:1024 -keyout cakey.pem -out careq.pem
openssl x509 -req -in careq.pem -extensions v3_ca  -signkey cakey.pem -out CA.pem
openssl req -newkey rsa:1024 -nodes -keyout key-server.pem -out servereq.pem
openssl x509 -req -in servereq.pem -out server.pem -extensions v3_usr -CA CA.pem -CAkey cakey.pem -CAcreateserial
```

Anexos VI

Configuração do arquivo de compilação .config do hostapd

As configurações a seguir, correspondem aos itens do arquivo que devem ser descomentadas para a compilação do hostapd, isto para reproduzir os experimentos realizados.

```
CONFIG_L2_PACKET=y
CONFIG_DRIVER_NL80211=y
CONFIG_EAP=y
CONFIG_EAP_MD5=y
CONFIG_EAP_TLS=y
CONFIG_EAP_MSCHAPV2=y
CONFIG_EAP_PEAP=y
CONFIG_EAP_TTLS=y
CONFIG_RADIUS_SERVER=y
CONFIG_IEEE80211R=y
```

Anexo VII

Configuração do arquivo de cliente radius hostapd.eap_user

Este anexo contém todo o conteúdo deste arquivo de configuração, para repetir os experimentos modificar apenas o usuário e senha.

```
#"user"            MD5   "password"
#"test user"       MD5   "secret"
#"example user"    TLS
#"DOMAIN\user"     MSCHAPV2   "password"
#"gtc user"        GTC   "password"
#"pax user"        PAX   "unknown"
#"pax.user@example.com"     PAX   0123456789abcdef0123456789abcdef
#"psk user"        PSK   "unknown"
#"psk.user@example.com"     PSK   0123456789abcdef0123456789abcdef
#"sake.user@example.com"    SAKE
   0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
#"ttls"            TTLS
#"not anonymous"       PEAP
# Default to EAP-SIM and EAP-AKA based on fixed identity prefixes
#"0"*               AKA,TTLS,TLS,PEAP,SIM
#"1"*               SIM,TTLS,TLS,PEAP,AKA
#"2"*               AKA,TTLS,TLS,PEAP,SIM
#"3"*               SIM,TTLS,TLS,PEAP,AKA
#"4"*               AKA,TTLS,TLS,PEAP,SIM
#"5"*               SIM,TTLS,TLS,PEAP,AKA
# Wildcard for all other identities
#*         PEAP,TTLS,TLS,SIM,AKA
*          TTLS,PEAP
```

```
# Phase 2 (tunnelled within EAP-PEAP or EAP-TTLS) users
#"t-md5"            MD5   "password"     [2]
#"DOMAIN\t-mschapv2"          MSCHAPV2   "password"     [2]
#"t-gtc"            GTC   "password"     [2]
#"not anonymous"          MSCHAPV2   "password"     [2]
#"user"             MD5,GTC,MSCHAPV2       "password"     [2]
#"test user"        MSCHAPV2   hash:000102030405060708090a0b0c0d0e0f [2]
#"ttls-user"        TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP,TTLS-MSCHAPV2
    "password"     [2]
"usuario"  TTLS-MSCHAPV2,TTLS-CHAP,TTLS-MSCHAP,TTLS-PAP,MSCHAPV2
    "senha"        [2]
# Default to EAP-SIM and EAP-AKA based on fixed identity prefixes in phase 2
#"0"*               AKA   [2]
#"1"*               SIM    [2]
#"2"*               AKA   [2]
#"3"*               SIM    [2]
#"4"*               AKA   [2]
#"5"*               SIM    [2]
```

Lista de Acrônimos

ACK – Acknowledge

BSS - Basic Service Set

CODEC - Codificador Decodificador

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DS - Distribution System

DSSS - Direct Sequence Spread Spectrum

EAP - Extensible Authentication Protocol

EAPOL - Extensible Authentication Protocol over LAN

ESS - Extended Service Set

FDM - Frequency Division Multiplexing

FHSS - Frequency Hopping Spread Spectrum

FIFO - First In, First Out

FT - Fast Transition

FT-EAP - Fast Transition Extensible Authentication Protocol

FTIE - Fast BSS Transition Information Element

FT-PSK - Fast Transition Pre-Shared Key

HTTP - Hypertext Transfer Protocol

IBSS - Independent Basic Service Set

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP - Internet Protocol

ITU-T - International Telecommunications Union – Telecomunications

LAN - Local Area Network

MAC - Medium Access Control

MD - Mobility Domain

MDIE - Mobility Domain Information Element

OFDM - Orthogonal Frequency-Division Multiplexing

PABX - Private Branch Exchange

PC - Personal Computer

PDU - Protocol Data Unit

PHY - Physical layer

PMK - Pairwise Master Key

PMK-R0 - Parwise Master Key, frist level

PMK-R1 - Parwise Master Key, second level

PSK - Pre-Shared Key

PSTN - Public switched telephone network

PTK - Pairwise Transient Key

R0KH - PMK-R0 Key Holder in the Authenticator

R0KH-ID - PMK-R0 Key Holder Identifier in the Authenticator

R1KH - PMK-R1 Key Holder in the Authenticator

R1KH-ID - PMK-R1 Key Holder Identifier in the Authenticator

RADIUS - Remote Authentication Dial In User Service

RDIE - RIC Data Information

RIC - Resource Information Container

RTCP - Realtime Transport Control Protocol

RTP - Real-time Transport Protocol

SIP - Session Initiation Protocol

SMTP - Simple Mail Transfer Protocol

SSID - Service Set Identifier

TCP - Transmission Control Protocol

TDM - Time division multiplexing

TIE - Timeout Interval Infrmation Element

UDP - User Datagram Protocol

VoIP - Voice over Internet Protocol

VoWiFi - Voice over WiFi

WDS - Wireless Distribution System

WEP - Wired Equivalent Privacy

WLAN - Wireless Local Area Network

WPA - Wi-Fi Protected Access

WPA-EAP - Wi-Fi Protected Access Extensible Authentication Protocol

WPA-PSK - Wi-Fi Protected Access Pre-Shared Key

WSTA - Wireless Station

Referências Bibliográficas

BANGOLAE, S.; Performance Study of Fast BSS Transition using IEEE 802.11r,

ERGEN, M.; Tutorial 802.11, Mustafa Ergen, 2002, Universidade da Califórnia Berkeley

FOROUZAN, B. A.;Data Communications and Networking, 2007, 4ª edição

GAST, M.; 802.11® Wireless Networks The Definitive Guide, 2005, editora O'Reilly

GEIER, J.; Implementing 802.1x Security Solutions, 2008

GOLENIEWSKI, L; Telecommunications Essentials, Lillian Goleniewski, 2002, editora Addison-Wesley

IEEE, IEEE 802.11r - Fast Basic Service Set (BSS) Transition, 2008

IEEE, IEEE 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007

IETF, RFC 3261 – SIP: Session Initiation Protocol, 2002

IETF, RFC 3550 - RTP: A Transport Protocol for Real-Time Applications, 2003

ITU-T; Recommendation G.114 , 2003

JESZENSKY, P. J. E.; Sistemas telefonicos, 2004, editora Manole, 1ª Edição

LEONEL, J.; Voz sobre IP, A revolução na Telefonia, 2003, publicação Promon Business & Technology Review.

NIST, (National Institute of Standads and Tecnology); Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, 2007

WARD, M.; Understand the design challenges of VoWi-Fi