5
Avaliação e Análise dos Resultados

Este capítulo tem, por objetivo, apresentar e fazer a avaliação e análise dos resultados obtidos na implementação dos mecanismos de segurança especificados no capítulo 4.

5.1
Experimentos Realizados

a) Rede com 01 cliente configurado em 11Mbps.
Parâmetros medidos para tráfegos FTP e HTTP:

- ⇨ *Throughput* (Bytes/seg)
- ⇨ *Throughput* (Mbps)
- ⇨ Tempo de Resposta (segundos)
- ⇨ Número de Pacotes Transmitidos
- ⇨ Tamanho Médio do Pacote
- ⇨ Quantidade de Bytes Transmitidos

b) Rede com 01 cliente configurado em 11Mbps.
Parâmetro medido para cada mecanismo de segurança externo:

- ⇨ Tempo de Autenticação (segundos)

c) Rede com 01 cliente interligado diretamente ao HUB (10Mbps).
Parâmetros medidos para tráfegos FTP e HTTP:

- ⇨ *Throughput* (Mbps)
- ⇨ Tempo de Resposta (segundos)

d) Rede com 01 cliente interligado diretamente ao SWITCH (100Mbps).
Parâmetros medidos para tráfegos FTP e HTTP:

- ⇨ *Throughput* (Mbps)
- ⇨ Tempo de Resposta (segundos)

e) Rede com 02 clientes configurados em 11Mbps.

Parâmetros medidos para tráfego FTP:

⇨ *Throughput* (Mbps)

⇨ Tempo de Resposta (segundos)

f) Rede com 02 clientes configurados em 1Mbps e 11Mbps.

Parâmetros medidos para tráfego FTP:

⇨ *Throughput* (Mbps)

⇨ Tempo de Resposta (segundos)

g) Rede com 03 clientes configurados em 11Mbps.

Parâmetros medidos para tráfego FTP:

⇨ *Throughput* (Mbps)

⇨ Tempo de Resposta (segundos)

h) Rede com 04 clientes configurados em 11Mbps.

Parâmetros medidos para tráfego FTP:

⇨ *Throughput* (Mbps)

⇨ Tempo de Resposta (segundos)

O Apêndice A contém as planilhas com os valores medidos para cada experimento.

5.2
Sistema Sem Autenticação Externa

Nesta situação, foram simulados os seguintes mecanismos:

a) *Sistema Sem segurança*

b) *Pelo Controle do Endereço MAC*

c) *WEP 64 Bits*

d) *WEP 128 bits*

Parâmetros medidos:

a) *Throughput* (Bytes/seg)

b) *Throughput* (Mbps)

c) Tempo de Resposta (segundos)
d) Número de pacotes transmitidos no período
e) Tamanho médio do pacote
f) Quantidade de bytes transmitidos

Calculou-se o valor médio e a variância de cada parâmetro das 15 medições realizadas em cada experimento.

A tabela a seguir contém a consolidação dos valores médios de *Throughput,* e de Tempo de Resposta, para cada mecanismo e para cada protocolo de aplicação.

Pelos valores calculados, observa-se que o comprometimento na *performance* da rede, devido aos mecanismos definidos pelo padrão IEEE 802.11b, é praticamente desprezível. A ativação do WEP, seja de 64 ou de 128bits, não ocasiona impacto ao desempenho da rede.

	FTP		**HTTP**	
	Throughput (Mbps)	$T_{Resposta}$ (seg)	*Throughput* (Mbps)	$T_{Resposta}$ (seg)
	Valor Médio	Valor Médio	Valor Médio	Valor Médio
Sem Segurança	5,4056	10,050	0,0722	23,218
Controle MAC	5,4126	10,036	0,0721	23,136
WEP 64 bits	5,4021	10,035	0,0720	23,122
WEP 128 bits	5,4092	10,043	0,0717	23,123

Tabela 4: Consolidação dos valores médios de *throughput* e tempo de resposta (mecanismos sem autenticação externa)

Os gráficos a seguir ilustram o *Throughput* e o *Tempo de Resposta* para cada protocolo de aplicação.

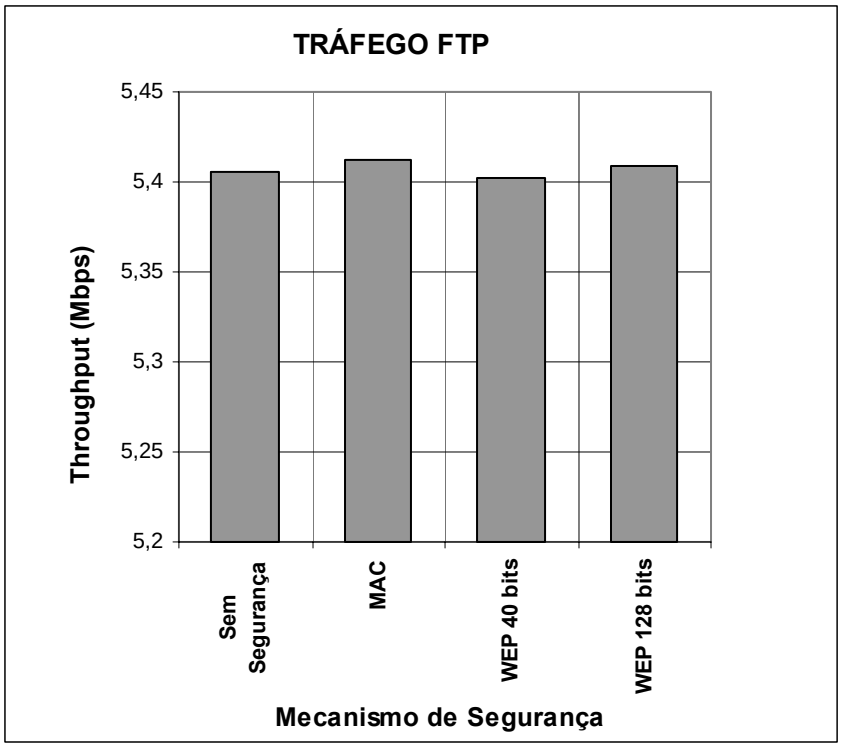

Figura 63: Valor médio de *throughput* - sem autenticação externa (Tráfego FTP)

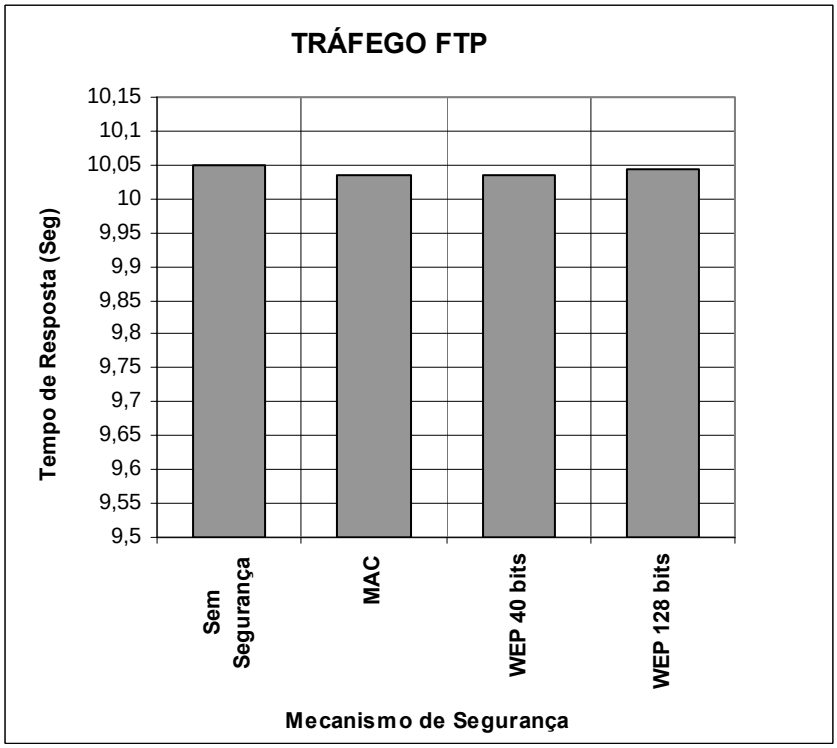

Figura 64: Valor médio do tempo de resposta - sem autenticação externa (Tráfego FTP)

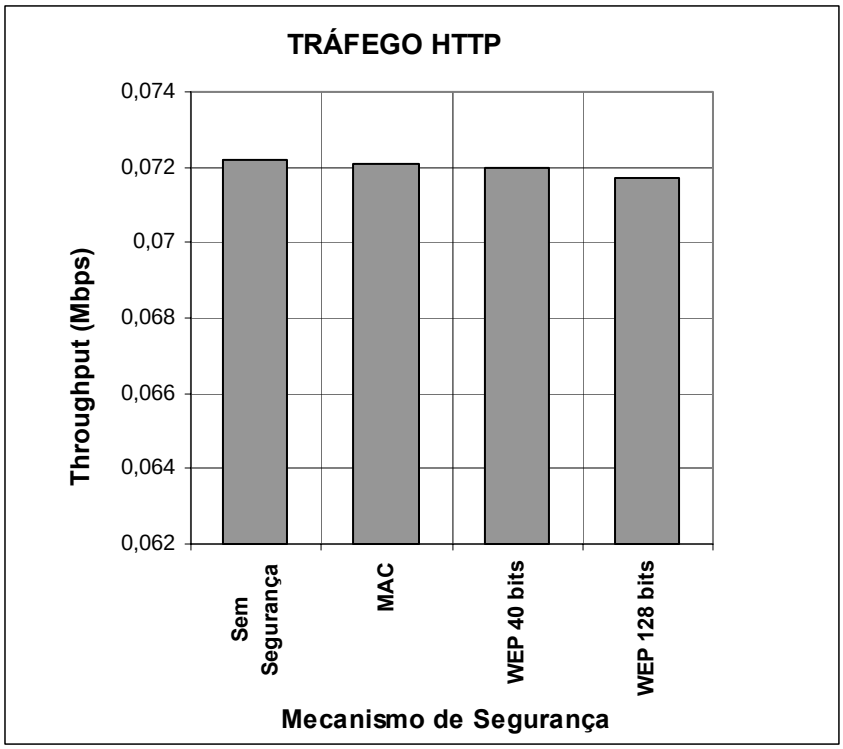

Figura 65: Valor médio de *throughput* - sem autenticação externa (Tráfego HTTP)

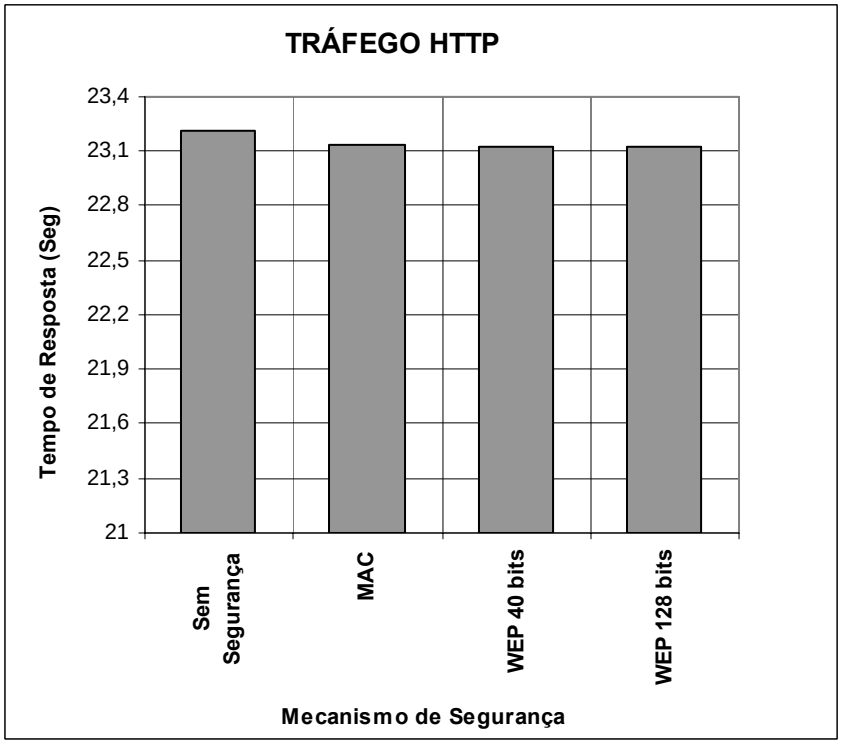

Figura 66: Valor médio do tempo de resposta - sem autenticação externa (Tráfego HTTP)

Na análise dos resultados obtidos, observa-se que:

a) Não há influência sobre a *performance* da rede quando se implementa qualquer mecanismo de segurança intrínseco do padrão IEEE 802.11b;

b) A pequena diferença entre os mecanismos deve-se basicamente à influência das condições e configurações da rede e dos equipamentos utilizados;

c) O desempenho, para cada tipo de tráfego, varia bastante, porém, não devido à rede sem fio, e sim ao funcionamento dos protocolos FTP e HTTP;

d) O tráfego FTP é influenciado pela rede sem fio. O valor médio de *Throughput* para a aplicação FTP está limitado pelo mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) de acesso ao meio, baseado no modo DCF (*Distributed Coordination Function*);

e) O tráfego HTTP não é influenciado pela rede sem fio. As características do protocolo HTTP reduzem substancialmente o desempenho, independente de se adotar ou não um modelo de segurança;

f) Para aumentar a segurança em uma rede desprovida de autenticação externa, deve-se implementar o WEP com 128bits, pois, como observado, não há comprometimento no desempenho da rede.

5.3
Sistema Com Autenticação Externa

Nesta situação, foram simulados os seguintes mecanismos:

a) *EAP-TLS*
b) *PEAP*
c) *EAP-TTLS*
d) *LEAP*

Para a configuração com autenticação externa, os parâmetros foram medidos em dois pontos distintos, de forma a se observar o tráfego da Estação Móvel para o AP, e do AP para o RADIUS.

Foram definidos 02 pontos de coleta e medição dos dados.

a) Medição no cliente. Esta medição permite:
   - ⇨ Analisar os pacotes do protocolo EAP;
   - ⇨ Medir o tempo de resposta total.

b) Medição em um computador medidor/coletor.

⇨ Analisar os pacotes do RADIUS;

Parâmetros avaliados em cada ponto de medição:

a) *Throughput* (Bytes/seg)

b) *Throughput* (Mbps)

c) Tempo de Resposta (segundos)

Calculou-se o valor médio e a variância de cada parâmetro das 15 medições realizadas em cada experimento.

A tabela a seguir contém a consolidação dos valores médios de *Throughput,* e de Tempo de Resposta, para cada mecanismo e para cada protocolo de aplicação.

	FTP		**HTTP**	
	Throughput (Mbps)	$T_{Resposta}$ (seg)	*Throughput* (Mbps)	$T_{Resposta}$ (seg)
	Valor Médio	Valor Médio	Valor Médio	Valor Médio
Sem Segurança	5,4056	10,050	0,0722	23,218
Controle MAC	5,4126	10,036	0,0721	23,136
WEP 64 bits	5,4021	10,035	0,0720	23,122
WEP 128 bits	5,4092	10,043	0,0717	23,123
EAP-TLS	5,3990	10,062	0,0708	23,657
PEAP	5,3795	10,099	0,0723	23,240
EAP-TTLS	5,4060	10,048	0,0719	23,185
LEAP	5,3802	10,097	0,0695	23,797

Tabela 5: Consolidação dos valores médios de *throughput* e tempo de resposta (todos os mecanismos)

Os gráficos a seguir ilustram o *Throughput* e o *Tempo de Resposta* para cada protocolo de aplicação.

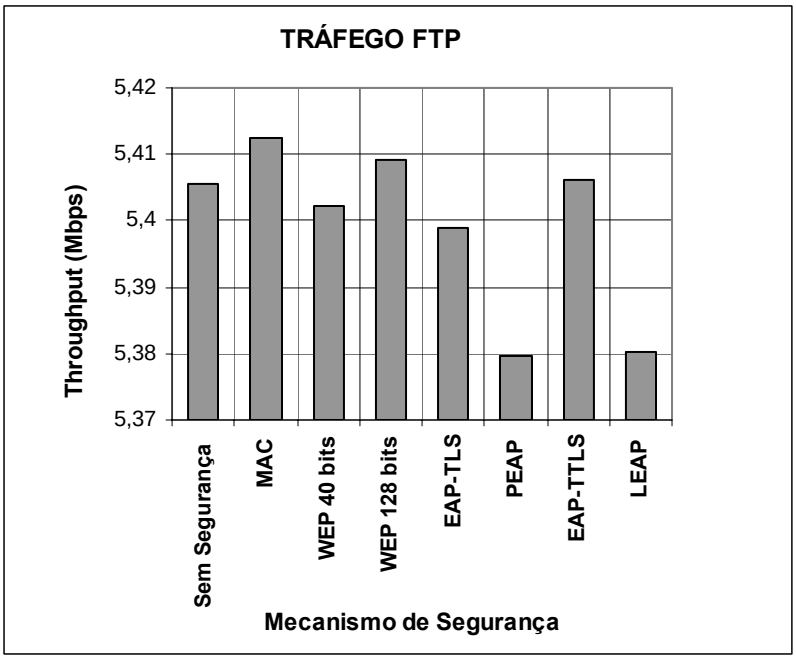

Figura 67: Valor médio de *throughput* (Tráfego FTP)

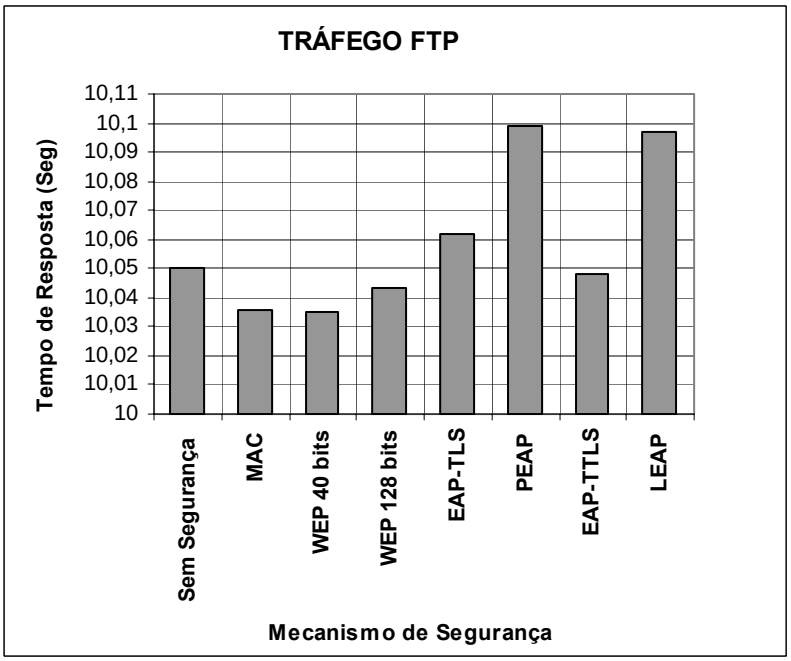

Figura 68: Valor médio do tempo de resposta (Tráfego FTP)

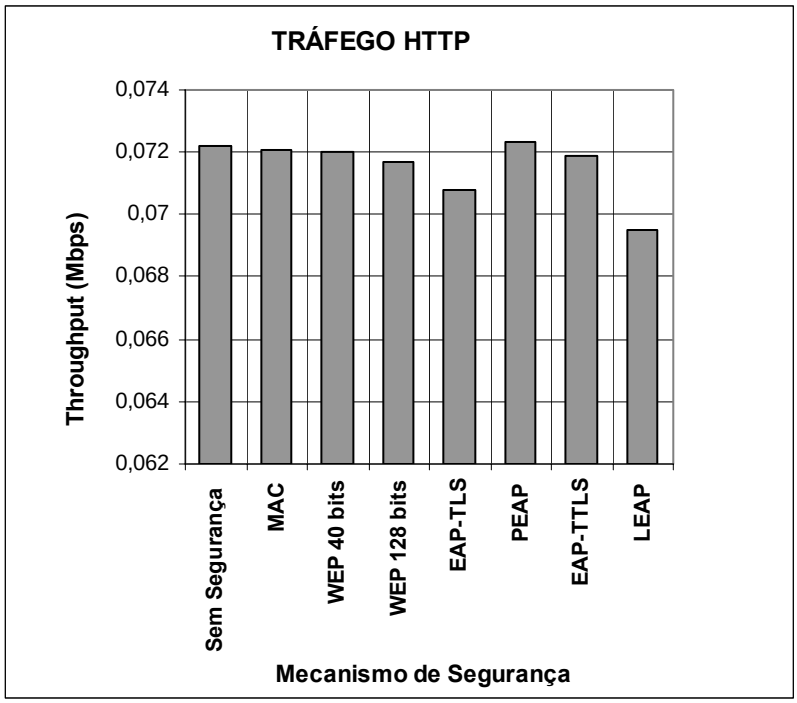

Figura 69: Valor médio de *throughput* (Tráfego HTTP)

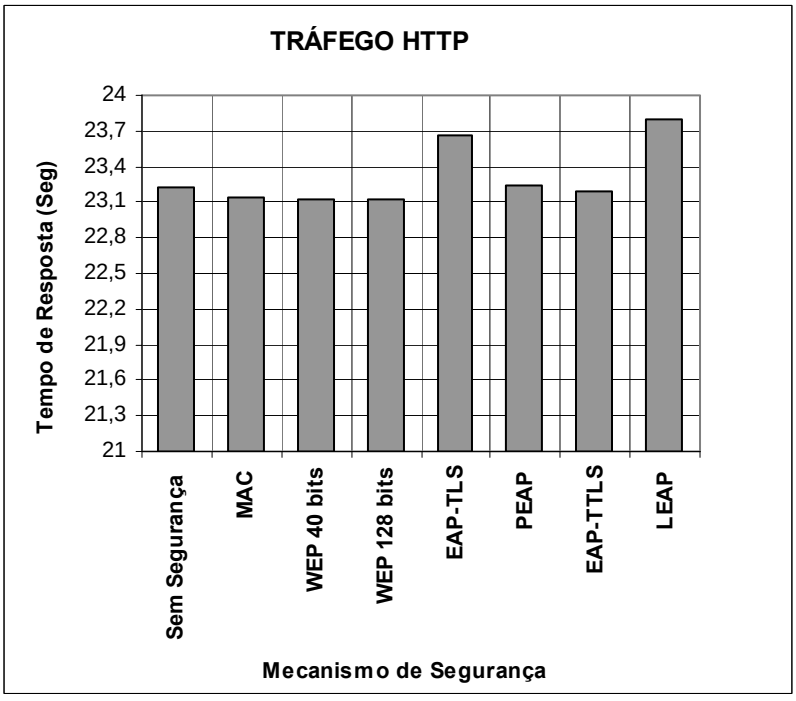

Figura 70: Valor médio do tempo de resposta (Tráfego HTTP)

Pelos valores calculados, observa-se que o comprometimento na *performance* da rede, devido aos mecanismos com autenticação externa implementados com o padrão IEEE 802.1x, com servidor RADIUS e com o WEP de 128 bits ativado, é praticamente desprezível, sendo o impacto maior para o PEAP e LEAP.

5.4
Análise do Impacto dos Mecanismos no Desempenho

O *Throughput* para o protocolo FTP é muito influenciado pelas condições e configurações da rede. Observa-se que o *Throughput* obtido é basicamente o máximo possível em uma rede IEEE 802.11b, devido aos procedimentos de contenção, conforme discutido no capítulo 2. Ou seja, o *Throughput* para o protocolo FTP, é limitado pela rede sem fio e não pelo *overhead* inserido nos mecanismos de segurança, ou pelos equipamentos externos interligados ao AP.

O *Throughput* para o protocolo HTTP já é influenciado pelo funcionamento do protocolo, não sendo dependente da rede sem fio. Ou seja, o *Throughput* para o HTTP é limitado pelo próprio protocolo.

Com o objetivo de validar as medidas obtidas, realizou-se dois experimentos sem o *access point*. Um com a presença do HUB de 10Mbps, e outro com um Switch de 100Mbps.

Na transação com os protocolos FTP e HTTP, foram obtidos os seguintes valores médios utilizando o HUB:

FTP		**HTTP**	
Throughput (Mbps)	$T_{Resposta}$ (seg)	*Throughput* (Mbps)	$T_{Resposta}$ (seg)
9,552	5,772	0,071	23.318

Tabela 6: *Throughput* e Tempo de Resposta (HUB)

Na transação com os protocolos FTP e HTTP, foram obtidos os seguintes valores médios utilizando o Switch:

FTP		HTTP	
Throughput (Mbps)	$T_{Resposta}$ (seg)	*Throughput* (Mbps)	$T_{Resposta}$ (seg)
75,673	0,723	0,071	23,314

Tabela 7: *Throughput* e Tempo de Resposta (*Switch*)

Na análise dos resultados obtidos, observa-se que:

a) A influência sobre a *performance* da rede, quando se implementa qualquer mecanismo de segurança, é pequena, sendo a degradação mais acentuada para os modelos PEAP e LEAP;

b) O desempenho para cada tipo de tráfego varia bastante, porém, não devido à rede sem fio, e sim ao funcionamento dos protocolos FTP e HTTP;

c) O tráfego FTP é influenciado pela rede sem fio. O valor médio de *Throughput* para a aplicação FTP está limitado pelo mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) de acesso ao meio, baseado no modo DCF (*Distributed Coordination Function)*;

d) O tráfego HTTP não é influenciado pela rede sem fio. As características do protocolo HTTP reduzem substancialmente o desempenho, independente de se adotar ou não um modelo de segurança;

e) Para aumentar a segurança em uma rede desprovida de autenticação externa, deve-se implementar o WEP com 128bits, pois, como observado, não há comprometimento no desempenho da rede;

f) Para aumentar a segurança em uma rede onde é possível se implementar um servidor RADIUS, deve-se adotar um dos três mecanismos: EAP-TLS, PEAP ou EAP-TTLS, em conjunto com o WEP 128bits para criptografia;

g) Deve-se evitar o mecanismo LEAP, pois, além de ser proprietário da CISCO, sua segurança é a mais baixa dentre todos os mecanismos com autenticação externa.

O EAP-TLS é uma solução para um sistema que implementa autenticação externa, pois o impacto no desempenho é pequeno, quando

comparado a qualquer mecanismo intrínseco do Padrão IEEE 802.11b. O EAP-TLS deve ser adotado caso a instituição/empresa possua certificado emitido por autoridade certificadora, tanto para o servidor quanto para o cliente. Este mecanismo tem a vantagem do usuário não precisar de *login* e *password*. Porém, é muito dispendioso devido à necessidade do certificado, e por gerar muito trabalho de administração em sua geração, controle e distribuição aos usuários.

O EAP-TTLS é a melhor solução, quando se é possível implementar a autenticação externa, pelos seguintes motivos:

1) Tem o melhor desempenho quando comparado com os mecanismos com autenticação externa;

2) É o mais viável para uma pequena e média empresa/instituição, pois não necessita de certificado no cliente. Por sua vez, para aplicações comerciais, haverá necessidade de aquisição e instalação de um Cliente de Autenticação.

O PEAP tem o pior desempenho. Porém, tem a grande vantagem de ser suportado pelo Windows, diferentemente do EAP-TTLS, que necessita de um Cliente de Autenticação, e não exigir certificado no cliente (usuário), o que facilita e reduz o custo de implementação.

5.5
Avaliação do Tempo de Autenticação

Um importante parâmetro a ser analisado nos sistemas com autenticação externa é o tempo médio para autenticação de um usuário. A cada autenticação, é gerada uma nova chave de sessão para ser utilizada pelo WEP na criptografia dos dados, na parte sem fio.

Mesmo ao usar o gerenciamento de chave dinâmica do padrão 802.1x e o WEP de 128 bits, é possível que determinados usuários mal–intencionados utilizem falhas de criptografia do WEP para realizar ataques de força bruta, descobrir a chave de criptografia e acessar dados potencialmente confidenciais. Essas técnicas são bem conhecidas e documentadas. Elas requerem que o usuário

mal–intencionado capture uma quantidade significativa de tráfego de rede e utilize recursos rápidos de computação para montagem de uma biblioteca <*chave, IV*>.

A primeira estratégia para reduzir ameaças à chave de criptografia WEP é garantir que as chaves de sessão do usuário sejam atualizadas, periodicamente, e em intervalos de tempo inferiores ao tempo necessário para capturar o tráfego e executar as operações de força bruta.

A solução consiste na configuração do servidor RADIUS para que seja aplicada a outra autenticação automática do cliente a intervalos de tempo pré-definidos e, assim, possibilitar a geração de uma nova chave de sessão de criptografia para o WEP com curta duração.

O tempo de outra autenticação dependerá da(o):

a) Quantidade de usuários na rede. Neste caso, deve-se estimar o número de autenticações por segundo que podem ser esperadas de uma determinada população de usuários;

b) *Valor* dos dados para empresa/instituição;

c) Sofisticação dos possíveis usuários mal–intencionados;

d) Tipo de aplicação normalmente trafegada na rede;

e) Carga maior no servidor RADIUS na nova autenticação dos usuários.

As opções de autenticação têm um efeito significativo na carga do servidor RADIUS. Protocolos como o PEAP executam uma operação de chave pública que exige muito da CPU durante o *logon* inicial, apesar de, para routras autenticações subseqüentes, serem usadas informações armazenadas em *cache*, permitindo o que é conhecido como "*reconexão rápida*" [*Microsoft*].

Deve-se considerar a carga de estado constante quando os usuários estiverem se autenticando normalmente e, a carga de "*pior caso*", durante horários de pico.

Deve-se considerar também a sobrecarga em caso de falha no sistema, o que exige a nova autenticação, imediata, de todos os usuários. O tempo para essa nova autenticação é realmente significativo, e deve ser levado em consideração no projeto da WLAN.

Com o objetivo de mensurar o tempo médio de autenticação de um usuário, foram realizados experimentos com cada mecanismo de segurança com autenticação externa.

As planilhas com os valores obtidos encontram-se no Apêndice A.

Para este experimento, configurou-se o servidor RADIUS para realizar uma nova autenticação do usuário a cada 60 segundos. Este tempo é pequeno e foi definido somente para avaliação do tempo de autenticação. Para um caso prático, este tempo deve ser de 10 a 60 minutos [*Microsoft*] e [Alfa & Ariss], dependendo das condições de projeto.

O tempo de autenticação foi calculado pela subtração do tempo de fim e início do processo de autenticação, conforme descrito abaixo:

$T_{Início}$*: Tempo de início do processo de autenticação*

T_{Fim}*: Tempo de fim do processo de autenticação*

T_{Aut}*:* $T_{Fim} - T_{Início}$

Calculou-se o valor médio e a variância do Tempo de Autenticação das 15 medições realizadas.

A tabela a seguir contém a consolidação dos valores médios do Tempo de Autenticação para todos os mecanismos, tanto no cliente, quanto no coletor.

	Tempo de Autenticação (seg)	
	Medição no CLIENTE	Medição no COLETOR
EAP-TLS	0,126	0,115
PEAP	0,093	0,083
EAP-TTLS	0,255	0,244
LEAP	-	0,018

Tabela 8: Consolidação dos valores médios do tempo de autenticação

O gráfico a seguir ilustra o *Tempo de Autenticação* para cada mecanismo.

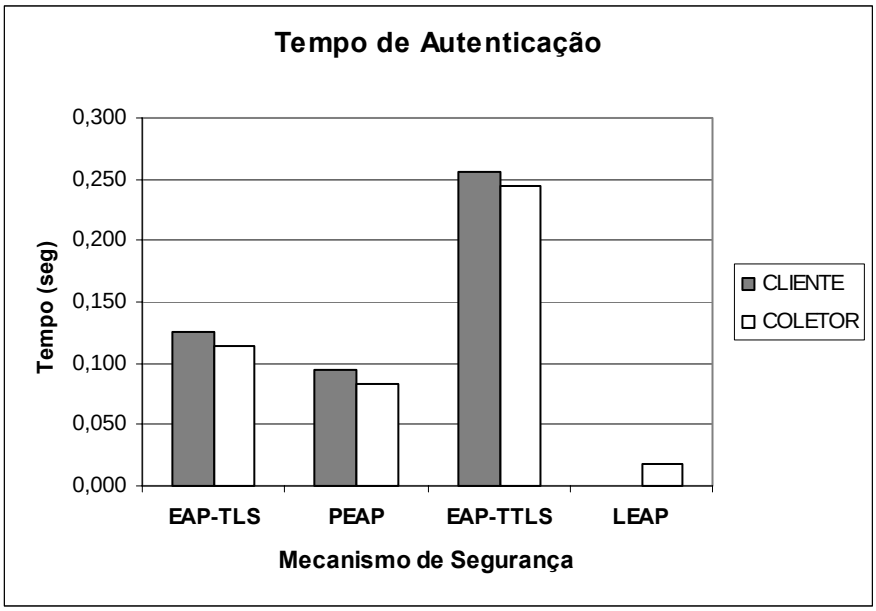

Figura 71: Tempo de Autenticação

Na análise dos resultados obtidos, observa-se que:

a) O menor tempo de autenticação corresponde ao LEAP, devido ao seu processamento ser mais simples que os dos demais. No entanto, este mecanismo está praticamente em desuso pelo fato de ser proprietário da CISCO e possuir uma solução de segurança fraca;

b) O maior tempo de autenticação corresponde ao EAP-TTLS, devido ao processamento do Cliente de Autenticação (*SecureW2*);

c) O PEAP é a solução mais adequada, pois possui o menor tempo de autenticação para os mecanismos que podem ser implementados em qualquer equipamento.

As figuras a seguir, obtidas através do software *Ethereal*, ilustram a troca de pacotes entre o AP e o RADIUS (medição no coletor) e entre o AP e a Estação Móvel (medição no cliente).

auttls - Ethereal

File Edit Capture Display Tools

No.	Time	Source	Destination	Protocol	Info
10	10.452991	Aironetw_55:88:6c	CDP/VTP	CDP	Cisco Discovery Protocol
11	11.891501	10.1.24.5	10.1.24.255	BROWSER	Domain/Workgroup Announcement SGRT, NT Workstation, Domain Enum
12	20.398246	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
13	35.402018	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
14	44.486176	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=225, l=175)
15	44.486605	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=225, l=70)
16	44.511729	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=226, l=282)
17	44.513410	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=226, l=1106)
18	44.578725	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=227, l=176)
19	44.579986	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=227, l=1006)
20	44.608044	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=228, l=1470)
21	44.613493	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=228, l=117)
22	44.623545	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=229, l=176)
23	44.624386	10.1.24.100	10.1.24.3	RADIUS	Access Accept(2) (id=229, l=187)
24	49.484960	AsustekC_b3:b6:36	Aironetw_55:88:6c	ARP	Who has 10.1.24.3? Tell 10.1.24.100
25	49.485807	Aironetw_55:88:6c	AsustekC_b3:b6:36	ARP	10.1.24.3 is at 00:40:96:55:88:6c
26	50.405955	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
27	65.409638	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
28	70.468231	Aironetw_55:88:6c	CDP/VTP	CDP	Cisco Discovery Protocol
29	71.901625	10.1.24.5	10.1.24.255	BROWSER	Domain/Workgroup Announcement SGRT, NT Workstation, Domain Enum
30	80.413634	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
31	95.417143	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
32	104.635899	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=230, l=175)
33	104.636748	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=230, l=70)
34	104.649321	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=231, l=282)
35	104.651002	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=231, l=1106)
36	104.666911	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=232, l=176)
37	104.668173	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=232, l=1006)
38	104.728910	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=233, l=1470)
39	104.734781	10.1.24.100	10.1.24.3	RADIUS	Access Challenge(11) (id=233, l=117)
40	104.743994	10.1.24.3	10.1.24.100	RADIUS	Access Request(1) (id=234, l=176)
41	104.744836	10.1.24.100	10.1.24.3	RADIUS	Access Accept(2) (id=234, l=187)
42	109.635810	AsustekC_b3:b6:36	Aironetw_55:88:6c	ARP	Who has 10.1.24.3? Tell 10.1.24.100
43	109.636240	Aironetw_55:88:6c	AsustekC_b3:b6:36	ARP	10.1.24.3 is at 00:40:96:55:88:6c
44	110.421279	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000
45	125.425083	Aironetw_55:88:6c	01:40:96:ff:ff:00	LLC	U, func = UI; SNAP, OUI 0x004096 (Unknown), PID 0x0000

Figura 72: Autenticação EAP-TLS (Medição no Coletor)

auttls - Ethereal

File Edit Capture Display Tools

No.	Time	Source	Destination	Protocol	Info
8	3.007884	10.1.24.100	10.1.24.5	ICMP	Echo (ping) reply
9	11.889232	10.1.24.5	10.1.24.255	BROWSER	Domain/Workgroup Announcement SGRT, NT Workstation, Domain Enum
10	44.479467	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, Identity [RFC2284]
11	44.480313	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, Identity [RFC2284]
12	44.486759	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]
13	44.505981	Cisco_89:f2:b5	Aironetw_55:88:6c	TLS	Client Hello
14	44.516851	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]
15	44.573259	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, EAP-TLS [RFC2716] [Aboba]
16	44.582936	Aironetw_55:88:6c	Cisco_89:f2:b5	TLS	Server Hello, Certificate, Certificate Request, Server Hello Done
17	44.598348	Cisco_89:f2:b5	Aironetw_55:88:6c	TLS	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake
18	44.613991	Aironetw_55:88:6c	Cisco_89:f2:b5	TLS	Change Cipher Spec, Encrypted Handshake Message
19	44.617828	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, EAP-TLS [RFC2716] [Aboba]
20	44.627458	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Success
21	44.627974	Aironetw_55:88:6c	Cisco_89:f2:b5	EAPOL	Key
22	44.628328	Aironetw_55:88:6c	Cisco_89:f2:b5	EAPOL	Key
23	71.895482	10.1.24.5	10.1.24.255	BROWSER	Domain/Workgroup Announcement SGRT, NT Workstation, Domain Enum
24	104.625134	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, Identity [RFC2284]
25	104.625966	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, Identity [RFC2284]
26	104.632434	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]
27	104.639380	Cisco_89:f2:b5	Aironetw_55:88:6c	TLS	Client Hello
28	104.650071	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]
29	104.657117	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, EAP-TLS [RFC2716] [Aboba]
30	104.666705	Aironetw_55:88:6c	Cisco_89:f2:b5	TLS	Server Hello, Certificate, Certificate Request, Server Hello Done
31	104.714791	Cisco_89:f2:b5	Aironetw_55:88:6c	TLS	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake
32	104.730586	Aironetw_55:88:6c	Cisco_89:f2:b5	TLS	Change Cipher Spec, Encrypted Handshake Message
33	104.733966	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, EAP-TLS [RFC2716] [Aboba]
34	104.743735	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Success
35	104.744102	Aironetw_55:88:6c	Cisco_89:f2:b5	EAPOL	Key
36	104.744861	Aironetw_55:88:6c	Cisco_89:f2:b5	EAPOL	Key
37	164.751309	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, Identity [RFC2284]
38	164.752140	Cisco_89:f2:b5	Aironetw_55:88:6c	EAP	Response, Identity [RFC2284]
39	164.758284	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]
40	164.764997	Cisco_89:f2:b5	Aironetw_55:88:6c	TLS	Client Hello
41	164.776222	Aironetw_55:88:6c	Cisco_89:f2:b5	EAP	Request, EAP-TLS [RFC2716] [Aboba]

Figura 73: Autenticação EAP-TLS (Medição no Cliente)

Na análise das mensagens trocadas entre as entidades, observa-se a coerência com o preconizado na RFC 2716 do EAP-TLS, conforme discutido no capítulo 3 (seção 3.8).

O tempo de autenticação para o mecanismo EAP-TLS não varia na implementação, pois utiliza certificados no cliente e no servidor.

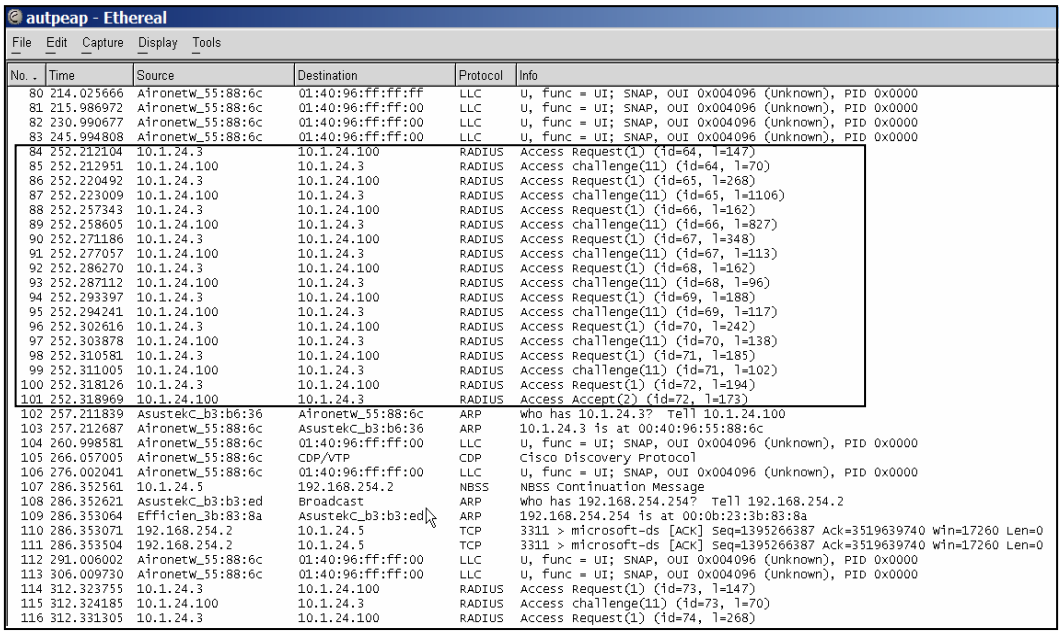

Figura 74: Autenticação PEAP (Medição no Coletor)

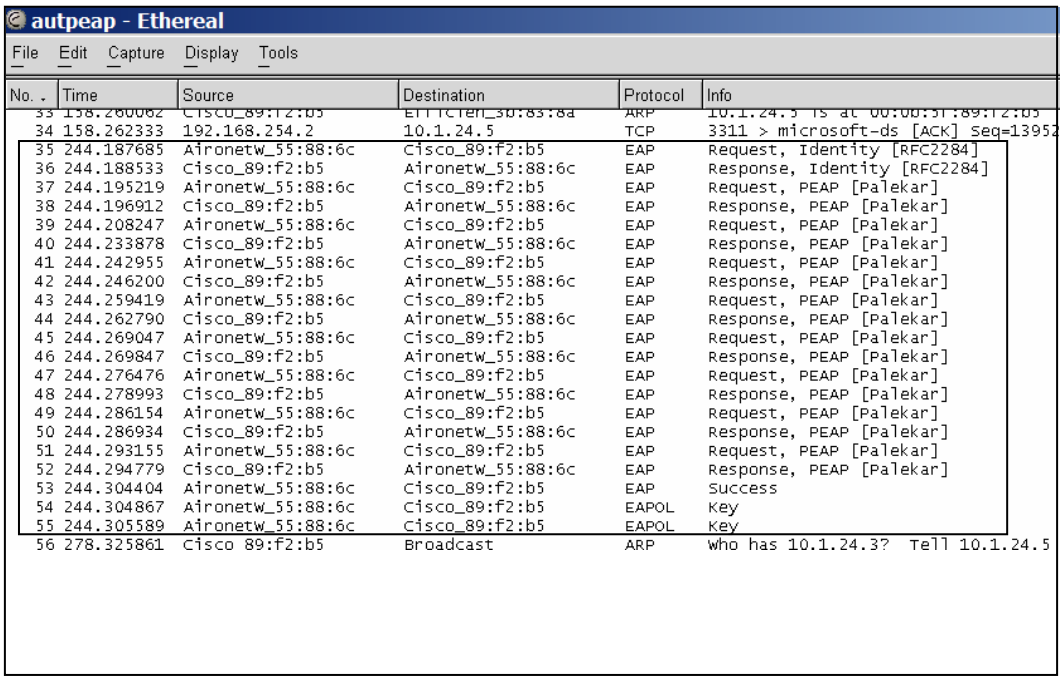

Figura 75: Autenticação PEAP (Medição no Cliente)

Na análise das mensagens trocadas entre as entidades, observa-se a coerência com o preconizado no *Draft* do IETF do PEAP, pois este protocolo ainda não existe em forma de RFC.

O tempo de autenticação para o mecanismo PEAP pode variar entre implementações, de acordo com o processo de autenticação adotado: MD-5, CHAP, MS-CHAP, MS-CHAPv2.

O método MS-CHAPv2 é mais amplamente utilizado na prática, pois é adotado pelo Windows e oferece o maior nível de segurança durante o processo de autenticação.

A autenticação no PEAP exige mais troca de mensagens, devido ao uso do MSCHAP-v2. A troca de mensagens está detalhada no capítulo 3 (seção 3.9).

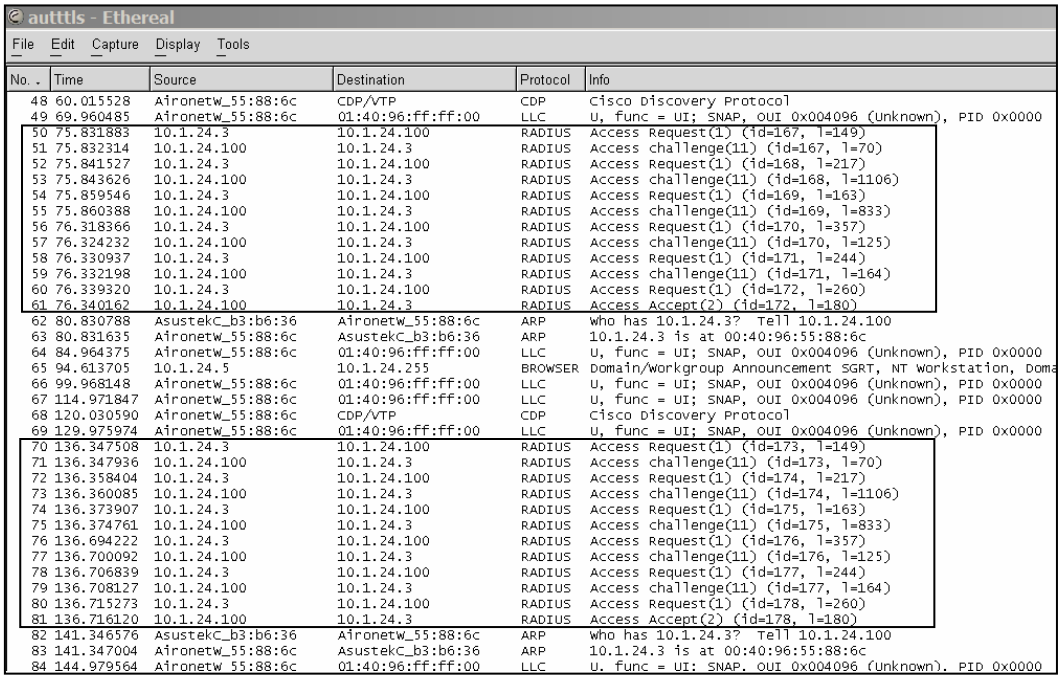

Figura 76: Autenticação EAP-TTLS (Medição no Coletor)

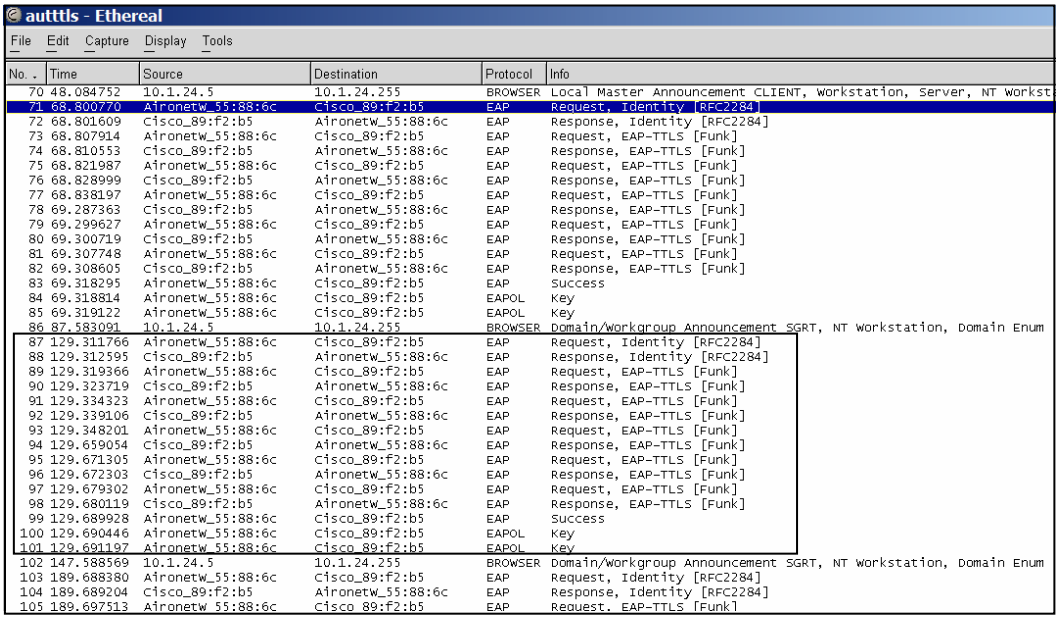

Figura 77: Autenticação EAP-TTLS (Medição no Cliente)

Na análise das mensagens trocadas entre as entidades, observa-se a coerência com o preconizado no *Draft* do IETF do EAP-TTLS, pois este protocolo ainda não existe em forma de RFC.

O tempo de autenticação para o mecanismo EAP-TTLS pode variar entre implementações, de acordo com o processo de autenticação adotado: MD-5, CHAP, MS-CHAP, MS-CHAPv2, e do Cliente de Autenticação: *SecureW2*, *Meetinghouse AEGIS Client* e o *Funk Odyssey*.

Neste trabalho foi adotado o método MD-5.

O mecanismo EAP-TTLS, apesar de necessitar de menos pacotes que o PEAP, possui um maior tempo de autenticação. Isto se deve ao Cliente de Autenticação *SecureW2*.

A troca de mensagens está detalhada no item 3.10.

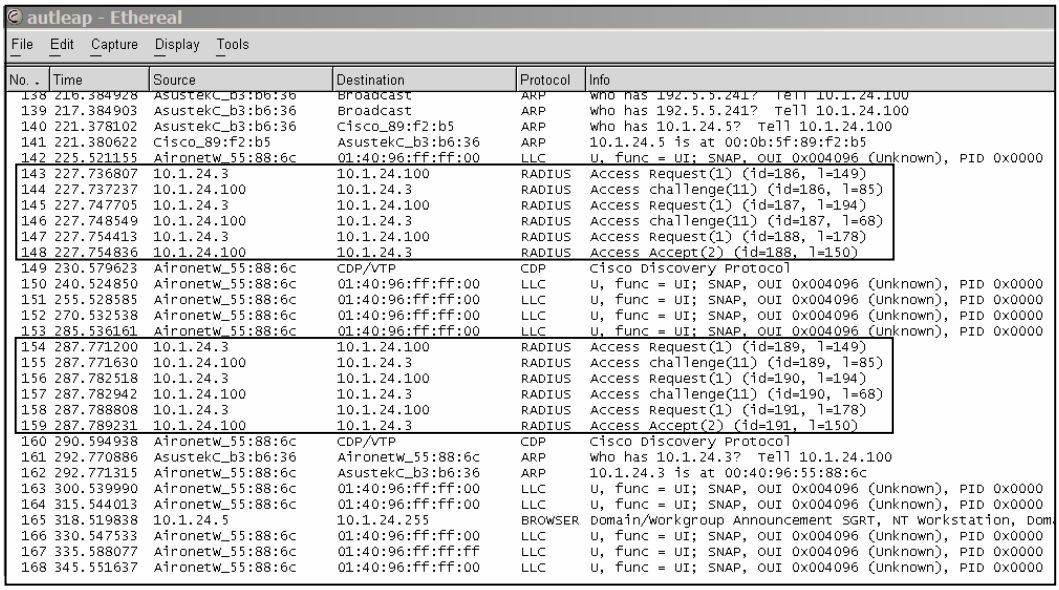

Figura 78: Autenticação LEAP (Medição no Coletor)

A visualização da troca de pacotes no método LEAP somente é possível entre o AP e o RADIUS.

5.6
Avaliação do Desempenho com Vários Clientes

Todos os experimentos realizados até o momento consideram a operação do *access point* com apenas 01 cliente (usuário).

Com objetivo de complementar o trabalho, realizou-se a medição do desempenho com 02, 03 e 04 usuários, a fim de se avaliar a degradação no desempenho quando mais usuários são inseridos na rede.

5.6.1
Avaliação do Desempenho com 02 Clientes

Esse experimento foi realizado em duas etapas:

a) Com os dois usuários configurados para transmitir a 11Mbps;

b) Com um usuário configurado para transmitir a 11Mbps e o outro a 1Mbps.

Para ambos os casos, os experimentos foram realizados utilizando os seguintes mecanismos de segurança com tráfego FTP:

a) *Sistema Sem segurança*

b) *WEP 128 bits*

5.6.1.1
Clientes Configurados a 11Mbps

Nesta situação, foram obtidos os seguintes valores médios para *Throughput* e Tempo de Reposta:

	FTP	
	Throughput (Mbps)	$T_{Resposta}$ (seg)
	Valor Médio	Valor Médio
Sem Segurança	3,130	17,377
WEP 128 bits	3,139	17,316

Tabela 9: Consolidação dos valores médios de *throughput* e tempo de resposta (02 clientes à 11Mbps)

Na análise dos resultados obtidos, observa-se que:

a) Os valores obtidos estão de acordo com os estudos realizados por *Andrzej Duda, Martin Heusse, Franck Rousseau e Gilles Berger-Sabbatel* [23.

b) Mesmo com 02 clientes, comprova-se que a influência sobre a *performance* da rede, quando se implementa um mecanismo de segurança, é desprezível;

c) O tráfego FTP permanece fortemente influenciado pela rede sem fio. O valor médio de *Throughput* para a aplicação FTP continua limitado pelo mecanismo CSMA/CA de acesso ao meio, baseado no modo DCF;

d) Para aumentar a segurança em uma rede desprovida de autenticação externa, deve-se implementar o WEP com 128bits, pois, como observado, não há comprometimento no desempenho da rede;

e) Para aumentar a segurança em uma rede onde é possível se implementar um servidor RADIUS, deve-se adotar um dos três mecanismos: EAP-TLS, PEAP ou EAP-TTLS, em conjunto com o WEP 128bits para criptografia.

5.6.1.2
Clientes Configurados a 1Mbps e 11Mbps

Esta situação é a mais comum na prática, pois a freqüência de 2,4 GHz é uma faixa liberada no Brasil e em um grande número dos países. Isto é, não é necessário obter nenhum tipo de autorização junto ao órgão responsável local, o que impulsiona ainda mais a utilização de tecnologias que utilizam esta faixa, sejam as *WLANs* baseadas no Padrão IEEE 802.11, o Bluetooth (Padrão IEEE 802.15) ou outras tecnologias *wireless* menos conhecidas.

As redes IEEE 802.11b têm sua aplicação mais difundida em ambientes fechados (*indoor*) e, por esse motivo, o comportamento do canal rádio pode ser fortemente influenciado por:

a) Interferências por equipamentos de terceiros e por equipamentos operando na mesma faixa de 2,4GHz;

b) Perdas de penetração em paredes e pisos;

c) Efeitos de movimentação de pessoas no ambiente;

d) Perdas decorrentes da distância da estação móvel ao AP;

e) Efeitos de multipercursos causados pelos fenômenos de reflexão, difração e espalhamento. Estes fenômenos permitem que um sinal atinja um

destino por diferentes percursos, além do percurso direto (*LoS – Line of Sight*), quando este existe;

f) Difração em bordas;

g) Incidência de chuvas. Quando muito alta, de modo que as paredes dos edifícios fiquem uma boa parte do tempo úmidas, normalmente se acrescenta uma perda adicional ao modelo de propagação.

Foram obtidos os seguintes valores médios para *Throughput* e Tempo de Reposta:

	FTP	
	Throughput (Mbps)	$T_{Resposta}$ (seg)
	Valor Médio	Valor Médio
Sem Segurança	0,724	75,150
WEP 128 bits	0,717	75,967

Tabela 10: Consolidação dos valores médios de *throughput* e tempo de resposta (clientes à 1Mbps e 11Mbps)

Na análise dos resultados obtidos, observa-se que:

a) A forte redução no *Throughput* deve-se às características do mecanismo CSMA/CA de acesso ao meio, baseado no modo DCF, conforme os estudos realizados por *Andrzej Duda, Martin Heusse, Franck Rousseau e Gilles Berger-Sabbatel*;

b) O *Throughput* dos usuários estará limitado ao *throughput* do usuário com a pior condição de propagação. O usuário reduz sua taxa nominal quando detecta um aumento na perda de pacotes, e degrada sua taxa para 5.5, 2 ou 1Mbps;

c) Ainda assim comprova-se que a influência sobre a *performance* da rede, quando se implementa um mecanismo de segurança, é desprezível;

d) O tráfego FTP permanece fortemente influenciado pela rede sem fio. O valor médio de *Throughput* para a aplicação FTP continua limitado pelo mecanismo CSMA/CA.

5.6.2
Avaliação do Desempenho com 03 e 04 Clientes

Foram obtidos os seguintes valores médios para *Throughput* e Tempo de Reposta:

	FTP	
	Throughput (Mbps)	$T_{Resposta}$ (seg)
	Valor Médio	Valor Médio
1 Cliente	5,415	10,050
2 Clientes	3,130	17,377
3 Clientes	2,052	26,476
4 Clientes	1,532	35,523

Tabela 11: Consolidação dos valores médios de *throughput* e tempo de resposta (01 à 04 Clientes à 11Mbps)

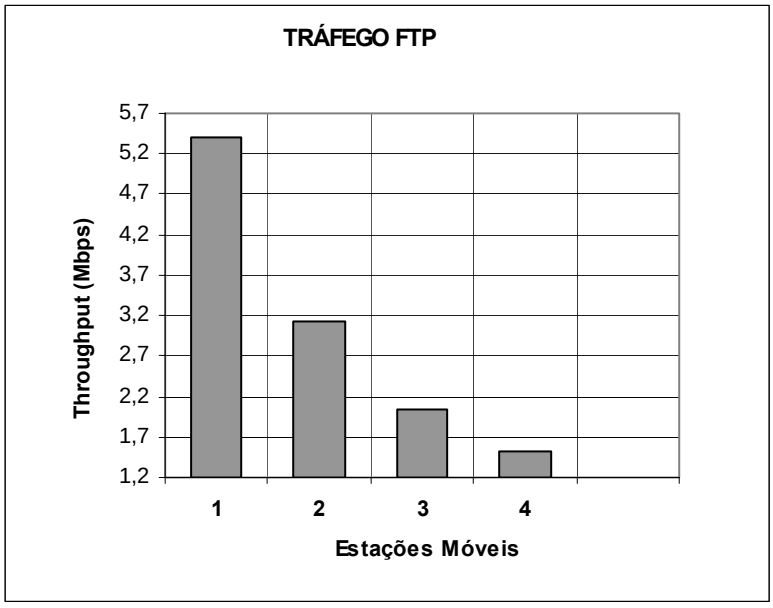

Figura 79: Valor médio de *throughput* (01 à 04 Clientes)

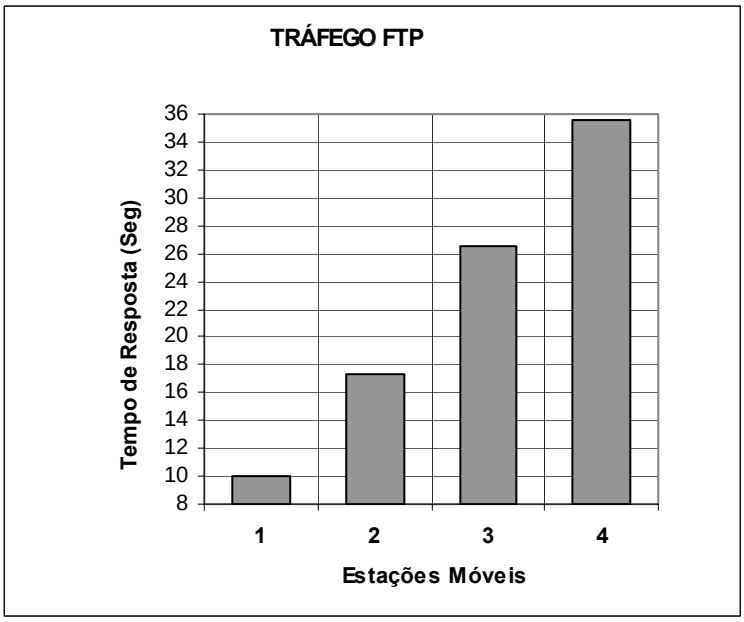

Figura 80: Valor médio do tempo de resposta (01 à 04 Clientes)