4
Metodologia e Implementação

Como estudado no capítulo 3, as redes IEEE 802.11b possuem diversas vulnerabilidades decorrentes da fragilidade dos mecanismos de autenticação, confidencialidade e integridade dos dados definidos pelo IEEE na elaboração do padrão.

A solução para aumentar a segurança é conjugar a operação dos mecanismos internos do padrão IEEE 802.11b com uma autenticação externa, através do padrão IEEE 802.1x. Esta combinação possibilitará a autenticação e criptografia dos dados de forma mais eficiente e confiável.

Neste trabalho serão usadas as expressões *mecanismos internos* e *mecanismos externos,* conforme definido abaixo:

a) ***Mecanismos Internos***: intrínsecos ao Padrão IEEE 802.11b;
b) ***Mecanismos Externos***: utilizam autenticação externa através do padrão IEEE 802.1x.

A adoção de um mecanismo de segurança, seja ele interno ou externo, gera uma sobrecarga de pacotes, devido à inserção de tráfego extra para autenticação dos usuários e criptografia das mensagens, diminuindo a *performanc*e da rede.

Esta preocupação é discutida em publicações acadêmicas [18], [19], [20] e [21]. Os resultados apresentados mostram que esta sobrecarga é considerável, dependente do mecanismo adotado e deve ser levada em conta na decisão de qual modelo a ser implementado, tendo em vista que a mesma pode degradar o desempenho da rede.

No projeto e planejamento de uma WLAN deve-se avaliar o quanto o mecanismo adotado irá influenciar e comprometer a *performance* da rede. Caberá ao projetista e administrador da rede decidir pelo modelo mais adequado às características e necessidades da empresa/instituição, a partir da avaliação do "*custo*" da informação e do prejuízo causado pela invasão por elementos estranhos.

4.1
Objetivo do Trabalho

O objetivo principal é estudar qual a efetiva degradação no desempenho (*performance*) das redes IEEE 802.11b devido à implementação de mecanismos de segurança, sejam eles intrínsecos do padrão ou uma combinação com sistemas de autenticação e criptografia externos, ambos estudados no capítulo 3.

Para isso, este trabalho propõe-se realizar uma simulação da operação de uma rede *wireless* com um cliente e um *Access Point*, utilizando cada um dos mecanismos de segurança. A partir dessa simulação, irá poder quantificar o real impacto no desempenho das redes IEEE 802.11b e responder as seguintes perguntas:

a) Como os diferentes mecanismos de segurança influenciam o desempenho da rede ?

b) Como varia o desempenho nos diferentes tipos de tráfego ?

c) Qual o impacto da autenticação de um usuário em cada mecanismo utilizando padrão IEEE 802.1x ?

4.2
Mecanismos de Segurança

A simulação foi realizada com 08 mecanismos de segurança.

Previstos no padrão IEEE 802.11b:

a) *Sistema Sem segurança*.
   - ⇨ A segurança restrita à identificação pelo SSID;
   - ⇨ O AP e estações móveis configurados com ***SSID = puc-rio***;

b) *Pelo Controle do Endereço MAC*.
   - ⇨ A segurança efetivada através do SSID e do endereço MAC da placa de rede sem fio;
   - ⇨ A tabela de endereços MAC configurada no AP;

c) *WEP 64 Bits (40+24bits)*.
   - ⇨ Utilização do SSID;
   - ⇨ Modo de Autenticação: *Shared;*

- ⇨ WEP configurado com senha de 64 bits para criptografia dos dados;

d) *WEP 128 bits (104 + 24bits)*.

- ⇨ Utilização do SSID;
- ⇨ Modo de Autenticação: *Shared*;
- ⇨ WEP configurado com senha de 128 bits para criptografia dos dados;

Proporcionados pelo padrão IEEE 802.1x sobre o IEEE 802.11b:

e) *EAP-TLS*.

- ⇨ Utilização de certificado no cliente e no servidor, gerados pelo OpenSSL no LINUX;
- ⇨ Certificado raiz instalado no cliente (estação) e no servidor (RADIUS): *cacert.pem*;
- ⇨ Certificado instalado no servidor para autenticação do cliente: *cert-clt.pem*;
- ⇨ Certificado instalado no cliente para autenticação do servidor: *cert-srv.pem*;
- ⇨ WEP configurado com senha de 128 bits para criptografia dos dados na rede sem fio, a partir de chave de sessão gerada na autenticação;

f) *PEAP*.

- ⇨ Utilização do método MS-CHAPv2 para autenticação de senha segura dentro do PEAP. O método MS-CHAPv2 é o mais seguro dentre os disponíveis pelo Windows;
- ⇨ Utilização de certificado no servidor, gerado pelo OpenSSL no LINUX;
- ⇨ Certificado raiz instalado no servidor (RADIUS): *cacert.pem*;
- ⇨ Certificado instalado no cliente para autenticação do servidor: *cert-srv.pem*;
- ⇨ WEP configurado com senha de 128 bits para criptografia dos dados na rede sem fio, a partir de chave de sessão gerada na autenticação;

g) *EAP-TTLS*.

- ⇨ Cliente de Autenticação: *SecureW2 Client* versão 2.2.0 (uso não comercial);
- ⇨ Utilização do método EAP-MD5 para autenticação de senha segura dentro do EAP-TTLS. O método EAP-MD5 foi definido no SecureW2;
- ⇨ Utilização de certificado no servidor;
- ⇨ Certificado raiz instalado no servidor (RADIUS): *cacert.pem*;
- ⇨ Certificado instalado no cliente para autenticação do servidor: *cert-srv.pem*;
- ⇨ *WEP configurado com senha de 128 bits para criptografia dos dados na rede sem fio, a partir de chave de sessão gerada na autenticação;

h) *LEAP*.

- ⇨ Funciona sem certificados, apenas com senha.

4.3
Medidas de Desempenho

O tempo de resposta e a vazão *(throughput)* são os parâmetros de interesse para avaliação e medição do desempenho. Eles são definidos neste trabalho com se segue:

a) ***Tempo de Resposta*** **($T_{Resposta}$)**: tempo total de transmissão da mensagem entre dois pontos. O tempo de resposta total inclui o tempo de negociação entre o cliente e o servidor, o tempo de efetiva transferência dos dados e o tempo de desconexão.

O diagrama abaixo ilustra como o tempo de resposta é mensurado:

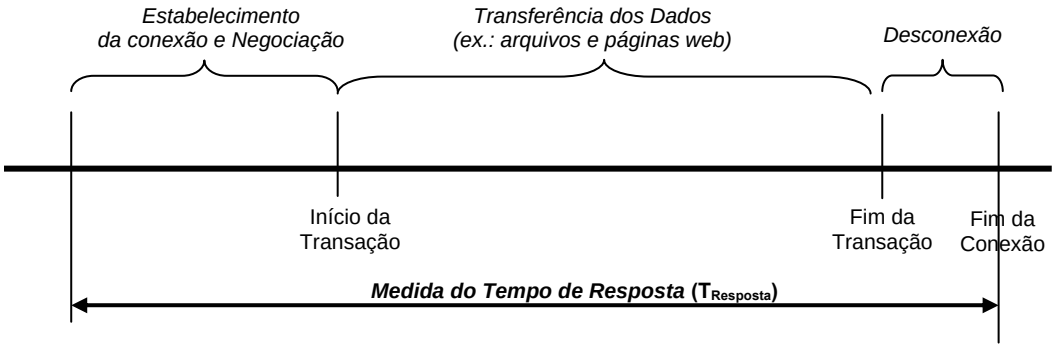

Figura 54: Medição do tempo de resposta

b) ***Throughput*** ***(T_h):*** número total de bytes que podem ser transmitidos na rede em um dado período de tempo (tempo de resposta).

4.4
Procedimentos para Medição

Para cada mecanismo, o experimento foi repetido 20 vezes, sendo que os cinco primeiros resultados foram desconsiderados, de forma a se evitar a influência de fatores dos sistemas operacionais e das máquinas, como por exemplo o processo de armazenamento de dados das páginas em memória *cache* .

Os experimentos foram realizados em laboratório com aproximadamente $20m^2$ de área livre, sem obstáculos. Em todas as medidas, o nível de sinal informado pelo AP foi excelente.

O tempo de autenticação definido no Servidor RADIUS foi de 10 min.

4.5
Protocolos de Aplicação

Neste trabalho foram utilizados os protocolos de aplicação FTP (F*ile Transfer Protocol*) e HTTP (*Hipertext Transfer Protocol*), tendo em vista serem os mais amplamente utilizados. Optou-se pelos protocolos FTP e HTTP, pois representam com mais fidelidade a maioria das aplicações em redes, e facilitam a avaliação da sobrecarga inserida pelos mecanismos de segurança no desempenho dos serviços proporcionados pelos referidos protocolos (transmissão de arquivos, acesso à internet, ...).

A fim de facilitar a medição do tempo de resposta, desenvolveu-se uma *script* de forma a automatizar e eliminar a influência do operador na transação FTP. Sem esse *script* o operador poderia inserir um retardo aleatório no início e fim da transação.

Texto do *script:*

Open www.example.com

teste (ID)

teste (Password)

get teste.mp3

quit

Comando para inicializar a *script*: *ftp –s: script.txt* .

O tráfego HTTP foi caracterizado por uma página *WEB* de aproximadamente 902Kbytes. A transação HTTP foi simulada com uma simples sessão com 251 links e com *download* de 197 arquivos, totalizando os 902Kbytes.

URL utilizada nos experimentos: www.example.com. Esta página foi hospedada no servidor do laboratório.

4.6
Equipamentos Utilizados

Os experimentos foram realizados utilizando equipamentos *wireless* IEEE 802.11b da marca CISCO.

a) *Access Point* (AP)

- ⇨ Modelo: Cisco, AIR-AP350 *Series*
- ⇨ *Firmware*: 12.04
- ⇨ Antenas: dois dipolos externos
- ⇨ Diagrama das antenas: H: omnidirecional; V: 70º
- ⇨ Freqüência: 2,4GHz. DSSS
- ⇨ *Throughput* máximo: 11Mbps

b) *Client Adapter*

- ⇨ Modelo: Cisco, AIR-PCM350 *Series*
- ⇨ *Software*: *Cisco Aironet Client Utility*

- ⇨ Antenas: dois dipolos integrados internos
- ⇨ Diagrama das antenas: H: omnidirecional ; V: não disponível
- ⇨ Freqüência: 2,4GHz DSSS
- ⇨ *Throughput* máximo: 11Mbps

c) Computador Cliente

- ⇨ *Notebook* Toshiba
- ⇨ Pentium III 800Mhz
- ⇨ RAM: 128Mbytes
- ⇨ Sistema Operacional: *Windows XP Pro Service Pack* 2

d) Computador Servidor RADIUS e Servidor de DNS

- ⇨ *Desktop*
- ⇨ Atlon XP 2000+
- ⇨ RAM: 256Mbytes
- ⇨ Sistema Operacional: Linux Conectiva 10

e) Computador Servidor de FTP e HTTP

- ⇨ Desktop
- ⇨ Atlon XP 1600+
- ⇨ RAM: 256Mbytes
- ⇨ Sistema Operacional: *Windows 2000 Pro Service Pack* 4

f) Computador Coletor e Medidor

- ⇨ Desktop
- ⇨ Atlon XP 2000+
- ⇨ RAM: 256Mbytes
- ⇨ Sistema Operacional: *Windows 2000 Pro Service Pack* 4

g) HUB (10Mbps)

- ⇨ Para permitir que o computador coletor/medidor possa coletar e medir os dados trocados entre o AP e o RADIUS.

4.7
Softwares e Ferramentas Utilizadas

Softwares e ferramentas utilizadas nos experimentos:

a) Computador Cliente

- ⇨ *Cisco Aironet Client Utility*
- ⇨ *Ethereal Network Analyser* versão 0.10.6 (Windows): para captura e análise do tráfego
- ⇨ *WinHTTrack Website Copier versão 3.32-2*: software para captura de página WEB, simulando a navegação

b) Computador Servidor de DNS (*Domain Name Server*).

- ⇨ *Bind* versão 9.2.3.: servidor de DNS.

c) Computador Servidor RADIUS

- ⇨ *FreeRADIUS* versão 1.0.1.

d) Computador Servidor de FTP

- ⇨ *Filezilla* versão 0.9.3.: servidor de arquivos FTP para Windows
- ⇨ URL: www.example.com (contendo o arquivo *teste.mp3)*
- ⇨ Para acesso ao arquivo:
  User: teste Password: teste

e) Computador Servidor HTTP

- ⇨ *Apache* versão 1.3.31: servidor HTTP para Windows

f) Computador Coletor e Medidor

- ⇨ *Ethereal Network Analyser* versão 0.10.6 (Windows): para captura e análise do tráfego

4.8
Configuração da Arquitetura de Rede

A arquitetura de rede para simulação foi dividida em duas etapas:

4.8.1
Arquitetura 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*.

Os diagramas a seguir ilustram a arquitetura e configuração da rede, com as características de cada equipamento.

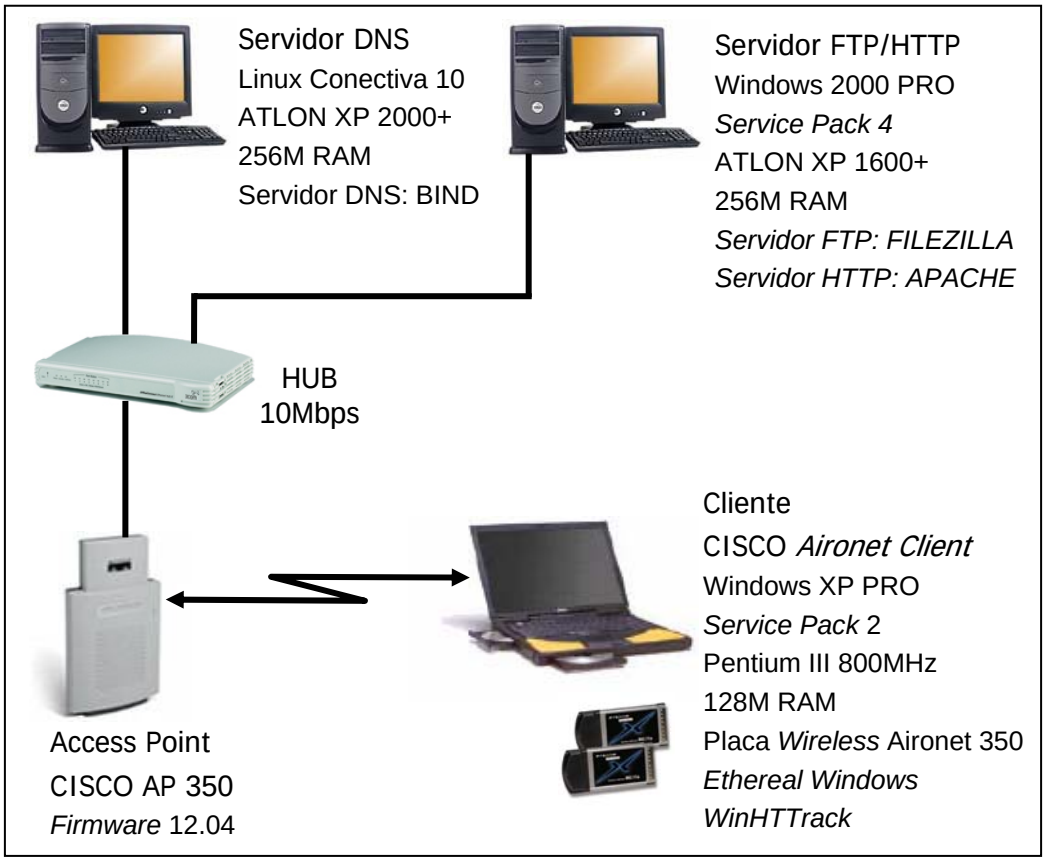

Figura 55: Especificação da rede sem autenticação externa

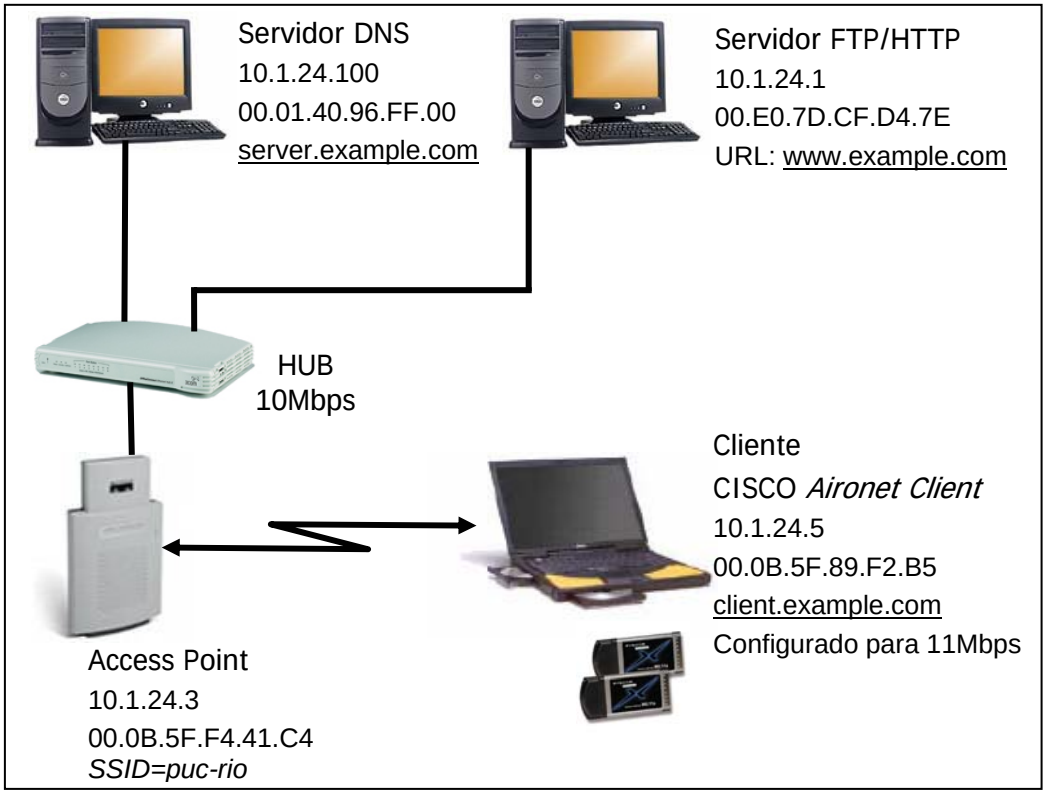

Figura 56: Configuração da rede sem autenticação externa

4.8.2
Arquitetura Com Autenticação Externa

Nesta situação, foram simulados os seguintes mecanismos:

a) *EAP-TLS*;

b) *PEAP*;

c) *EAP-TTLS*;

d) *LEAP*.

Os diagramas a seguir ilustram a arquitetura e configuração da rede, com as características de cada equipamento.

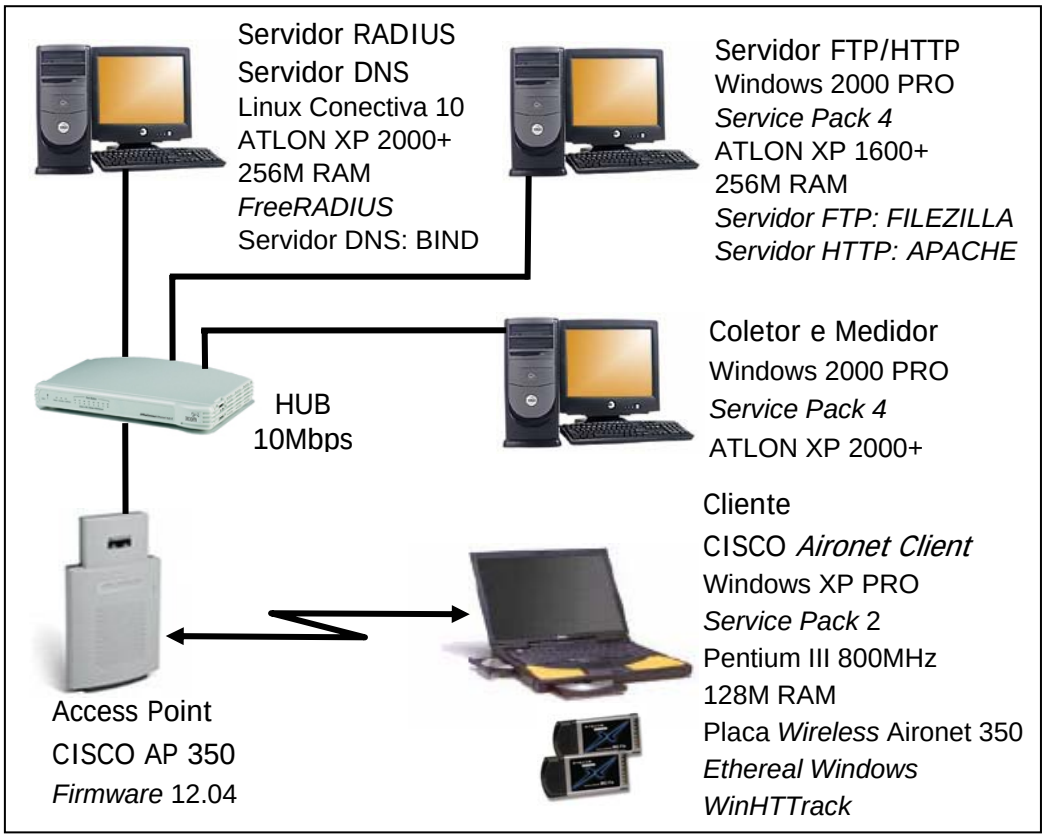

Figura 57: Especificação da rede com autenticação externa

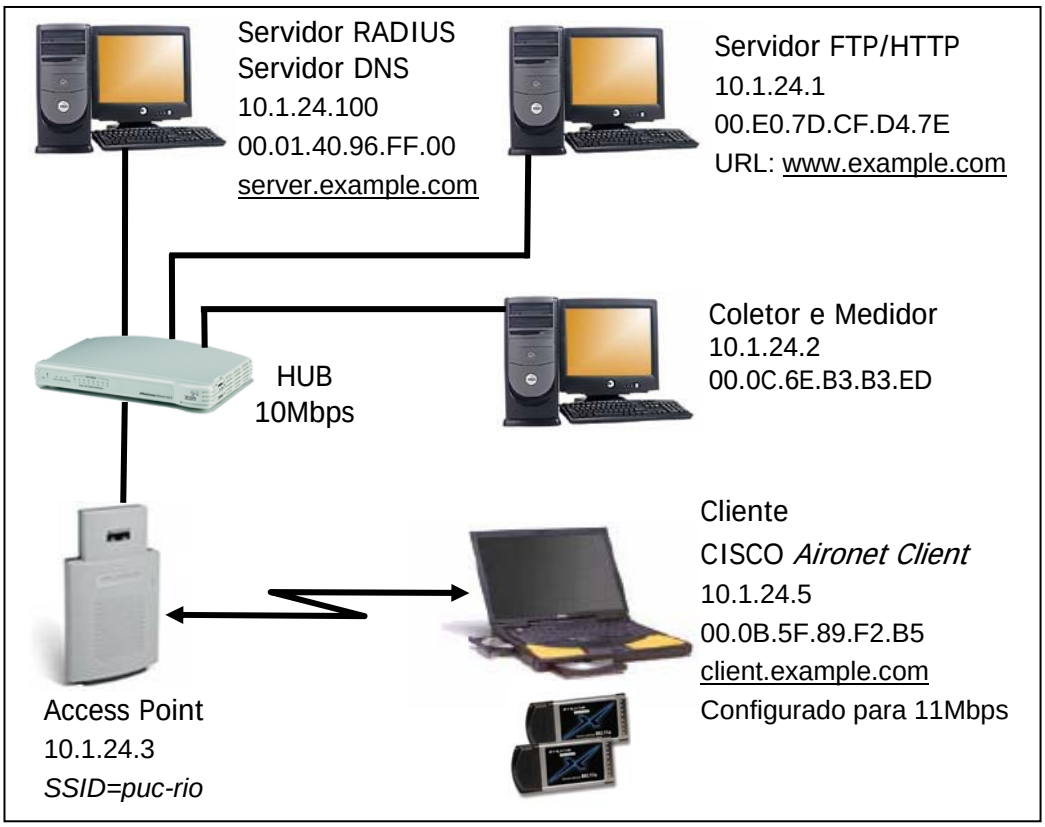

Figura 58: Configuração da rede com autenticação externa

4.9
Operação da Rede Sem o AP

Para complementar a conclusão do trabalho, realizou-se a medição do desempenho da rede sem a presença do AP, permitindo avaliar se é somente o *Acess Point* que está interferindo e reduzindo o *throughput* da rede.

O experimento foi realizado em duas etapas:

a) Com a presença do HUB: este equipamento está limitado a 10Mbps, pois sua tecnologia é obsoleta. Os fabricantes deixaram de produzir equipamentos HUB, principalmente de 100Mbps. A utilização do HUB é devido à necessidade de replicar fielmente os dados entre o AP e o RADIUS, no computador utilizado para coleta e medição, o que não seria possível com um switch;

b) Com a presença de um Switch de 100Mbps: optou-se por fazer este experimento para se avaliar o comportamento da rede operando em 100Mbps.

Os diagramas a seguir ilustram a arquitetura e configuração da rede, com as características de cada equipamento.

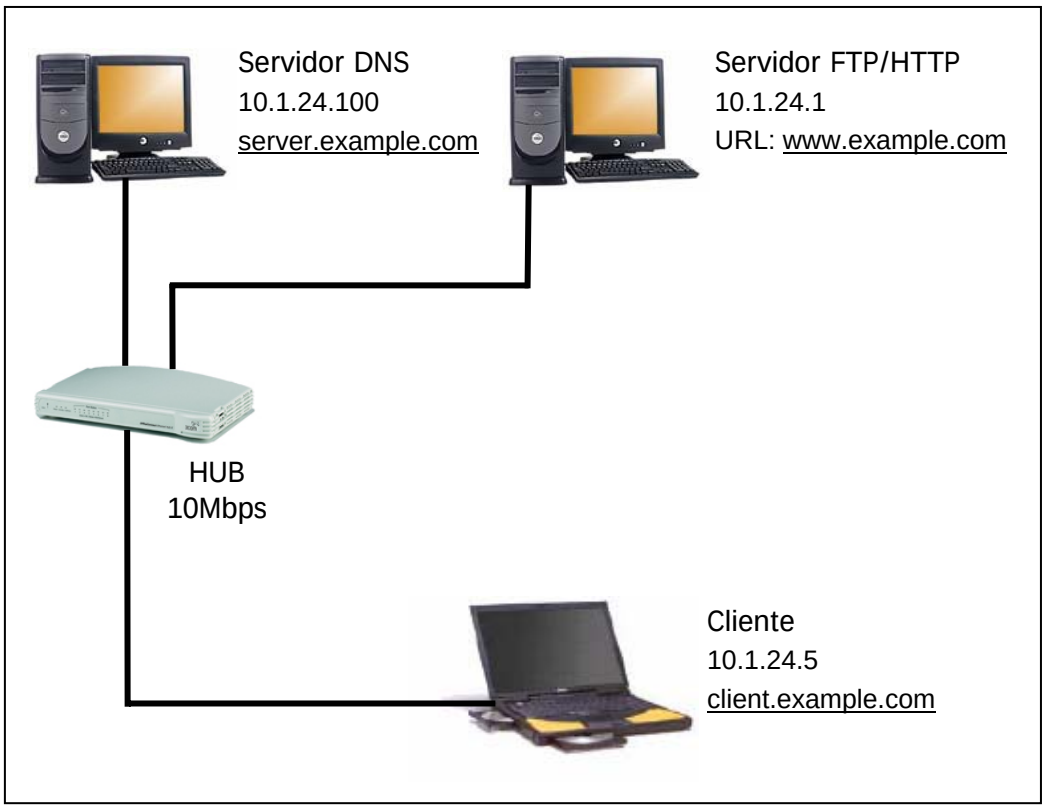

Figura 59: Configuração da rede sem AP (Operação com HUB)

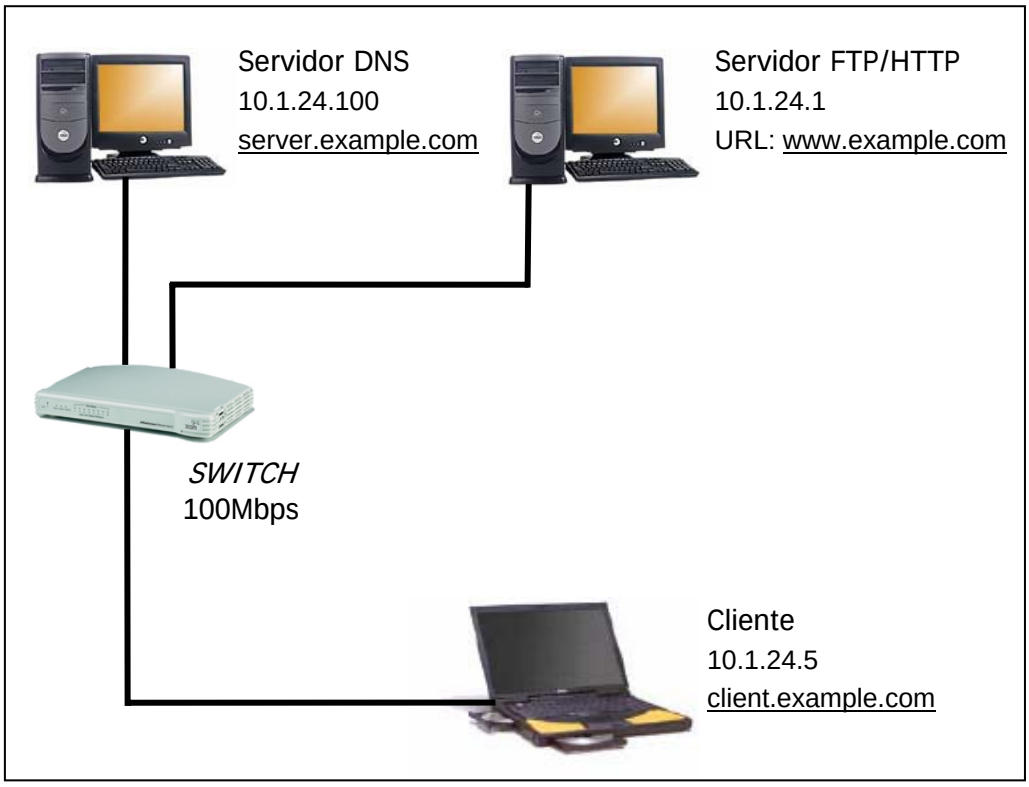

Figura 60: Configuração da rede sem AP (Operação com *Switch*)

4.10
Operação da Rede Com Vários Clientes

Os experimentos realizados até o momento consideram a operação do AP com apenas 01 cliente (usuário).

A fim de complementar o trabalho, realizou-se a medição do desempenho com 02, 03 e 04 usuários, permitindo avaliar qual o impacto no *throughput* quando mais usuários são inseridos na rede.

4.10.1
Operação da Rede 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.

- ⇨ Este caso simula a situação onde o sistema reduz a taxa nominal de um usuário quando o mesmo está com dificuldade de se comunicar com o AP, devido à degradação do sinal de RF por interferências e desvanecimentos;
- ⇨ Esta situação é muito comum em redes *wireless*, o que justifica aqui seu estudo.

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

a) *Sistema Sem segurança*;
b) *WEP 128 bits*.

Para medição do desempenho, um usuário foi configurado para realizar uma transação FTP de um arquivo MPEG com 163 Mbytes, caracterizando a ocupação da rede sem fio. Simultaneamente, os experimentos foram realizados com outro usuário, utilizando o arquivo teste.MP3.

Os diagramas a seguir ilustram a arquitetura e configuração da rede, com as características de cada equipamento.

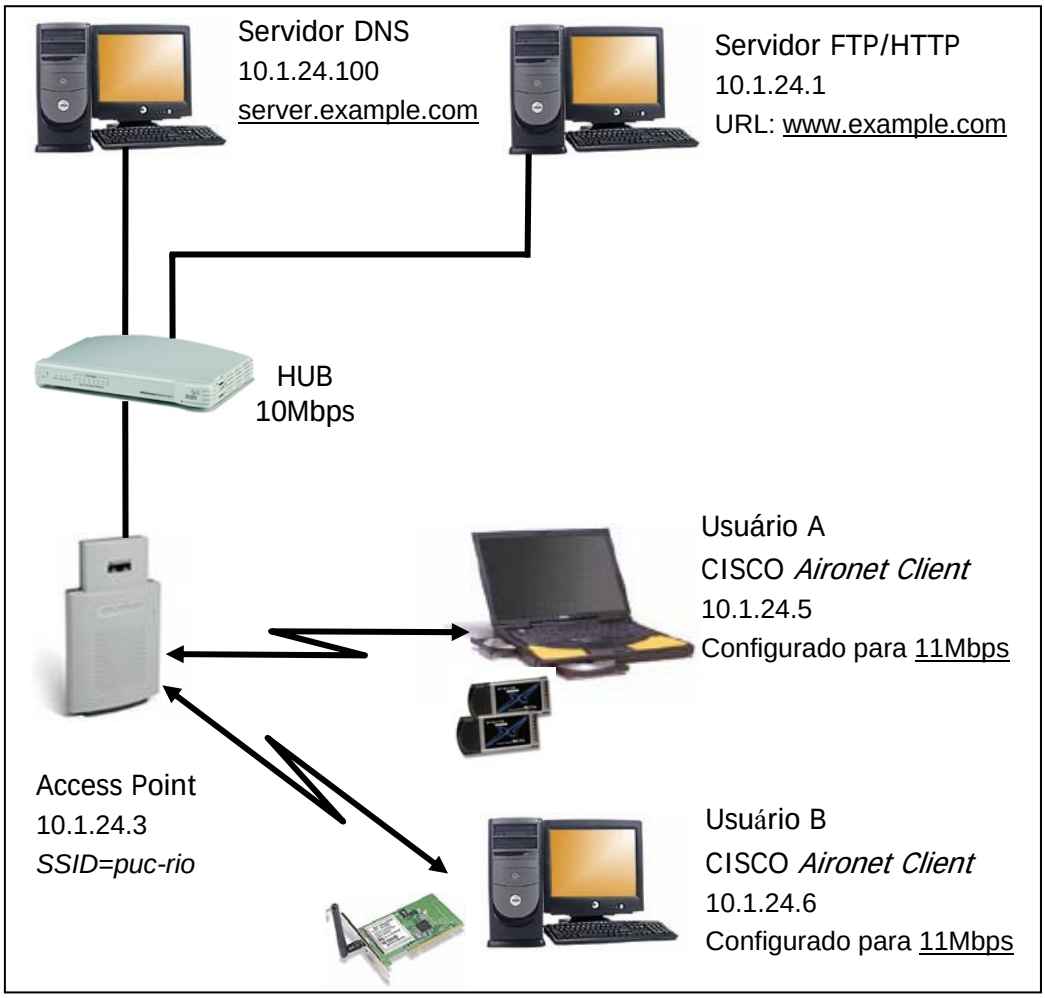

Figura 61: Configuração da rede com 02 usuários configurados em 11Mbps

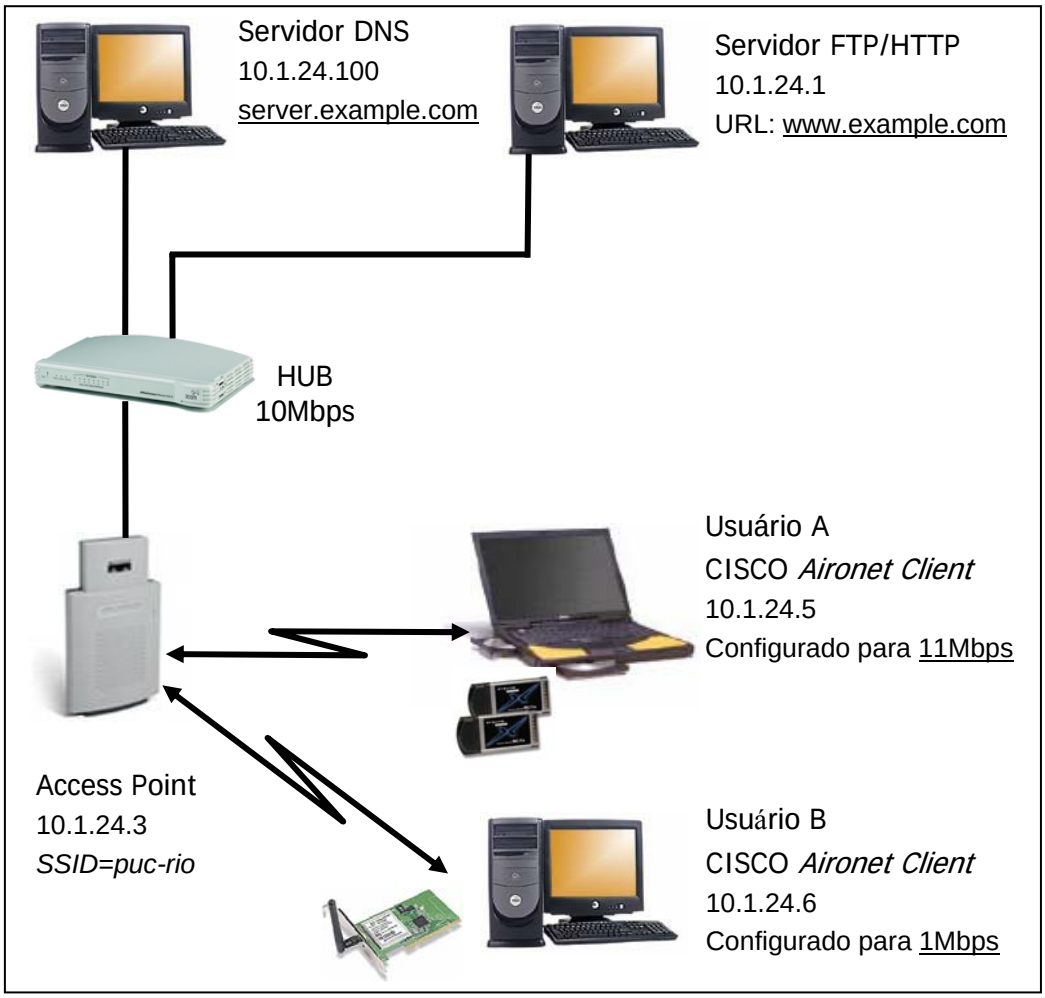

Figura 62: Configuração da rede com 02 usuários configurados em 11Mbps e 1Mbps

4.10.2
Operação da Rede Com 03 Clientes

Esse experimento foi realizado com 03 usuários configurados para transmitir a 11Mbps e operando com *Sistema Sem segurança*.

4.10.3
Operação da Rede Com 04 Clientes

Esse experimento foi realizado com 04 usuários configurados para transmitir a 11Mbps e operando com *Sistema Sem segurança*.