
Redes Locais sem Fio

Como montar sua rede sem cabos

Gilberto Sudré

gilberto@unitera.com.br

UNITERA Tecnologia

0 xx 27 3200-3160

www.unitera.com.br



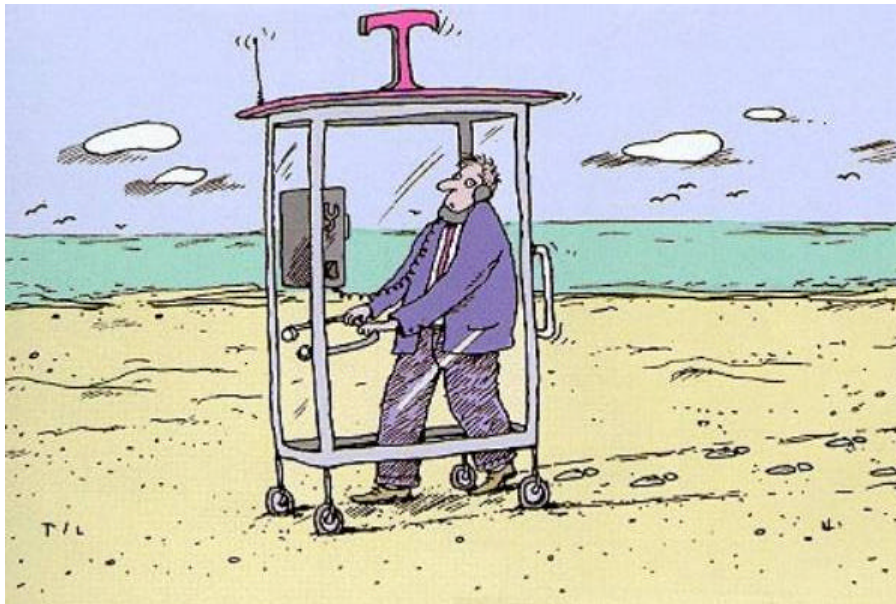
Agenda

- Conceitos de redes sem fio
- IEEE 802.11
- Performance e alcance
- Elementos de Hardware
- Topologias
- Projeto (site survey)
- Aspectos de segurança



2

Redes sem Fio



Redes sem Fio

- Largamente adotadas pela facilidade de uso e instalação
- Número de implementações de redes wireless nos EUA duplicaram nos últimos 12 meses
Yankee Group – julho/2002
- Em 2005 existirão aproximadamente 137 milhões de usuários de redes sem fio
Gartner Group

Redes sem Fio Benefícios

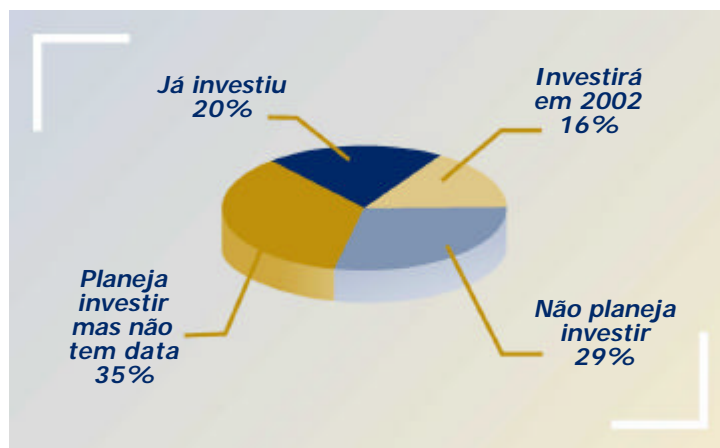
- Mobilidade
- Instalação Rápida, Simples e Flexível
- Redução de custo
 - As despesas de instalação podem ser significativamente menores comparados a redes cabeadas
- Não substituem as redes cabeadas
- Escalabilidade

Redes sem Fio Histórico

- 1940 – Primeiro uso da tecnologia spread spectrum
- 1980 – Aplicações limitadas usando Narrowband
- 1980 – FCC atribui freqüências para uso comercial
- 1989 – ISM autoriza uso em 900MHz 2.4GHz e 5 GHz
- 1989 – Produtos usando 900MHz são produzidos
- 1990 – IEEE começa a trabalhar em um padrão industrial para WLAN
- 1994 – Produtos usando 2.4GHZ são produzidos
- 1994 – Aprovado o padrão IEEE 802.11
- 1997 – Produtos 2.4GHz começam a roubar a cena
- 1999 – Ratificação da IEEE 802.11a e 802.11b
- 1999 – Produtos baseado em 802.11b começam a ser produzidos

7

Redes sem Fio Brasil



8

Redes sem Fio Desafio


- Implementação de um ambiente seguro para o tráfego das informações
- Problema
 - Uso do meio compartilhado





Redes sem Fio Tipos

- Radiofrequência
 - IEEE 802.11
 - WLAN – Wireless Lan
 - Bluetooth
- Laser
- Infravermelho





Bluetooth



Bluetooth

- Protocolo padrão para conexão wireless de:
 - Telefones sem fio
 - PDAs
 - Computadores
 - Impressoras
 - Eletrodomésticos



- Curiosidade:
 - O nome Bluetooth é oriundo do conquistador Viking chamado Harald Bluetooth que unificou a Dinamarca e a Noruega no século X



12



Bluetooth

- Utiliza a frequência de 2.4GHz
- Velocidade de até 740 kbps
- Alcance de até 100 mts
- Modo de transmissão
 - Frequency hopping (1600 mudanças por segundo)
- Pode provocar interferência em redes 802.11



13

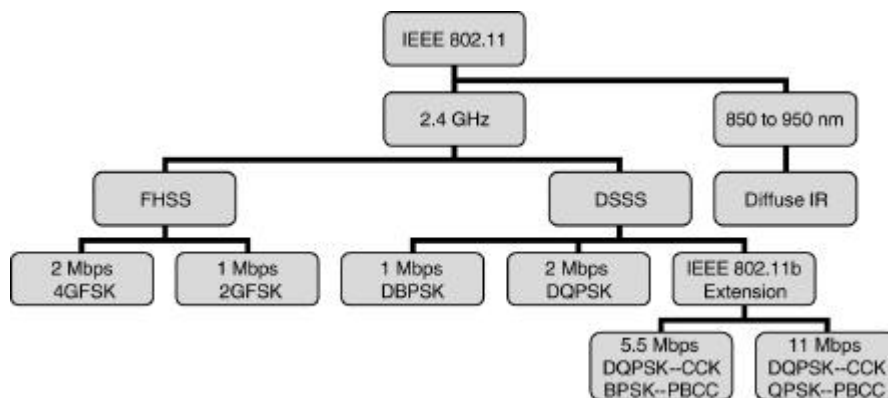
IEEE 802.11

O que é o IEEE 802.11

- IEEE
 - Institute of Electrical and Electronics Engineers
- 802.11
 - Família de padrões que especificam o funcionamento das redes sem fio
 - WLAN – Wireless LAN



15



16

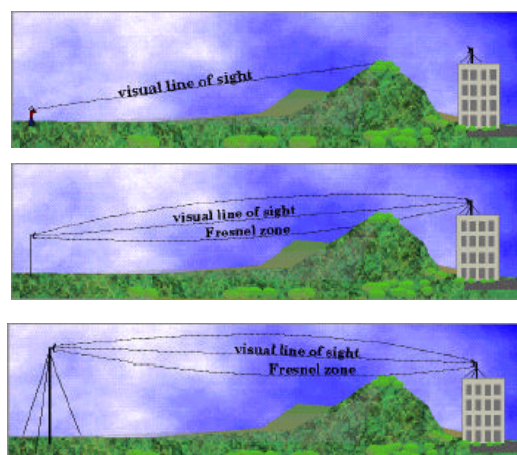


IEEE 802.11 Características

- Transmissão de dados por ondas de Rádio
- Modulação do sinal sobre uma onda portadora
- Visada
 - Ambientes externos
 - Requer visada direta
 - Ambientes internos
 - NÃO requer visada direta

17

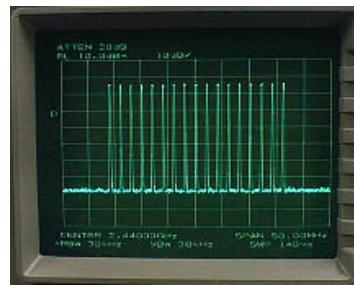
IEEE 802.11 Visada



18

IEEE 802.11 Tipo de Transmissão

- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping
- CSMA/CA
- Funcionamento
 - Ambiente externo
 - Ponto a ponto
 - Ambiente Interno
 - Multiponto



19

Rede sem Fio IEEE 802.11 Padrões



802.11b

- 11 Mbps
- 2.4 GHz

802.11a

- 54 Mbps
- 5 GHz

802.11g

- 54 Mbps
- 2.4 GHz

20

Congresso InfoWorld 2003
Tutorial – Redes Locais sem Fio

Localização	Faixa de frequência (MHz)	Potência de saída máxima	Padrão
Europa	2400 – 2483.5	10 mW/MHz	IEEE 802.11b, HomeRF, Bluetooth
	5150 – 5350	200 mW/MHz	HIPERLAN/2
	5470 – 5725	1000 mW/MHz	IEEE 802.11a
US, Canada, America Latina	2400 – 2483.5	1000 mW/MHz	IEEE 802.11b
	5150 – 5250	2.5 mW/MHz	HomeRF, Bluetooth
	5250 – 5235	12.5 mW/MHz	HIPERLAN/2
	5725 – 5825	50 mW/MHz	IEEE 802.11a, BWIF
Japão	2400 – 2497	10 mW/MHz	IEEE 802.11b HomeRF, Bluetooth
	5150 – 5250	200 mW/MHz	HIPERLAN/2 IEEE 802.11a Wireless Home-link

21

IEEE 802.11b

- Padrão estabelecido em setembro de 1999
- Velocidade de até 11 Mbps
- Utiliza frequência de 2.4 GHz
- Conectividade robusta
- Padrão mais utilizado de comunicação sem fio
- Também conhecido como Wi-Fi (Wireless Fidelity)



22

IEEE 802.11a

- Padrão “Fast Ethernet” para redes sem fio
- Velocidades de até 54 Mbps
- Padrão estabelecido em 2002/2
- Ainda em aceitação pelo mercado
 - Diversos produtos disponíveis

23

IEEE 802.11a

- Vantagens
 - Alta velocidade
 - Menor nível de interferência que o 2.4 GHz
 - 2.4 GHz utilizado pelo Bluetooth, Telefones sem fio, Celulares e fornos de microondas
- Desvantagens
 - Menor alcance
 - Necessidade de maior número de Access Points (4 x)

24

IEEE 802.11g

- Outro padrão de alta velocidade
- Visto como uma evolução do 802.11a
- Velocidades de até 54 Mbps
- Funciona em 2.4 GHz
- Vantagens
 - Compatibilidade com o 802.11b
 - Melhor alcance que o 802.11a

25

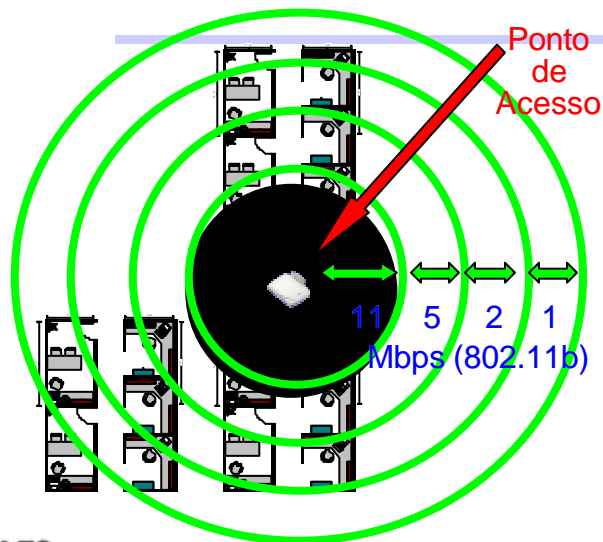
IEEE 802.11e

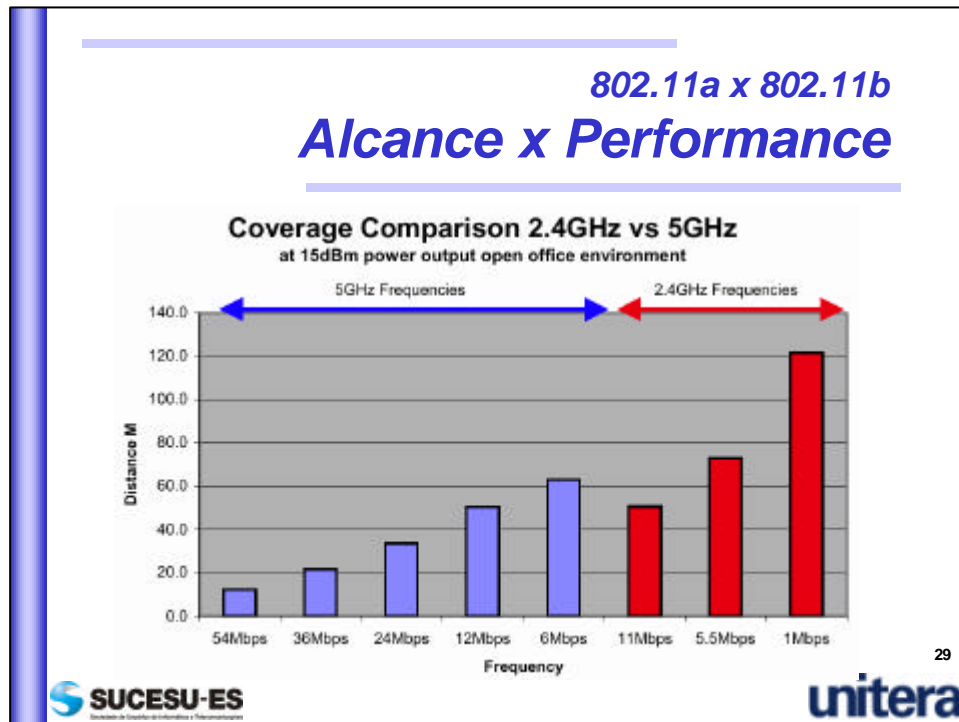
- Padrão em estudo para as redes sem fio
- Implementa
 - QoS para redes 802.11b
 - Melhor gerência de banda
 - Melhor imunidade a interferências
 - Detecta interferências e tenta mudar a frequência de funcionamento

26

IEEE 802.11a x IEEE 802.11b Performance

Alcance x Performance





802.11a x 802.11b 2.4 GHz x 5 GHz

Characteristics	2.4 GHz	5GHz
Max Bandwidth / channel	11Mbps	54Mbps
Min Bandwidth / channel	1Mbps	6Mbps
# Available Non Interfering channels	3	US 4 indoor + 8 Indoor /outdoor EU 8 indoor + 10 indoor /outdoor JP 4 indoor
Total Max indoor capacity	33Mbps	US 648Mbps EU 972Mbps JP 216Mbps
Peak Transmit Power usage	280-300 mW	400-500mW (estimate)

30

SUCESU-ES **unitera**

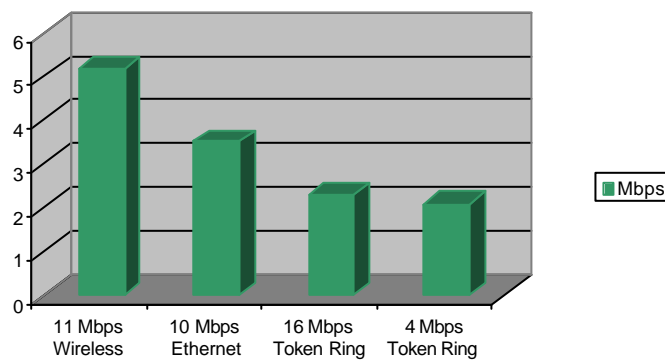
802.11a x 802.11b
2.4 GHz x 5 GHz

2.4GHz		
Mbit/s	Net Mbit/s	Efficiency
1	0.8	82%
2	1.5	76%
5.5	3.4	62%
11	5.2	47%

5GHz		
Mbit/s	Net Mbit/s	Efficiency
6	4.6	77%
9	6.7	75%
12	8.7	73%
18	12.4	69%
24	15.8	66%
36	21.5	60%
48	26.2	55%
54	28.3	52%

31

Comparativo de Throughput



32

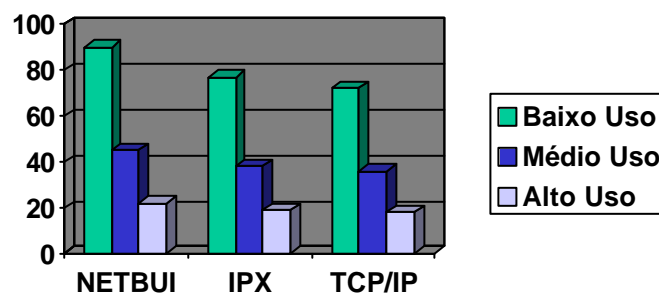
Utilização de Banda

Application	Avg. data rates (kbps)	Peak data rate (kbps)	Maximum delay (sec)	Maximum packet loss rate
e-mail, paging	0.01–0.1	1–10	< 10–100	< 10^{-9}
computer data	0.1–1	10–100	< 1–10	< 10^{-9}
telephony	10–100	10–100	< 0.1–1	< 10^{-4}
digital audio	100–1000	100–1000	< 0.01–0.1	< 10^{-5}
video-conference	100–1000	1000–10000	0.001–0.01	< 10^{-5}


33

Usuários x Célula




- 802.11b (11Mbps)



34





IEEE 802.11
Elementos de Hardware



Elementos de Hardware

- Placa de rede sem fio
- Access Point (AP's)
- Antena
- Cabo
- Amplificador de potência



36

Placa de rede sem fio

- Faz a interface entre a estação de trabalho e a rede
- Cartão PCMCIA
- Adaptador PCI
- Silver x Gold
 - Tamanho da chave de criptografia



37

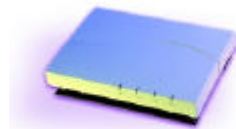
Placa de rede sem fio



38

Access Points

- Conecta a rede cabeada a rede sem fio
 - Função de bridge
 - Pode assumir a função de roteador
- Configuração da frequência dos canais
- Permite roaming entre celulas
 - Se área de cobertura dos APs for sobreposta
 - APs devem estar em canais diferentes
- Gateway entre 802.11a e 802.11b



39

Access Points



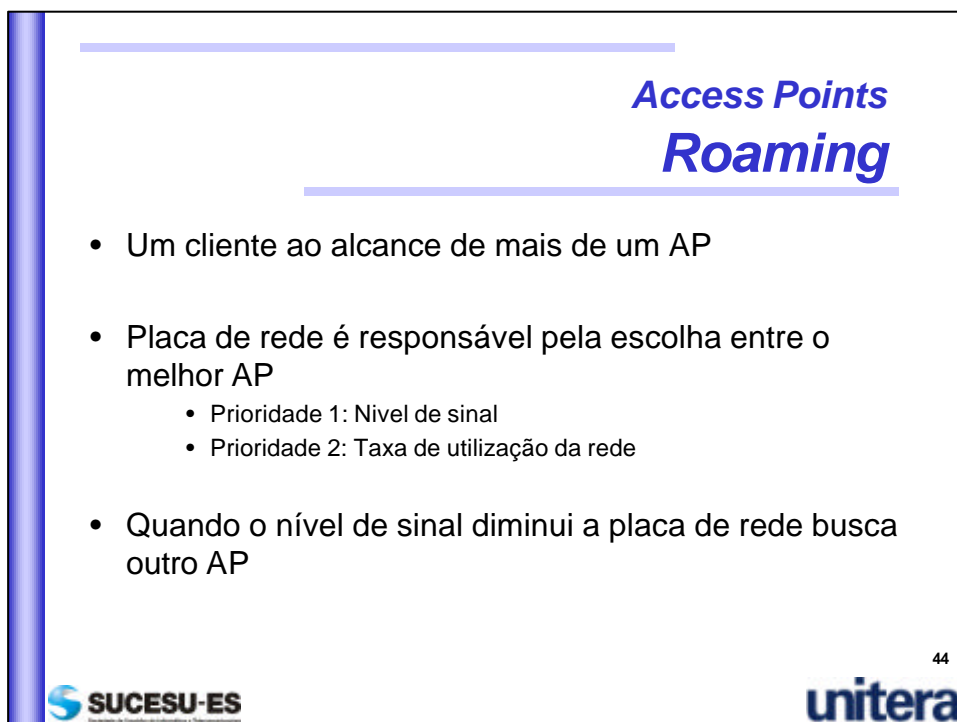
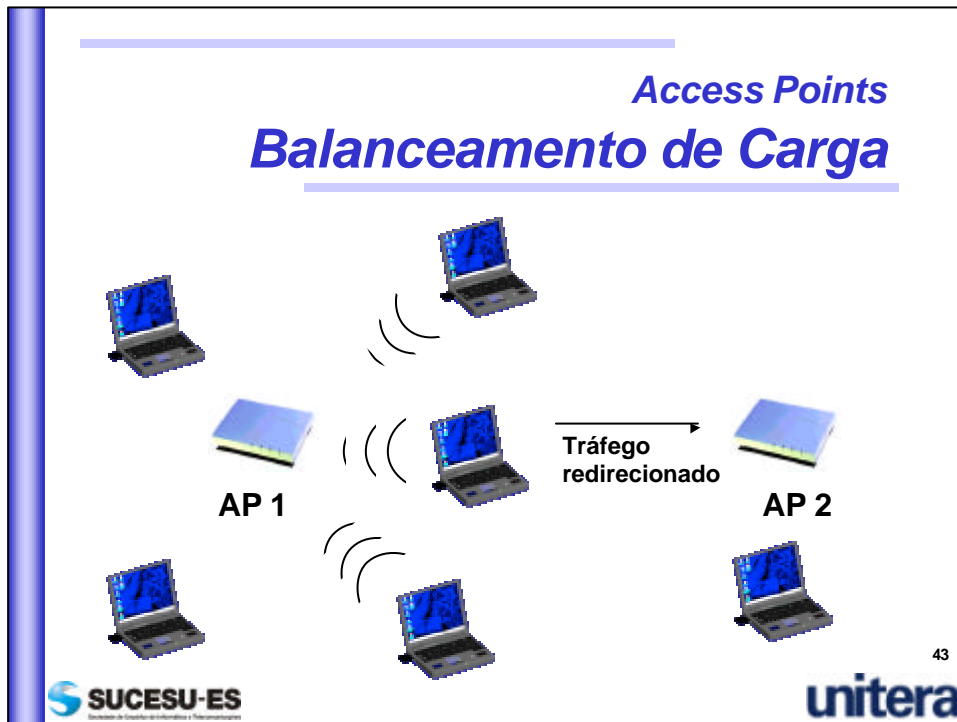
40

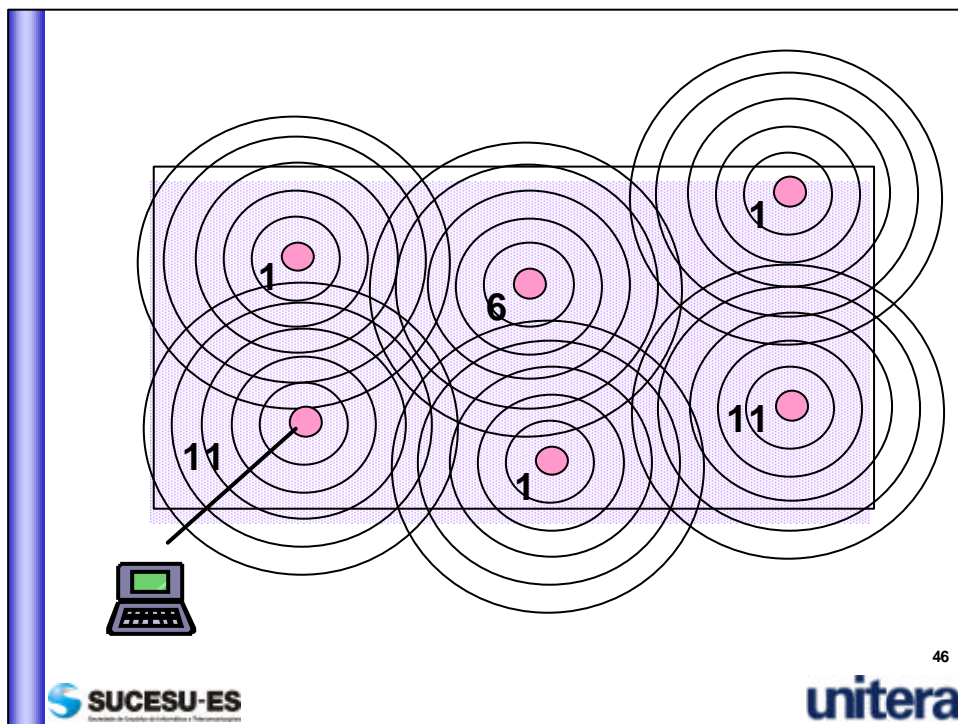
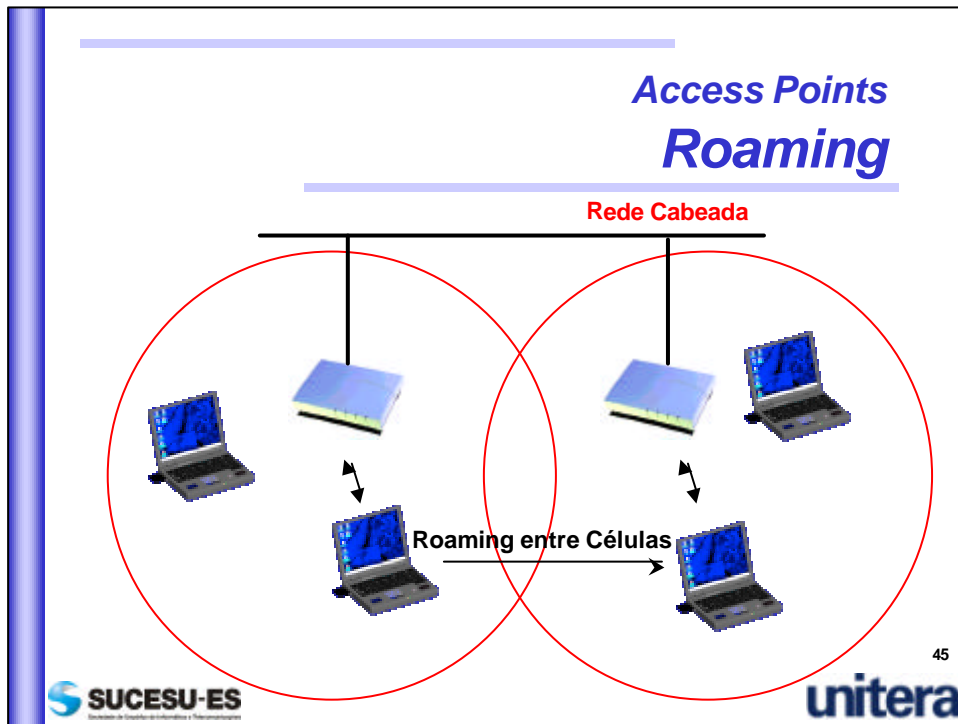
Access Points **Gerenciamento**

- Implementa o gerenciamento da rede sem fio
- Monitora
 - Erros
 - Tráfego
 - Nível de sinal
 - Acessos não autorizados

Access Points **Melhoria de velocidade**

- Redução da área de cobertura de cada Access Point
- Redução da relação Cliente x AP
- Utilização de Balanceamento de carga





Access Points Configuração

- Interface de configuração
 - HTTP, Telnet, SNMP ou Interface serial
- Parâmetros de segurança
 - SSID: Service Set Identifier
 - WEP: Wired Equivalent Privacy
 - EAP: Extensible Authentication Protocol
- Parâmetros de rede
 - DHCP: Dynamic Host Configuration Protocol
 - NAT: Network Address Translation

47

System Configuration - Microsoft Internet Explorer

Orinoco

System Network Wireless DHCP WEP

Information

Name: AP2000-1
Location: Física 2000
Contact Name: Faria Ota. Pinheiro
Contact Email: fariasota@unitera.com
Contact Phone: 5170260781
ObjectID: 1.3.6.1.4.1.1731.1.4.6
Ethernet MAC Address: 00:60:1D:21:09:76
DeviceID: AP-2000-w-726-00-01-01-01-01-01-v2.5
Up Time (DD:HH:MM:SS): 00:00:11:58

Inventory Management

Serial Number	Name	ID	Variant	Version
NetApp:6496	AP-2000 Software Image	85	1	0.7.28
11F7348C328	AP-2000 Hardware Inventory	07	1	1.8
NetApp:6496	AP-Firmware	339	1	7.48
NetApp:6496	BSP-EL-0:spml	111	1	2.5
NetApp:6496	Orinoco MB v1r2.03a	122	1	3.1
NetApp:6496	CardB-FW	123	1	3.1
NetApp:6496	Wireless Card & RF Firmware	21	1	4.4
30UT1458173	Wireless Card A-MC	1	1	4.3
NetApp:6496	Wireless Card B-FW Firmware	1	1	4.3
NetApp:6496	Wireless Card G-NO	1	1	4.3

48

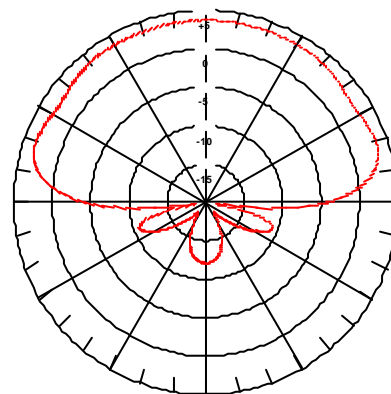
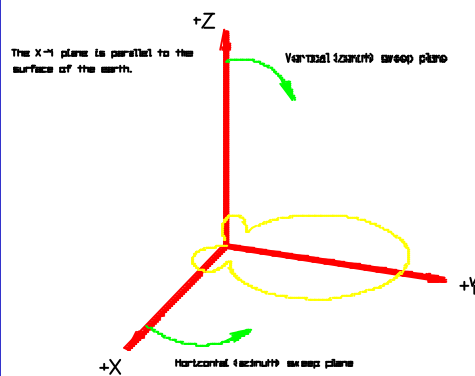
Antenas

- Parte fundamental para o bom funcionamento do sistema sem fio
- Tipos
 - Interna / Externa
 - Direcional / Omnidirecional



49

Antenas Padrão de irradiação



50

Antenas - tipos Direcional

- Concentra o sinal em uma única direção
- Modelos
 - Grade
 - Semi-parabólica
 - Yagi

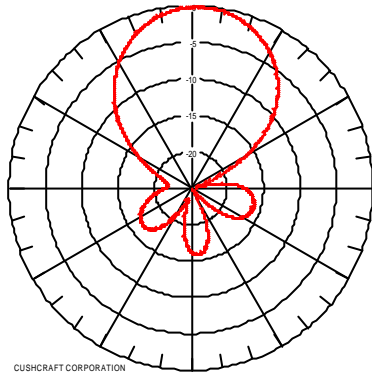
51

Antenas - tipos Direcional

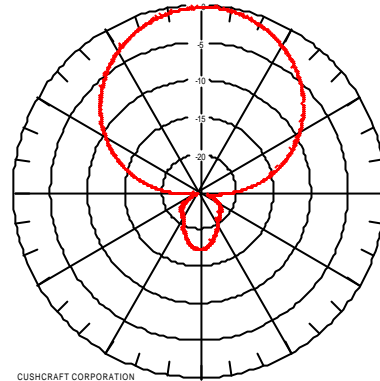


52

Antenas - tipos Direcional



CUSHCRAFT CORPORATION
48 Perimeter Road, Manchester, NH 01103

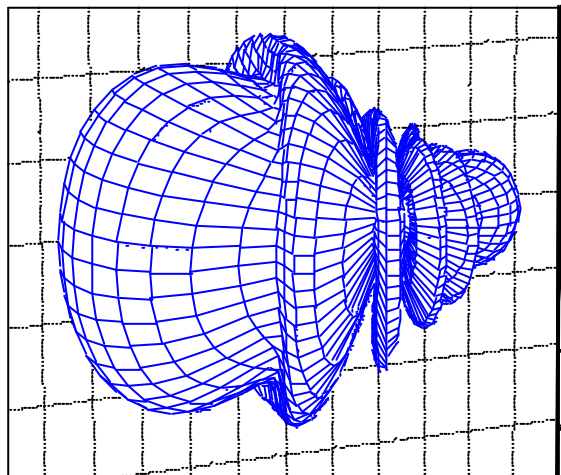


CUSHCRAFT CORPORATION
48 Perimeter Road, Manchester, NH 01103

 **SUCESU-ES**
Universidade de São Carlos - Instituto de Engenharia de São Carlos

unitera

Antenas - tipos Direcional



54

 **SUCESU-ES**
Universidade de São Carlos - Instituto de Engenharia de São Carlos

unitera

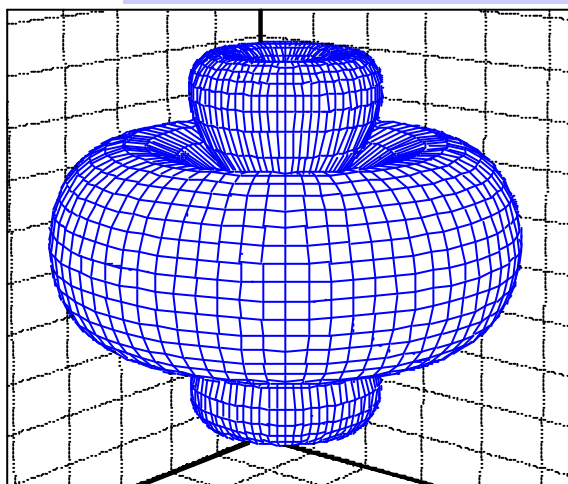
Antenas - tipos *Omnidirecional*

- Transmitem 360 graus em torno do seu eixo
- Também conhecidas como Dipolo



55

Antenas - tipos *Omnidirecional*



56

Antenas Tipos

Externa

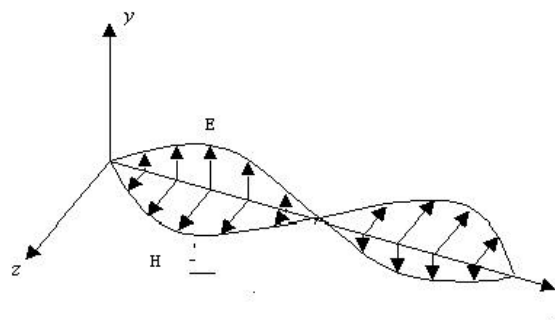


Interna



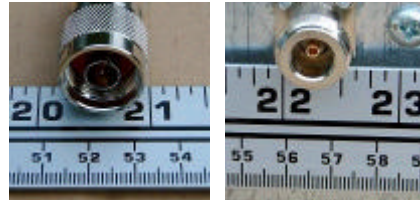
Antenas Polarização

- Define a orientação da onda eletromagnética
- Deve ser igual entre as antenas transmissoras e receptoras

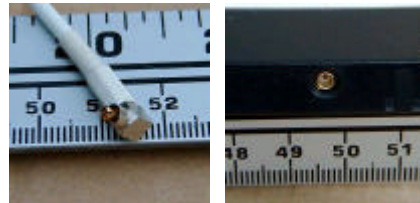


Conectores

Conectot "N"



Conector Lucent



59

Diversos

- Cabo
– RGC213



- Patch cord



60

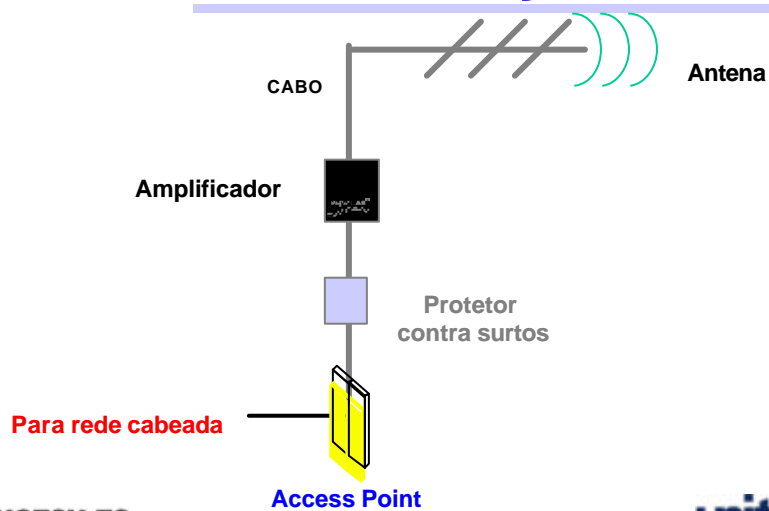
Diversos

- Amplificador de potência
- Protetor de surto
 - Surge protector

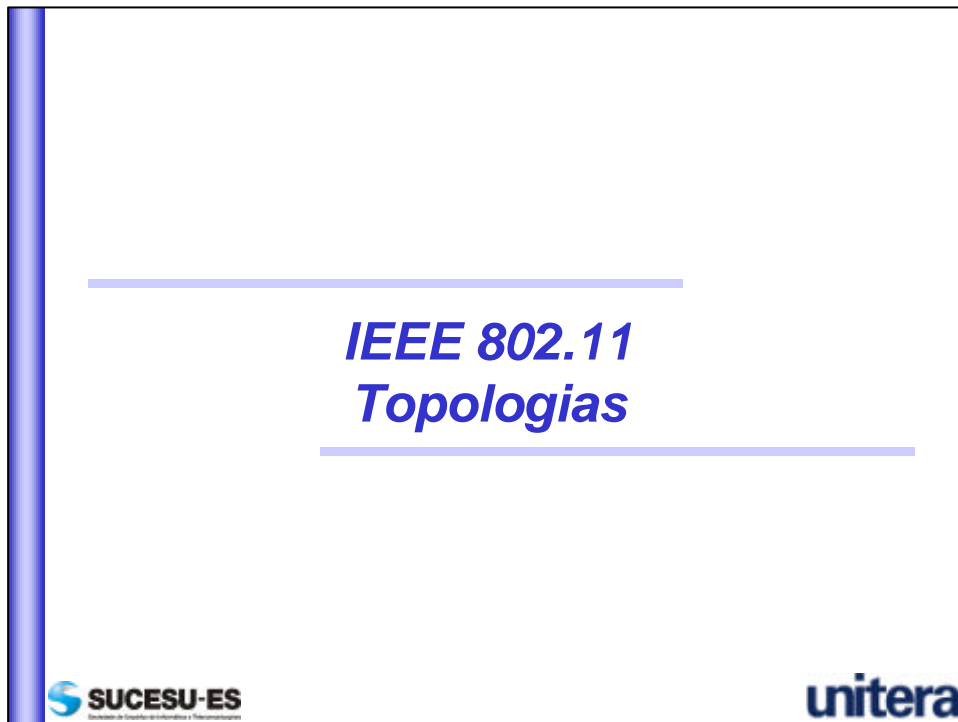


61



Ambiente Externo Instalação Típica



62



**IEEE 802.11
Topologias**



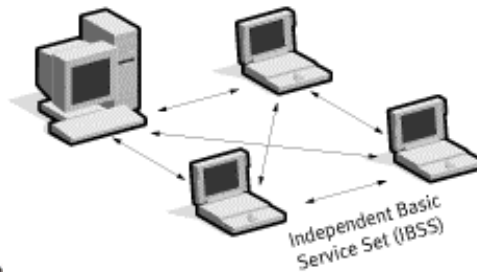
**IEEE 802.11
Topologias**

- O padrão estabelece três topologias básicas
 - IBSS: Independent Basic Service Set
 - BSS: Basic Service Set
 - ESS: Extended Service Set

  64

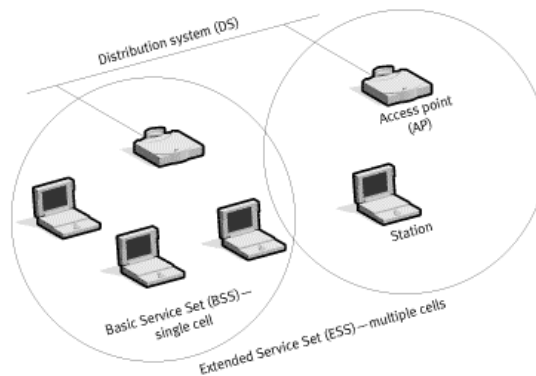
IEEE 802.11 IBSS

- IBSS: Independent Basic Service Set
 - Rede Par-a-Par ou ad-hoc
 - Estações trocam mensagens entre si diretamente
 - Geralmente esta rede não é conectada a uma rede maior
 - Não utiliza Access Points (AP)



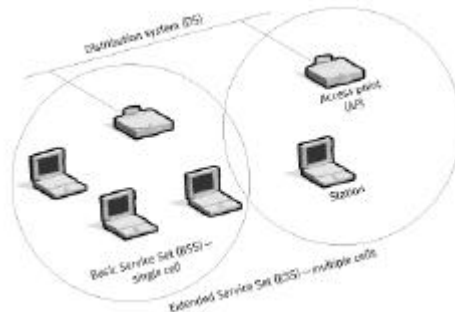
IEEE 802.11 BSS

- BSS: Basic Service Set
 - Utilizado como infra-estrutura básica
 - Os access Points conectam os clientes a uma rede cabeada



IEEE 802.11 ESS

- ESS: Extended Service Set
 - Utilizado como infra-estrutura básica
 - Área de cobertura dos APs é sobreposta
 - APs devem estar em canais diferentes
 - Permite o roaming



IEEE 802.11 Projeto

Projeto

- Análise prévia do ambiente (Site Survey)
- Medida das distâncias entre dispositivos sem fio
- Avaliação das possíveis fontes de interferências

Site Survey

- Etapa mais importante na elaboração dos projetos de wireless
- Atividades
 - Análise do lay-out ou planta do local a ser atendido pela rede wireless
 - Identificar a quantidade de células e Access Points
 - Uso de ferramentas (softwares) para análise de intensidade de sinal e fontes de interferências

Site Survey

- Baseado no levantamento podemos especificar
 - Equipamentos e acessórios necessários
 - Antenas
 - Access Points
 - Quantidade de cabo
 - Conectores
 - Amplificadores

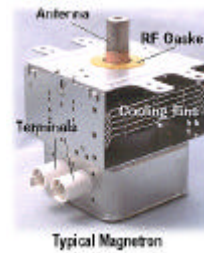
Interferências

- Fontes mais comuns
 - Fornos de microondas
 - Telefones sem fio na mesma frequência
 - Alarmes de segurança na mesma frequência
 - Equipamentos Bluetooth
 - Motores elétricos
 - Outros equipamentos sem fio operando na mesma faixa de frequência



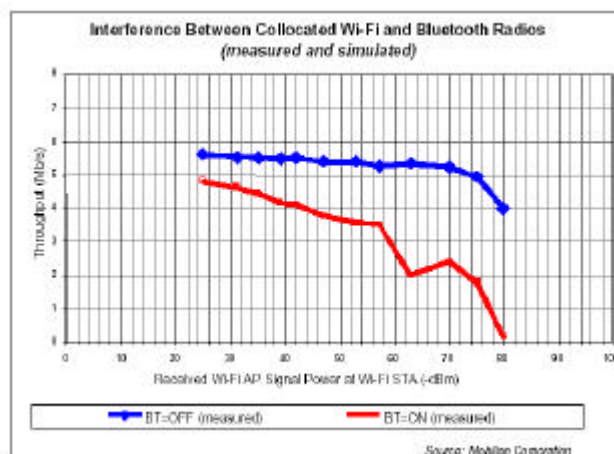
Interferência Forno de microondas

- O Magnetron dos fornos de microondas tem a frequência central de funcionamento em 2450~2458 MHz
 - Interfere com 802.11b/g
- Intensidade de sinal de 18 dBm
 - Medida a 3 metros de distância
 - Conseguir corromper todos os sinais de WLAN !!!
- Soluções
 - Tentar utilizar canais diferentes
 - Aumentar a distância entre o forno e os equipamentos sem fio
 - Utilizar materiais bloqueadores de RF
 - Utilizar 802.11a

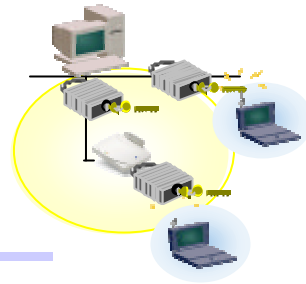


73

Interferência Bluetooth



74



IEEE 802.11

Aspectos de segurança

Segurança em Redes sem Fio

Características

- Um dos maiores desafios do ambiente de redes sem fio é a implementação de um ambiente seguro para o tráfego das informações
- Para cada solução de rede sem fio devemos avaliar ferramentas e topologias que atendam as necessidades da aplicação
- Nenhuma rede é 100% segura e nenhuma ferramenta ou tecnologia utilizada isoladamente garante proteção completa contra ataques e invasões

Segurança em Redes sem Fio **SSID - Service Set ID**

- O SSID é o nome de uma rede sem fio
- Para produtos WLAN o default é "101" para 3COM e "tsunami" para Cisco
- Pode ser necessário para acesso ao Access Point por nome (o SSID funciona como uma senha)
- Quanto mais pessoas conhecerem o SSID, maior a chance de ser mal utilizado
- A mudança do SSID requer a mudança em todos os usuários da rede

77

Padrões **WEP - Wired Equivalent Privacy**

- Criptografia entre o cliente e o Access Point
- Opera na camada de enlace
- Algoritmo criptográfico RC4 da RSA
- Vulnerável a ataques
 - Ataques passivos podem decifrar o tráfego baseado em análises estatísticas
 - Ataques ativos podem gerar novo tráfego de estações "estranhas" baseado em textos planos conhecidos
- Todos os usuários de um mesmo Access Point compartilham a mesma chave de criptografia

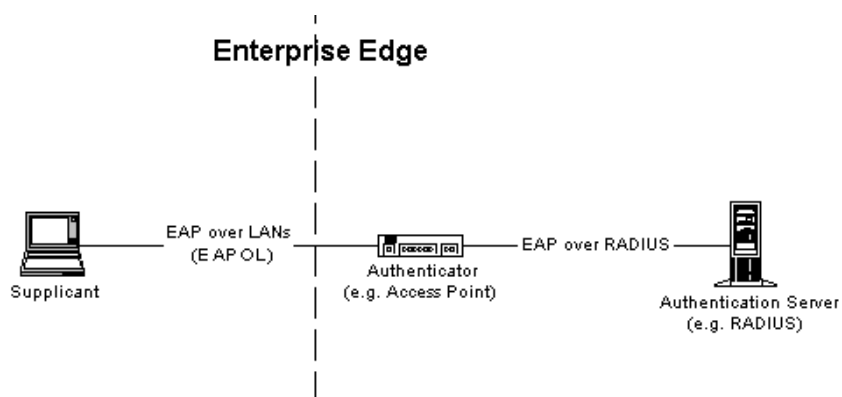
78

Padrões 802.1X

- Especificação para redes cabeadas e Redes sem Fio
- Baseado em portas TCP/IP controladas e não controladas
- Utiliza o protocolo EAP - Extensible Authentication Protocol (RFC 2284)
- Suporte ao protocolo RADIUS e autenticação forte
 - Autenticação centralizada
- Pode prover troca dinâmica de chaves, eliminando alguns dos problemas do WEP
- Roaming é transparente para o usuário final

79

Padrões Arquitetura 802.1X



80

Ataques e Vulnerabilidades

Ataques e Vulnerabilidades Falhas do WEP

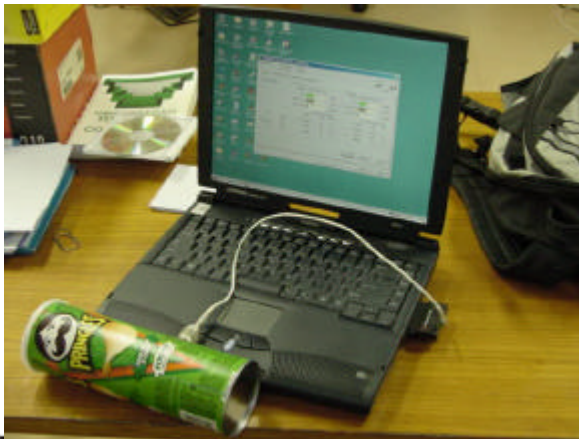
- Os cabeçalhos dos quadros continuam em texto plano, permitindo ao atacante “ver”
 - Origem e destino (MAC)
 - SSID
 - Vetor de inicialização da criptografia
- Captura de vários frames de mesmo vetor de inicialização (IV)
 - Ataques passivos podem decifrar o tráfego baseado em análises estatísticas
 - Ataques ativos podem gerar novo tráfego de estações “estranhas”
- Ataques baseados na construção de dicionários de vetores de inicialização permitem automatizar o processo de invasão

Ataques e Vulnerabilidades Scanners e Sniffers

- Meio compartilhado
 - Uso de outros equipamentos com interface 802.11
- Busca de Access Points e redes “ad-hoc” em funcionamento
- Captura do tráfego
 - NetStumbler (Windows)
 - MiniStumbler (PocketPC)
- Quebra das chaves WEP
 - AirSnort (Linux)
 - WEPCrack (Linux)

Ataques e Vulnerabilidades Scanners e Sniffers




- Vamos comer batatas fritas!!



Ataques e Vulnerabilidades War Driving / War Chalking

- Dirigir ou andar pela cidade e podemos fazer o acesso a redes sem fio
- Instalação default de placas de rede já nos permite acesso a rede sem fio
- Acesso “dentro” da rede, ou seja “atrás” do firewall
- Muitas vezes não precisamos estar próximos da rede invadida
 - Relatos de ataques a redes com distâncias de até 8Km

Ataques e Vulnerabilidades War Driving / War Chalking

KEY	SYMBOL
OPEN NODE	 ssid bandwidth
CLOSED NODE	 ssid
WEP NODE	 ssid access contact bandwidth



Ataques e Vulnerabilidades **Negação de serviço (DoS)**

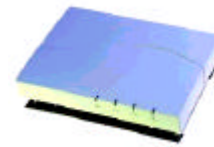
- Geração de tráfego ou interferência na frequência utilizada
 - Acidental
 - Intencional
- Causada por:
 - Telefone sem fio
 - Fornos de microondas
 - Equipamentos Bluetooth
 - Outros Access Points WLAN



87

Ataques e Vulnerabilidades **Acesso físico**

- Roubo ou uso de equipamentos WLAN
 - Access points
 - Estações ou PDA's com acesso autorizado





88

Defesas e Ferramentas



Defesas e ferramentas

- Bloqueio por MAC Address
- SSID – Service Set ID
- WEP – Wired Equivalent Privacy
- Firewall
- VPN – Virtual Private Network
- VLAN – Virtual LAN
- SLAN – Secure LAN
- 802.1x



90

Defesas e Ferramentas **Políticas de Segurança**

- Levantamento dos riscos e vulnerabilidades
- Definição de procedimentos para ativação e uso das Redes sem Fio
 - Quem, quando e onde
- Proibição de Access Points não autorizados
- Proibição de redes “ad-hoc”
- “No final de 2004 o uso de Access Points e redes ad-hoc’s não autorizadas será responsável por mais de 50% das vulnerabilidades em redes sem fio (probabilidade de 0.8)”

Gartner Group - Set/2002

91

Defesas e Ferramentas **Bloqueio por MAC Address**

- Controle do acesso das estações definindo os endereços MAC permitidos na rede
- Este endereço pode ser atacado por Spoofing
- Problemas
 - Devemos listar, manter e distribuir a lista de endereços MAC válidos para cada Access Point
 - Solução inviável para aplicações de acesso público

92

Defesas e Ferramentas *Troca do SSID*

- Desabilitar o broadcast do SSID
- Não utilizar
 - Valores default dos fabricantes
 - Valores "sugestivos"
- Quanto mais pessoas conhecerem o SSID, maior a chance de ser mal utilizado
- A mudança do SSID requer a mudança em todas as estações da rede

93

Defesas e Ferramentas *Uso do WEP*

- Apesar das vulnerabilidades melhor do que não utilizar
- Utilizar a maior chave possível (128 bits)
 - Depende do Hardware
- Uso combinado com outras defesas como VPN ou Criptografia adicional
- Soluções proprietárias
 - Cisco - LEAP

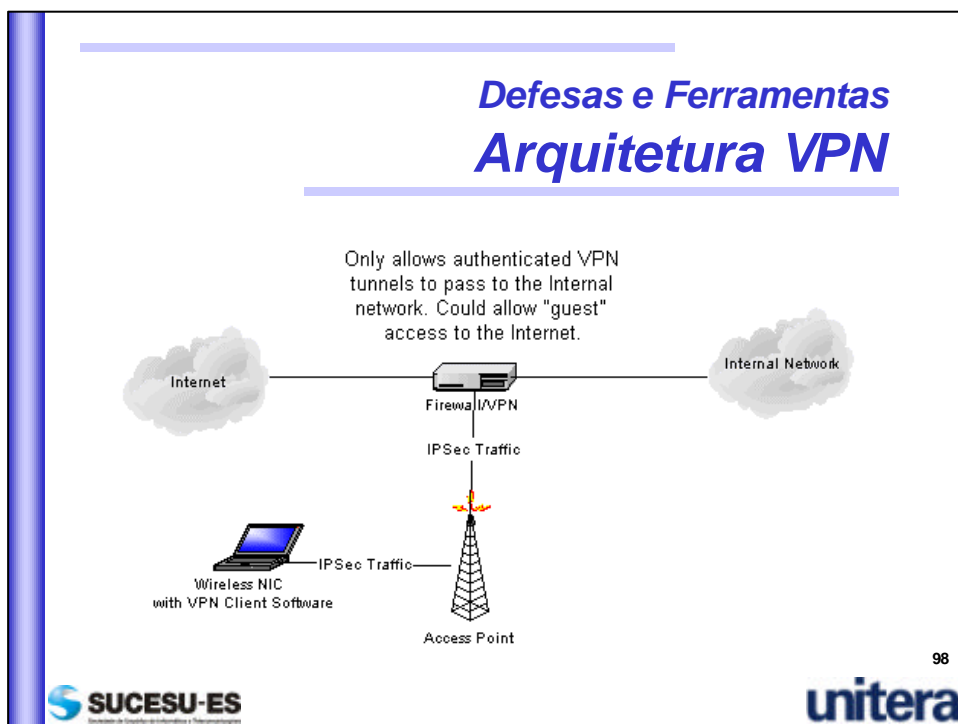
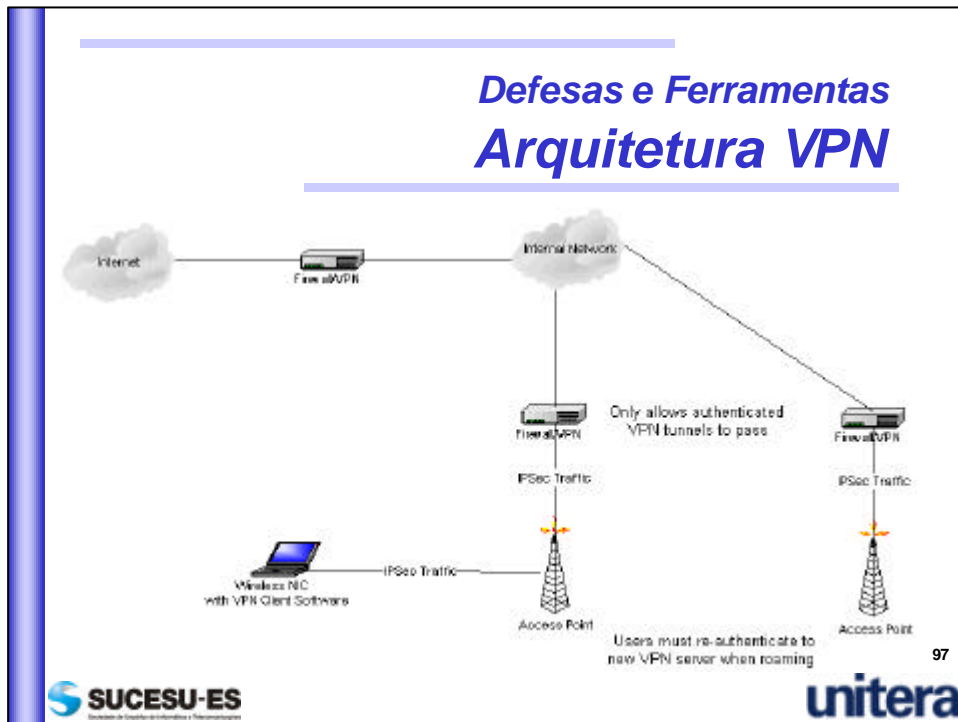
94

Defesas e Ferramentas **Firewall**

- Isola o tráfego da rede sem fio da rede cabeada
- Utilização de uma DMZ
- Provê autenticação para usuários da Rede sem Fio terem acesso a rede cabeada

Defesas e Ferramentas **VPN – Virtual Private Network**

- Provê uma solução escalável de autenticação e criptografia
- Utilização do protocolo IPSec
- Outros protocolos de criptografia como
 - SSL
 - SSH
 - PGP

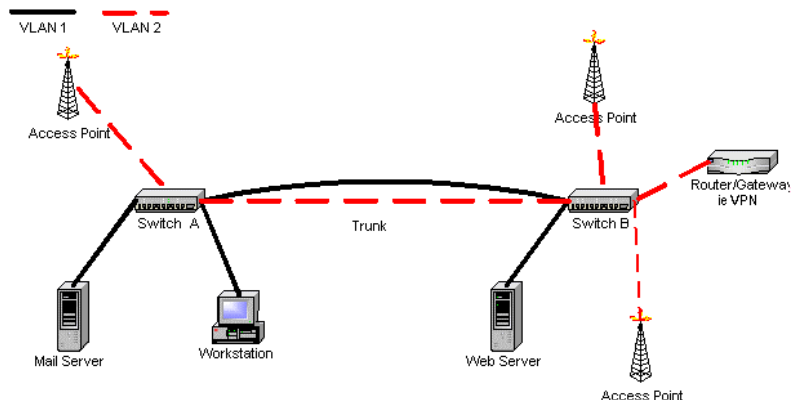


Defesas e Ferramentas VLAN – Virtual LAN

- Possibilita reunir redes sem fio em uma única VLAN, mesmo atingindo regiões geográficamente separadas
- Utiliza o padrão 802.1Q VLAN tagging para criar uma subrede sem fio e um gateway VPN para autenticação e encriptação

99

Defesas e Ferramentas Arquitetura VLAN



100

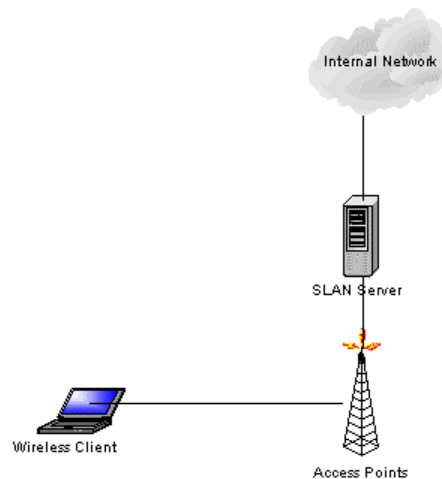
Defesas e Ferramentas **Autenticação (802.1X)**

- RADIUS
 - Remote Autentication Dial-in User Services
- Biometria
- Chaves Públicas – PKI
- Tokens
- Uso de senhas fortes

Defesas e Ferramentas **SLAN - Secure LAN**

- Tem o objetivo de proteger o link entre o cliente Wireless e a rede cabeada
- Similar a VPN e provê:
 - Autenticação do Servidor e Cliente
 - Privacidade e integridade de dados
 - Chaves por sessão, de curta duração
- Mais simples, mais eficiente e melhor custo benefício em comparação com a VPN
- Não é muito escalável
- Suporta Linux e Windows
- É Open Source (<http://slan.sourceforge.net>)

Defesas e Ferramentas Arquitetura SLAN



Defesas e Ferramentas SLAN – passo a passo

1. Handshake entre Cliente e Servidor
2. Troca de chaves (Diffie-Hellman)
3. Autenticação do Servidor (public key fingerprint)
4. Autenticação do Cliente (optional)
5. Configuração do IP
 - Pool de endereços IP
 - Ajuste na tabela de roteamento

Defesas e Ferramentas *Estação WLAN*

- Segurança física da estação
- Uso de Firewalls pessoais
- Evitar o compartilhamento de diretórios

105

Defesas e Ferramentas *Outras*

- Desabilitar o DHCP
- Troca da senha default do AP
- Access Point
 - Localização física
 - Desativação fora dos horários de uso
- Uso de Ferramentas de detecção de ataques
 - Assinaturas de ataques
 - Monitoramento das taxas de conexão
 - A ferramenta não é 100% confiável

106

Implementando WLAN

- A implementação de segurança em redes sem fio dependem do tamanho da empresa e informações que trafegarão na rede
- Veremos algumas questões relativas a implementação de WLAN para redes:
 - Básicas
 - Intermediárias
 - Enterprise

107

Implementando WLAN **WLAN - Básica**

- Poucos usuários (5 – 10)
- Uso de WEP (alguns fabricantes dispõem de soluções proprietárias de 128-bits)
- Permitir somente alguns endereços MAC terem acesso a rede
- Troca do SSID e chaves WEP keys a cada 30-60 dias
- Não há a necessidade de adquirir hardware e software adicional

108

Implementando WLAN **WLAN – Intermediária**

- Atende de 11 a 100 usuários
- Pode utilizar o bloqueio por endereço MAC e troca periódica de chaves
- Alguns fabricantes tem limitação do número de endereços MAC na tabela de bloqueio
- A solução SLAN também é uma opção
- Outra solução é utilizar tuneis VPN




109

Implementando WLAN **WLAN – Enterprise**



- Atende a mais de 100 usuários
- Troca periódica de chaves WEP não é prática
- Múltiplos Access Points e subredes
- Soluções possíveis incluem:
 - VLAN
 - VPN
 - Soluções customizadas
 - 802.1x

110

Conclusão



Referências



Bibliografia Internet

- Intel:
 - Wireless white papers:
http://www.intel.com/network/connectivity/resources/doc_library/index.htm
 - 802.11b white paper:
http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/NP1692-01.pdf
 - 802.11a white paper:
http://www.intel.com/network/connectivity/resources/doc_library/wHITE_papers/NP2040_11.01.pdf
 - 802.11g white paper:
http://www.intel.com/network/connectivity/resources/doc_library/wHITE_papers/802_11g.pdf

113

Bibliografia Internet

- 3Com
 - http://www.3com.com/other/pdfs/infra/corpinfo/en_US/50307201.pdf
- National Institute of Standards and Technology
 - <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>
- Wi-Fi Alliance
 - <http://www.wi-fi.org/>
- IEEE 802.11 Standards
 - <http://standards.ieee.org/getieee802/>

114

Congresso InfoWorld 2003
Tutorial – Redes Locais sem Fio



Gilberto Sudré

Av. N. Sra. da Penha, 520 / 3 and

0 xx 27 320-03160

gilberto@unitera.com.br

www.unitera.com.br

UNITERA Tecnologia



115

