Cisco Systems

# Segurança em Ambientes Wireless

**Mauricio Gaudencio**
**System Engineer**
**mgaudenc@cisco.com**

## Mercado Corporativo

Cisco.com

- Os funcionários querem Wireless
- ROI— Aumento de produtividade em até 70 minutos por dia – 22% de ganho de produtividade
- Se o IT não instalar Wireless, os funcionários irão
  - APs de baixo custo disponíveis em lojas de departamento
- Instalações inadequadas expõe a rede corporativa
- IT deve instalar WLANs, e implementar com segurança

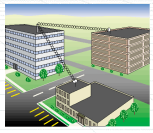
  

## Principais aplicações para redes Wireless

Cisco.com

In-Building Wireless LANs

Wireless Bridges



Acesso públicos - Hot Spots

Rede Residencial

## IEEE 802.11 Standards

Cisco.com

- 802.11a - 5GHz – Ratificado em 1999
- 802.11b - 11Mb 2.4GHz—ratificado em 1997
- 802.11d - World Mode e domínios regulatórios adicionais
- 802.11e – Qualidade de Serviço
- 802.11f - Inter-Access Point Protocol (IAPP)
- 802.11g – Maiores taxas de transmissão (>20mBps) em 2.4GHz
- 802.11h – Seleção dinâmica de freqüência e mecanismos para controle de potência de transmissão
- 802.11i – autenticação e segurança (WPA)

## 802.11a

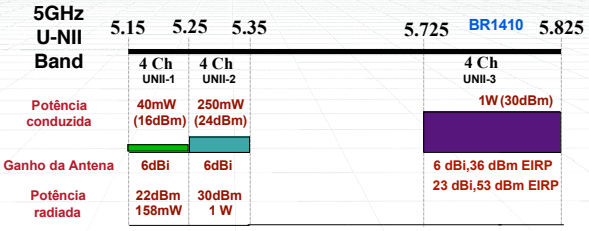
Cisco.com

- Ratificado em Setembro de 1999
- Tecnologia similar à HylerLAN2
- Definido a 54Mb
- Provê 8 canais para uso indoor (UNII1 e UNII2 combinados)
- Regulação varia muito de pais para pais
- Não liberado para Brasil e Europa
  - Seleção dinâmica de freqüência e controle de potência de transmissão – não são parte do 802.11a

## Potência conduzida e Radiada

Cisco.com




UNII-1: *Uso Indoor, antena deve ser fichada ao radio*
UNII-2: *Uso Indoor/Outdoor, antena ficha ou removível*
UNII-3: *Apenas uso Outdoor (Bridging)*

## 802.11b

11Mb 2.4GHz Direct Sequence

Cisco.com

- Ratificado em Setembro, 1997
- 11Mb 2.4Gz
- 11 canais - US
- 13 canais – ETSI, Brasil
- 14 canais - Japão
- Níveis de potência - 36dBm EIRP-FCC, Anatel
  20dBm EIRP-ETSI
- Aprovado praticamente no mundo todo

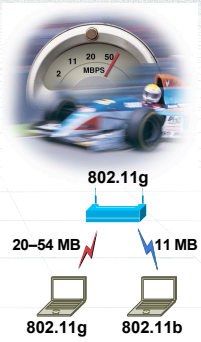
  

## IEEE802.11g

*Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band*

Cisco.com

- Provê maiores velocidades a 2.4 GHz
- Velocidades similares às do 802.11a
- Compatibilidade com 11 Mbps (802.11b)
- Mesma modulação que o 802.11a - OFDM
- Standard ratificado em Junho 2003



## IEEE 802.11i – Segurança

Cisco.com

**Nova versção (WPA) ratificado em Setembro/03**

**Inclui:**

**Melhorias para Autenticação e Criptografia**

- **MIC, IV Sequencing, Fast Packet Keying**
- **Substitui WEP por TKIP**
- **TKIP (Temporal Key Integrity Protocol)**
  - **Funções de Text/hash, MIC etc ainda em estudo**
- **Nova versão (WPA2) ainda em draft**
  - **Criptografia AES (requer substituição de hardware)**



## Preocupação n.º 1: Segurança

Cisco.com

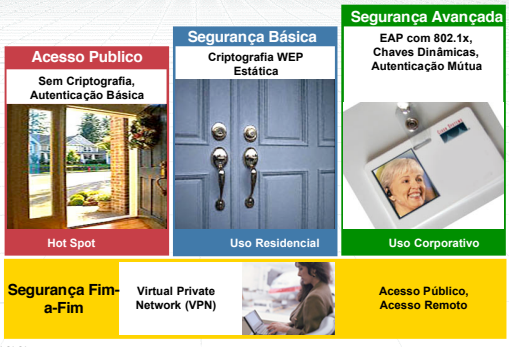
- **De 43 redes rastreadas nos maiores centros de concentração de escritórios de São Paulo apenas 08 tomaram medidas de segurança pertinentes**

*Fonte: Info Exame Junho/2002*




## Diferentes necessidades de Segurança

Cisco.com






## Diferentes necessidades de Segurança

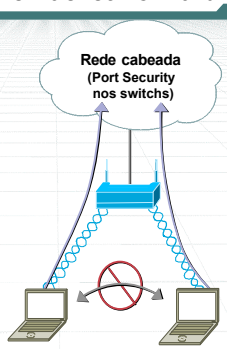
Cisco.com


**Necessidades:**

- **Facilidade de uso**
- **Proteção da Infra-estutura**
- **Mecanismos de**
- **Autenticação e bilhetagem**

## PSPF—
## Publicly Secure Packet Forwarding

Cisco.com




- Bloqueia a comunicação entre clientes WLAN

## Diferentes necessidades de Segurança

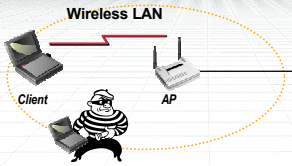
Cisco.com

- Segurança Básica
- Segurança do padrão 802.11:
  - SSID
  - Autenticação MAC
  - WEP Estática

## Segurança padrão 802.11

Cisco.com




Desafios

- Autenticação – Qualquer um na área de cobertura pode entrar na rede WLAN
- Privacidade – Pacotes podem ser capturados com uso de sniffer Wireless

- SSID
- Open Authentication
- MAC Authentication
- Chaves WEP estáticas (WECA exige chaves de apenas 40 bit)
- Shared Key Authentication

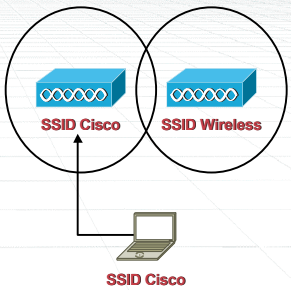
*Objetivo: Fazer a segurança das redes WLAN equivalente a das redes cabeadas (WEP - Wired Equivalent Privacy)*

## O Service Set Identifier (SSID)

Cisco.com

- Usados para separar redes Wireless logicamente

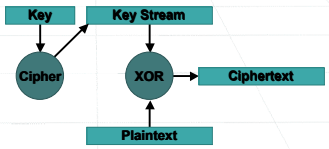


## Criptografia WEP

Cisco.com

- Wired Equivalent Privacy
- Baseado no protocolo RC4 symmetric stream cipher da RSA
- Estático, pre-shared, 40 bit ou 104 bit Chaves nos clientes e access point




WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 17

## 802.11 Open Authentication

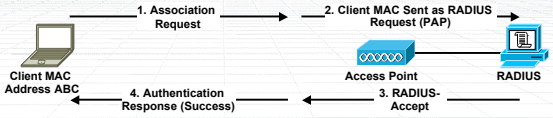
Cisco.com

- Autenticação orientada a dispositivo
- Utiliza autenticação nula – Toda requisição é aceita
- Sem WEP, a rede está aberta para qualquer usuário
- Se criptografia WEP está habilitada, WEP se torna um autenticador indireto

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 18

## Autenticação 802.11 - MAC Address

Cisco.com




- Não é parte do padrão 802.11
- Implementação específica de cada Vendor
- Usado para aumentar a segurança da autenticação Open ou Shared Key

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 19

## Diferentes necessidades de Segurança

Cisco.com

**Necessidade de Segurança avançada**

**Segurança Avançada**

EAP com 802.1x, Chaves Dinâmicas, Autenticação Mútua

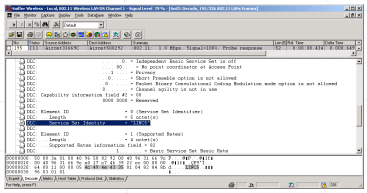
**Uso Corporativo**

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 20

## Vulnerabilidades do padrão 802.11

Cisco.com

- SSID não é um mecanismo de segurança!
- Mesmo desabilitando o broadcast do SSID não evita que um hacker possa ver
- Desabilitar broadcasts de SSID pode impactar a compatibilidade WiFi





## Vulnerabilidades do padrão 802.11

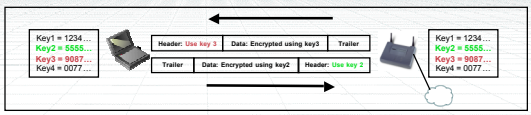
Cisco.com

- Autenticação MAC é fraca
- Endereços MAC são enviados em clear text
- Endereços MAC podem ser "sniffados" e "spoofados"



## Wired Equivalent Privacy (WEP) Estática

Cisco.com




- Criptografia de dados para evitar espionagem
- Necessário conhecer a chave para comunicar com a rede
- Todos os equipamentos Wireless (clientes e APs) usam a mesma chave.
- Gerenciamento e distribuição de chaves é problemático
  - Impossível escalar com segurança



## Wep Estática (cont)

Cisco.com

- Para criptografar, XOR da chave com o texto aberto
  - Chave ⊗ Texto aberto => Texto criptografado
- Para decriptografar, XOR da chave com o texto criptografado
  - Chave ⊗ Texto criptografado => Texto aberto

"WIRELESS" = 58495245C455353
Chave = 123456789ABCDEF XOR
4A7D043D6FBE9C
Chave = 123456789ABCDEF XOR
"WIRELESS" = 58495245C455353

## Derivação estática da chave

Cisco.com

- 802.11 WEP é vulnerável
- A chave WEP pode ser derivada, utilizando análise estatística, com 1M a 4M de frames
- O ataque é passivo, e apenas 'escuta' a rede wireless
- Implementado no AirSnort

## Segurança 802.11

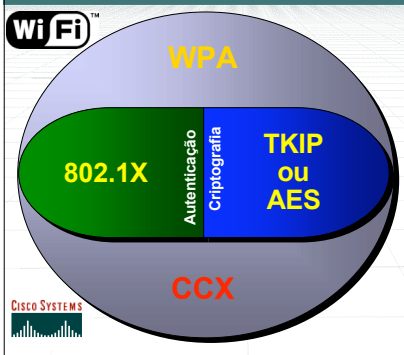
Cisco.com

- Os mecanismos de segurança 802.11 foram desenvolvidos em 1997 e são vulneráveis!
  - SSID
  - Shared Key authentication
  - MAC authentication
  - Static WEP
- Ok para uso residencial, mas NÃO para uso corporativo!!

## Enterprise-Class WLAN Security: Arquitetura de Segurança Wireless

Cisco.com




**WPA**
Wi-Fi Protected Access

**TKIP**
Temporal Key Integrity Protocol

**AES**
Advanced Encryption Standard

**CCX**
Cisco Compatible eXtensions

## 802.1X para 802.11

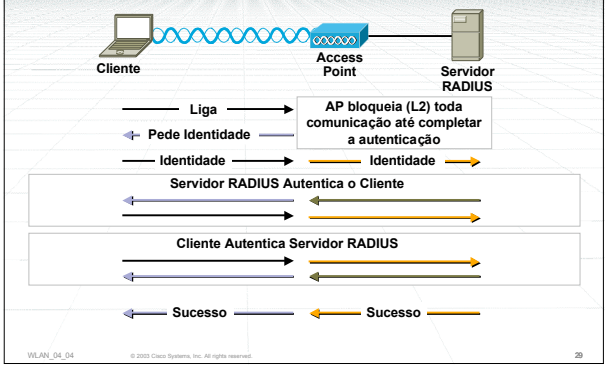
Cisco.com

- Mecanismo de autenticação para acesso à redes
- Bloqueia toda a comunicação, permitindo apenas a autenticação
- Algorítmos Extensible Authentication Protocol (EAP)
  - Password-based
  - Baseado em chaves (PKI)
  - Biometrics
  - Outros

## 802.1X - Como Funciona

Cisco.com

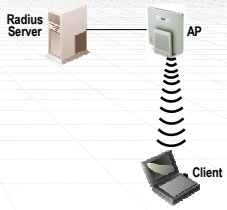





## Segurança WLAN : Autenticação 802.1X

Cisco.com

- Autenticação Mútua
- LEAP
  - "Lightweight" EAP
  - Suporta os principais sistemas operacionais: WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS
- EAP-TLS
  - EAP-Transport Layer Security
  - Utilização de Certificados Digitais (PKI)
- PEAP / EAP-FAST
  - "Protected" EAP
  - Estabelece um Túnel segura (similar a SSL)
  - Suportado por Cisco, Microsoft, & RSA
  - Suporte a One-Time Passwords ("OTP")

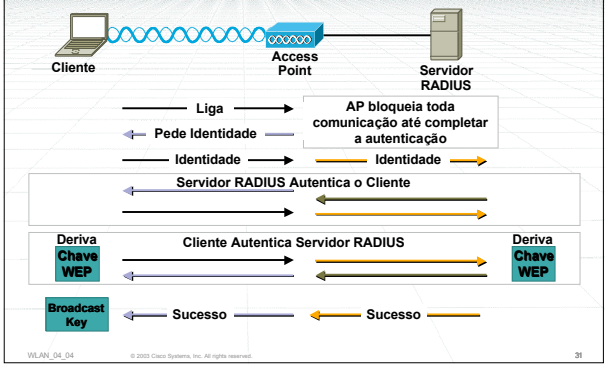



Cisco Systems RSA Security Microsoft



## Autenticação EAP

Cisco.com






## Criptografia Forte

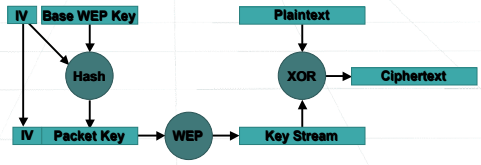
Cisco.com

- Temporal Key Integrity Protocol (TKIP)
  - Aumenta segurança da criptografia WEP
  - Chaves novas por pacotes
  - Message Integrity Check
- AES
  - Advanced Encryption Standard
  - Mais novo padrão de criptografia
  - Requer criptografia em Hardware
- VPN over Wireless
  - Criptografia 3DES—Seguro e confiável

## Criptografia TKIP

Cisco.com

- Per Packet Keying
- IV Hashing
- Message Integrity Check
- Broadcast Key Rotation






## Diferentes necessidades de Segurança

Cisco.com

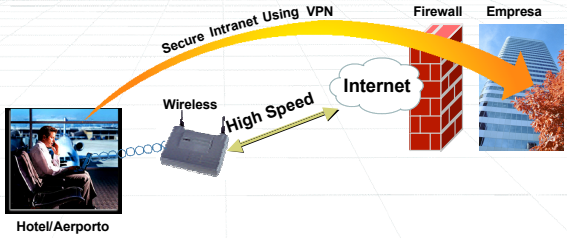
### Segurança Fim a Fim

| Segurança Fim-a-Fim | Virtual Private Network (VPN) |  | Acesso Público, Acesso Remoto |
|---|---|---|---|



## Segurança de Acesso Remoto VPNs

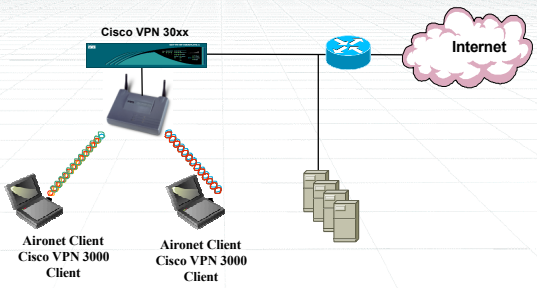
Cisco.com






## VPN over 802.11

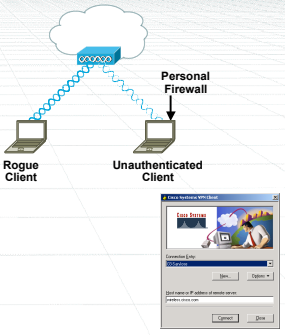
Cisco.com



## VPN over 802.11

Cisco.com

- Requer dois Logins separados
- Impacto de 30% a 40% na performance
- Pode requerer diversos concentradores de VPN
- Suporta apenas IP unicast
  - Não suporta IPX, AppleTalk
  - Não suporta multicast

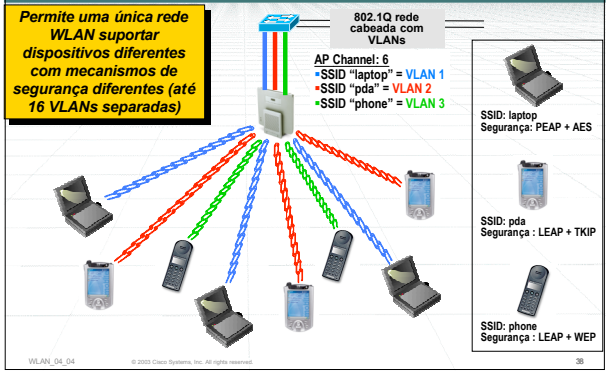





## Diferenciação de Clientes com VLANs

Cisco.com

*Permite uma única rede WLAN suportar dispositivos diferentes com mecanismos de segurança diferentes (até 16 VLANs separadas)*






## New Security Enhancements Mitigate Network Attacks

Cisco.com

| Attack | Authentication: Open<br>Encryption: Static WEP | Authentication: Cisco LEAP, EAP-TLS or PEAP<br>Encryption: Dynamic WEP | Authentication: Cisco LEAP, EAP-TLS or PEAP<br>Encryption: TKIP or AES |
|---|---|---|---|
| Man-in-the-Middle | Protected from War Driving | Protected from Script Kiddies | Protected from Professionals |
| Authentication Forging | Vulnerable | Protected | Protected |
| Weak key attacks | Vulnerable | Vulnerable | Protected |
| Packet Forgery | Vulnerable | Vulnerable | Protected |
| Brute Force Attacks | 40-bit WEP Vulnerable | Protected * | Protected * |

* Strong passwords required with Cisco LEAP

** PEAP vulnerable to man-in-the-middle attacks when used with legacy authentication that derives keys, e.g., GSM-SIM



## Conclusão

Cisco.com

- Diferentes utilizações para as redes Wireless tem necessidades de segurança diferentes
- Sua rede Wireless pode ser tão segura quanto sua necessidade
- Políticas e procedimentos de segurança são tão importantes quanto tecnologias