

CISCO SYSTEMS

Segurança em Ambientes Wireless

Mauricio Gaudencio
System Engineer
mgaudenc@cisco.com



WLAN_04_04 © 2003, Cisco Systems, Inc. All rights reserved. 1

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**



WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 2

Principais aplicações para redes Wireless

Cisco.com

<p>In-Building Wireless LANs</p> 	<p>Wireless Bridges</p> 
<p>Acesso públicos - Hot Spots</p> 	<p>Rede Residencial</p> 

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 3

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 frequência e mecanismos para controle de potência de transmissão
- 802.11i** – autenticação e segurança (WPA)

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 4

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 frequência e controle de potência de transmissão – não são parte do 802.11a

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 5

Potência conduzida e Radiada

Cisco.com

5GHz U-NII Band	5.15	5.25	5.35	5.725	BR1410	5.825
4 Ch UNII-1	40mW (16dBm)	250mW (24dBm)				
4 Ch UNII-2						
4 Ch UNII-3					1W (30dBm)	
Potência conduzida	40mW (16dBm)	250mW (24dBm)			1W (30dBm)	
Ganho da Antena	6dBi	6dBi			6 dBi, 36 dBm EIRP	23 dBi, 53 dBm EIRP
Potência radiada	22dBm 158mW	30dBm 1 W				

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)

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 6

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 7

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 8

IEEE 802.11i – Segurança

Cisco.com

Nova versão (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)



WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 9

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

<http://www.arwain.net/evan/pringles.htm>



WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 10

Diferentes necessidades de Segurança

Cisco.com

<p>Acesso Público</p> <p>Sem Criptografia, Autenticação Básica</p>  <p>Hot Spot</p>	<p>Segurança Básica</p> <p>Criptografia WEP Estática</p>  <p>Uso Residencial</p>	<p>Segurança Avançada</p> <p>EAP com 802.1x, Chaves Dinâmicas, Autenticação Mútua</p>  <p>Uso Corporativo</p>
<p>Segurança Fim-a-Fim</p> <p>Virtual Private Network (VPN)</p> 	<p>Acesso Público, Acesso Remoto</p> 	

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 11

Diferentes necessidades de Segurança

Cisco.com

<p>Acesso Público</p> <p>Sem Criptografia, Autenticação Básica</p>  <p>Hot Spot</p>	<p>Necessidades:</p> <ul style="list-style-type: none"> •Facilidade de uso •Proteção da Infra-estrutura •Mecanismos de Autenticação e bilhetagem
--	--

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 12

PSPF— Publicly Secure Packet Forwarding

Cisco.com

Rede cabeada
(Port Security nos switches)

• Bloqueia a comunicação entre clientes WLAN

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 13

Diferentes necessidades de Segurança

Cisco.com

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

Segurança Básica

Criptografia WEP Estática

Uso Residencial

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 14

Segurança padrão 802.11

Cisco.com

Wireless LAN

Rede Corporativa

Client AP

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)

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 15

O Service Set Identifier (SSID)

Cisco.com

- Usados para separar redes Wireless logicamente

SSID Cisco

SSID Wireless

SSID Cisco

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 16

Criptografia WEP

- 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

The diagram shows a flow from a 'Key' box to a 'Cipher' circle, which outputs a 'Key Stream' box. This 'Key Stream' box then goes to an 'XOR' circle, which also receives 'Plaintext' from below. The output of the XOR circle is a 'Ciphertext' box.

802.11 Open Authentication

- 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

Autenticação 802.11 - MAC Address

The diagram shows a sequence of four steps: 1. Association Request from Client MAC Address ABC to Access Point. 2. Client MAC Sent as RADIUS Request (PAP) from Access Point to RADIUS. 3. RADIUS-Accept from RADIUS to Access Point. 4. Authentication Response (Success) from Access Point to Client MAC Address ABC.

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

Diferentes necessidades de Segurança

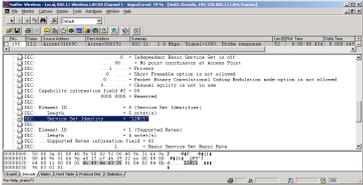
Segurança Avançada
EAP com 802.1x, Chaves Dinâmicas, Autenticação Mútua

Necessidade de Segurança avançada

Uso Corporativo

Vulnerabilidades do padrão 802.11

- 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



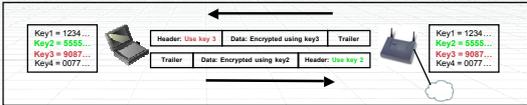
WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 21

Vulnerabilidades do padrão 802.11

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 22

Wired Equivalent Privacy (WEP) Estática



- 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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 23

Wep Estática (cont)

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



“WIRELESS” = 58495245C455353
 Chave = 123456789ABCDEF XOR 4A7D043D6FBE9C
 Chave = 123456789ABCDEF XOR “WIRELESS” = 58495245C455353

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 24

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 25

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!!

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 26

Enterprise-Class WLAN Security: Arquitetura de Segurança Wireless

Cisco.com

The diagram shows a central sphere representing the security architecture. The top part is labeled 'WPA'. The middle part is split into '802.1X' (Authentication) and 'TKIP ou AES' (Encryption). The bottom part is labeled 'CCX'. A legend on the right lists: WPA (Wi-Fi Protected Access), TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption Standard), and CCX (Cisco Compatible eXtensions).

WPA
Wi-Fi Protected Access

TKIP
Temporal Key Integrity Protocol

AES
Advanced Encryption Standard

CCX
Cisco Compatible eXtensions

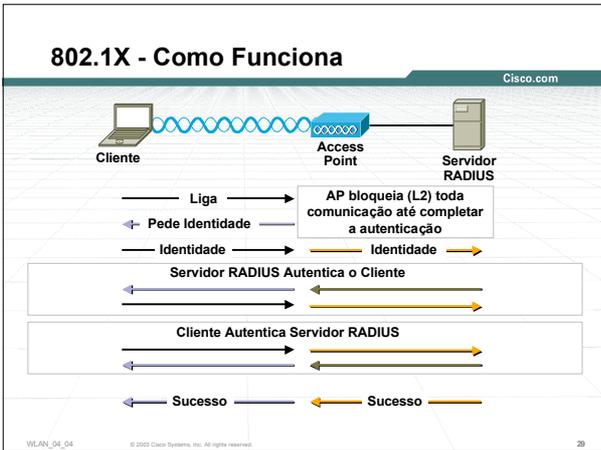
WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 27

802.1X para 802.11

Cisco.com

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 28

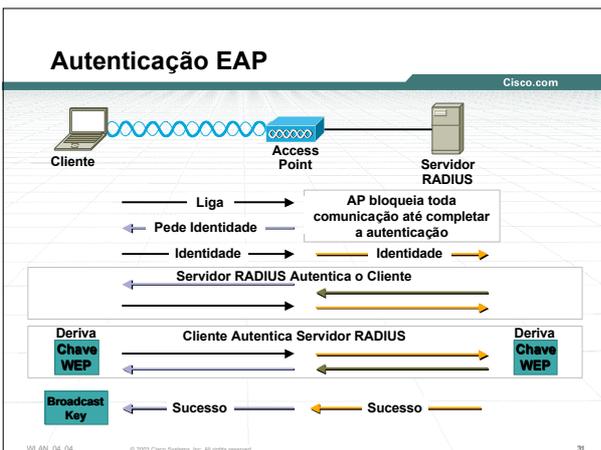


Segurança WLAN : Autenticação 802.1X

- 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")

Logos for Cisco Systems, RSA Security, and Microsoft are shown at the bottom right.

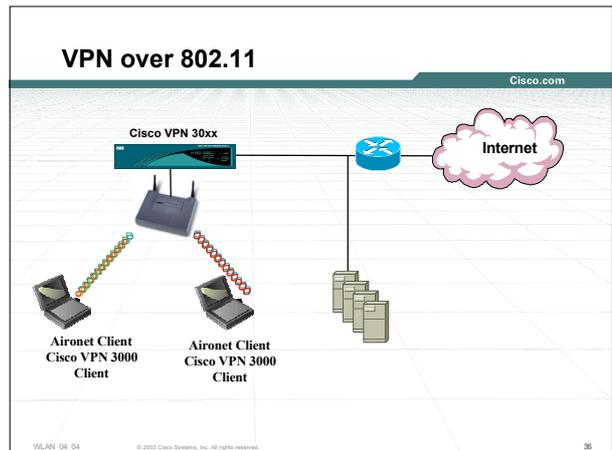
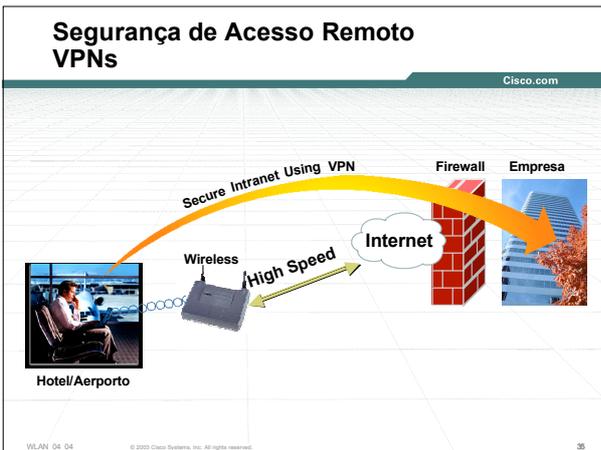
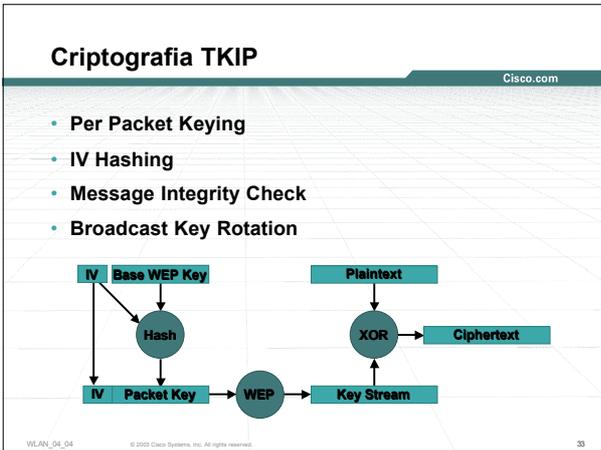
WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 30



Criptografia Forte

- 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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 32



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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 37

Diferenciação de Clientes com VLANs

Cisco.com

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

802.1Q rede cabeada com VLANs

AP Channel: 6
 •SSID "laptop" = VLAN 1
 •SSID "pda" = VLAN 2
 •SSID "phone" = VLAN 3

SSID: laptop
Segurança: PEAP + AES

SSID: pda
Segurança: LEAP + TKIP

SSID: phone
Segurança: LEAP + WEP

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 38

New Security Enhancements Mitigate Network Attacks

Cisco.com

Attack	Authentication: Open Encryption: Static WEP	Authentication: Cisco LEAP, EAP-TLS or PEAP	Authentication: Cisco LEAP, EAP-TLS or PEAP
Man-in-the-Middle	Protected from War Driving	Protected from Script Kiddies	Protected from Professionals
Authentication Forgery	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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 39

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

WLAN_04_04 © 2003 Cisco Systems, Inc. All rights reserved. 40

WLAN Security White Papers Cisco.com

Wireless LAN Security & the Cisco Wireless Security Suite

SAFE for Wireless
(recently updated Mar. '03)

SAFE:
Wireless LAN Security in Depth

Abstract

Since the release of the IEEE 802.11 standard in 1999, wireless LANs have become popular. Today, wireless LANs are widely deployed in offices and homes. After conference rooms, industrial facilities, border security, classrooms, and transit applications, IEEE 802.11 is used in a wide range of applications. However, the security of wireless LANs is still a concern. This paper provides a comprehensive review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite.

1. Introduction

Since the release of the IEEE 802.11 standard in 1999, wireless LANs have become popular. Today, wireless LANs are widely deployed in offices and homes. After conference rooms, industrial facilities, border security, classrooms, and transit applications, IEEE 802.11 is used in a wide range of applications. However, the security of wireless LANs is still a concern. This paper provides a comprehensive review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite.

2. IEEE 802.11 Security

IEEE 802.11 security is based on the IEEE 802.11 standard. The standard defines the security of wireless LANs. However, the security of wireless LANs is still a concern. This paper provides a comprehensive review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite.

3. Cisco Wireless Security Suite

The Cisco Wireless Security Suite provides a comprehensive review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite.

4. Conclusion

The Cisco Wireless Security Suite provides a comprehensive review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite.

5. References

1. IEEE 802.11 standard, IEEE Std. 802.11-2007, IEEE, 2007.

2. Cisco Wireless Security Suite, Cisco Systems, Inc., 2003.

3. Wireless LAN Security in Depth, Cisco Systems, Inc., 2003.

4. Wireless LAN Security in Depth, Cisco Systems, Inc., 2003.

5. Wireless LAN Security in Depth, Cisco Systems, Inc., 2003.

www.cisco.com/in/US/products/wireless/ps430/products_white_paper0186a0800b469f.shtml

www.cisco.com/application/pdf/m/ps/ps128/c654/cmigration_09186a08000c8b3.pdf

WLAN_01_04 © 2003 Cisco Systems, Inc. All rights reserved. 41

CISCO SYSTEMS



EMPOWERING THE INTERNET GENERATIONSM

ptomus_WLAN_01_02 © 2003, Cisco Systems, Inc. All rights reserved. Cisco Confidential 42