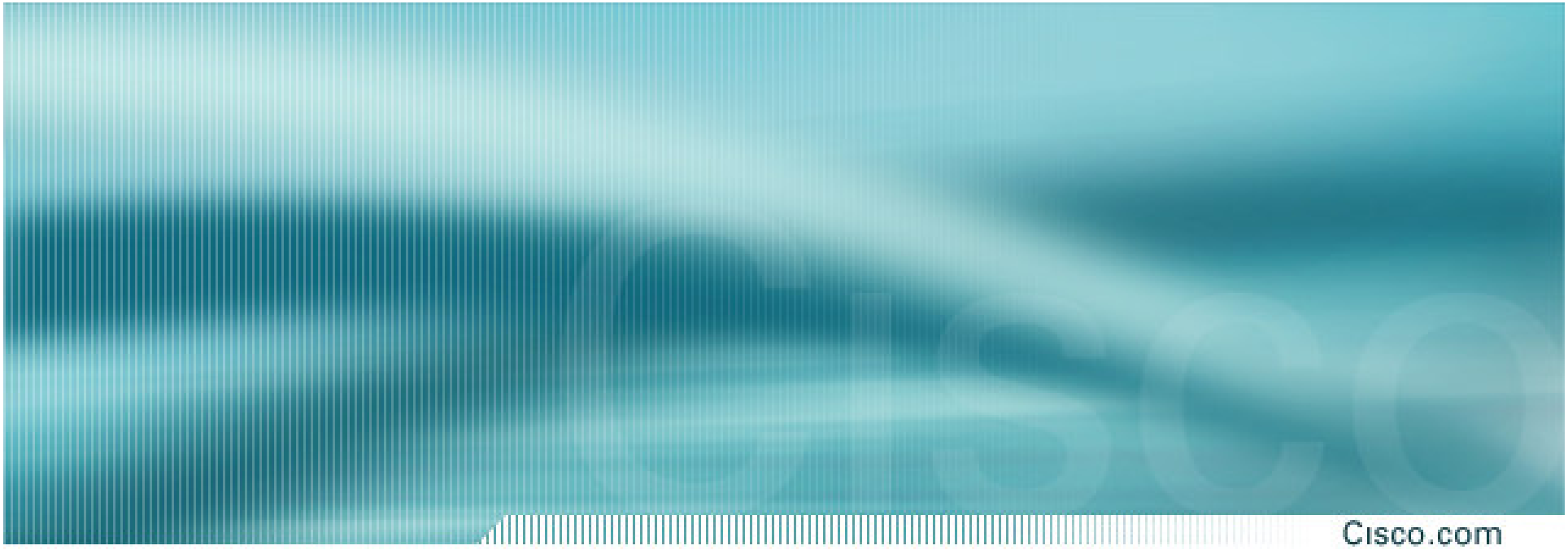


Cisco WLAN Technology and Standards Evolution

Mauricio Gaudencio
Business Developer Manager
Security / Wireless
mgaudenc@cisco.com

NOP Study—Wireless LANs Increase Productivity

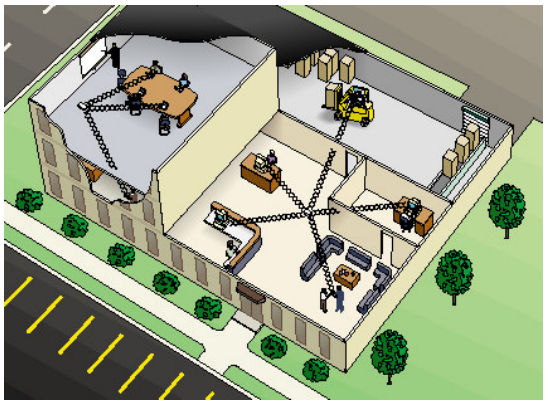
Based on a survey of 300+ U.S.-based organizations with more than 100 employees:

- **End users stayed connected an average of 1¾ hours more per day to their corporate network**
- **Average daily time savings: 70 minutes**
- **Productivity: +22%**

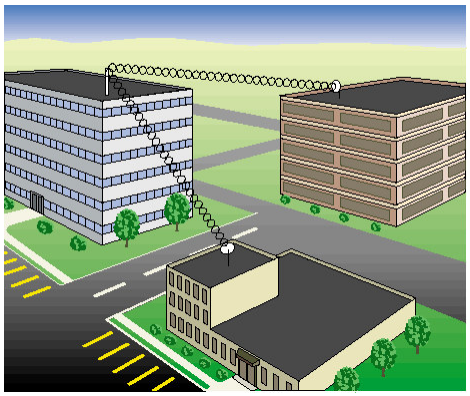
Source: NOP World-Technology, Sept. 2001

Extending the Network Through Wireless

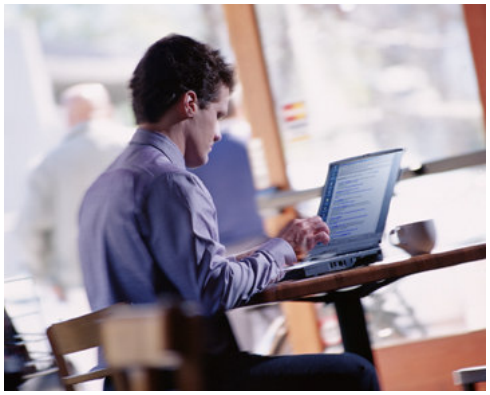
In-Building Wireless LANs



Wireless Bridges



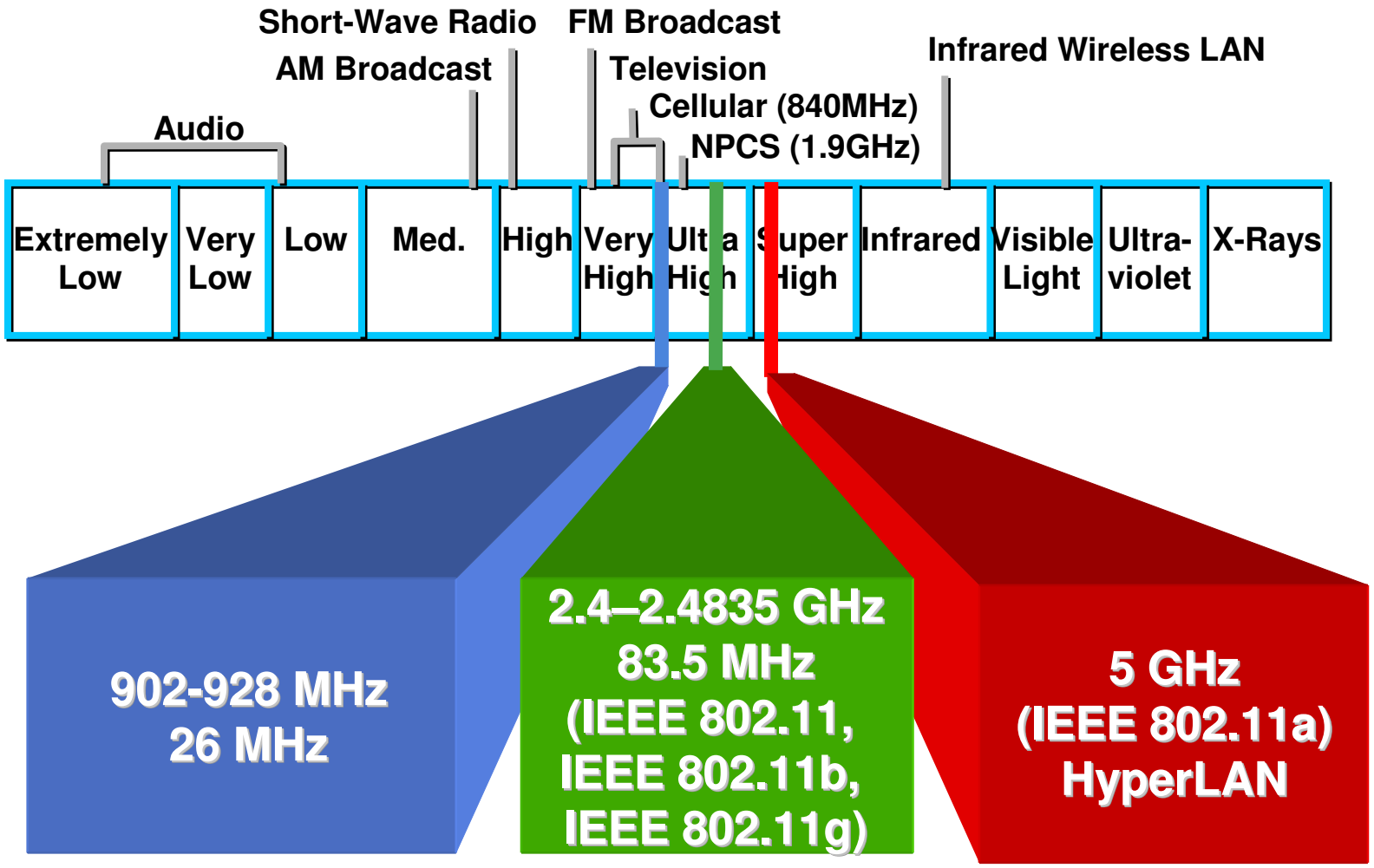
Public Access Hot Spots



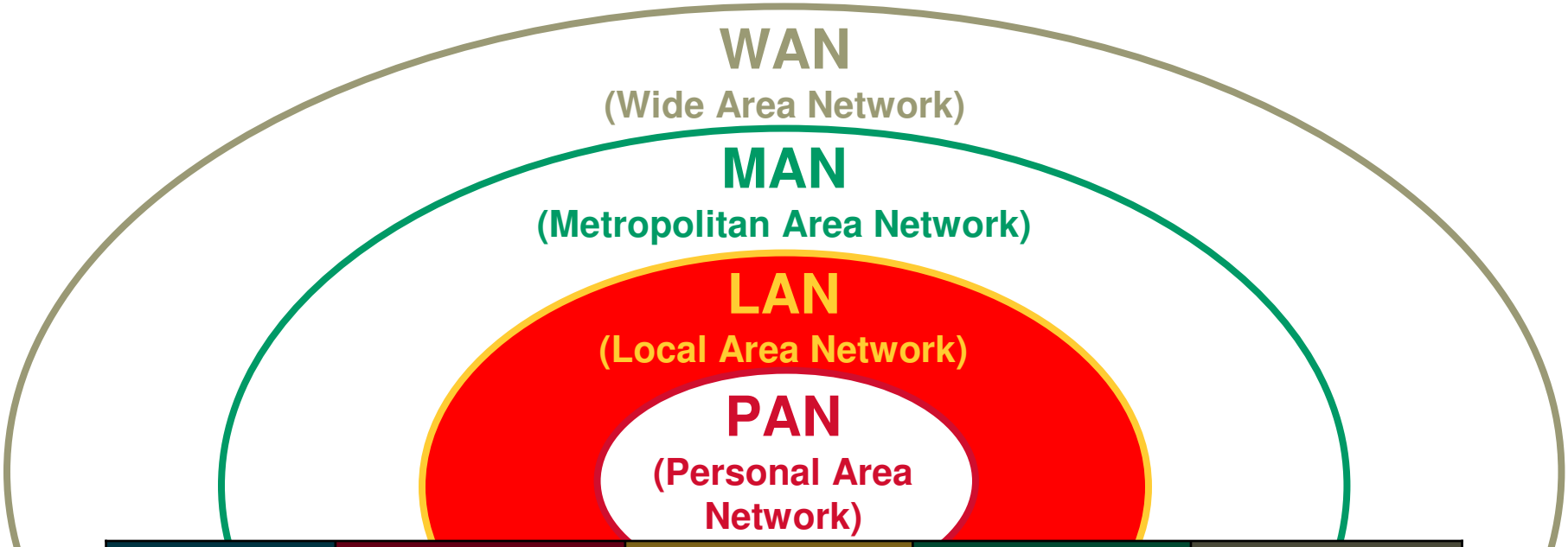
Home Networking

ISM Unlicensed Frequency Bands

Cisco.com

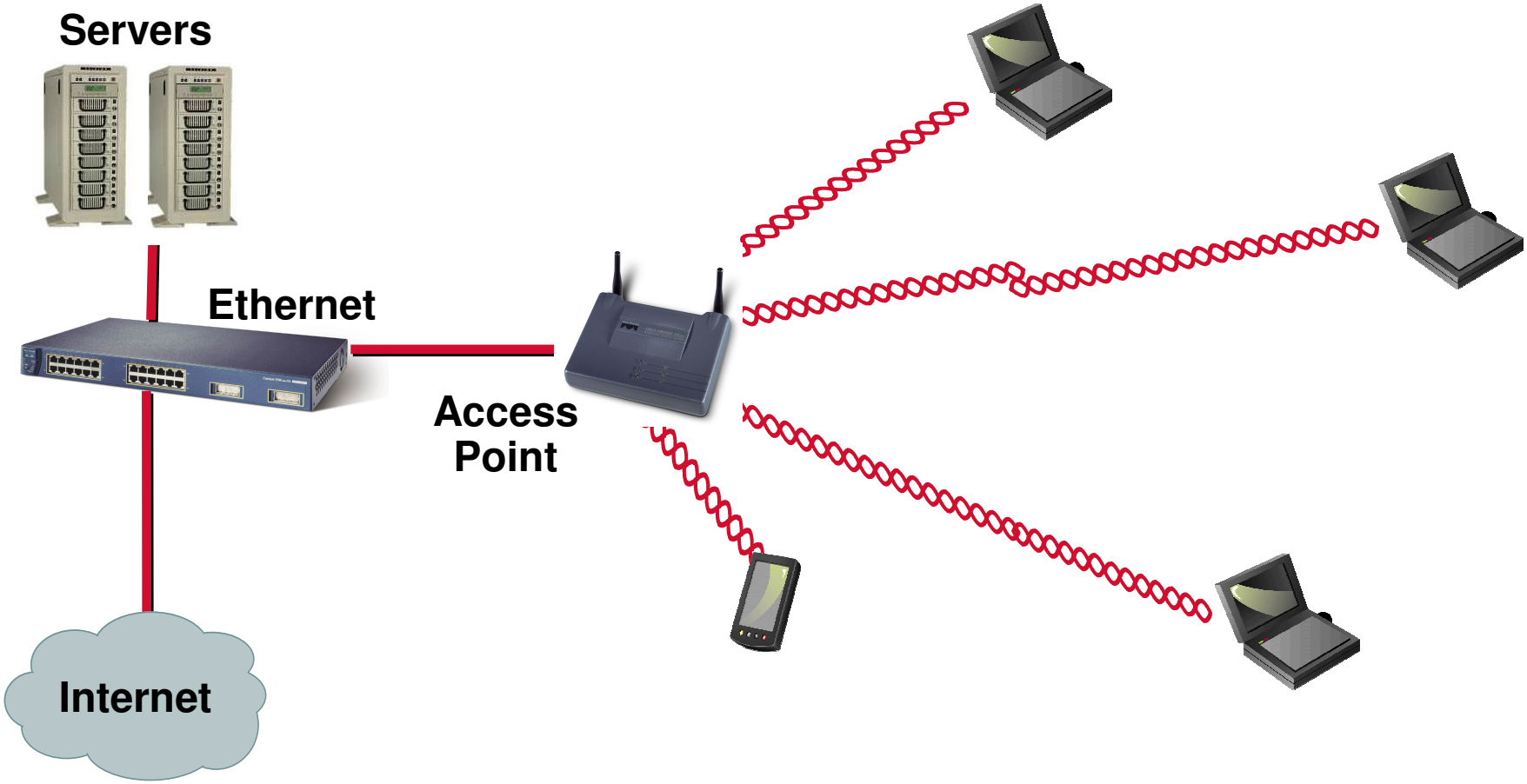


Wireless Technologies



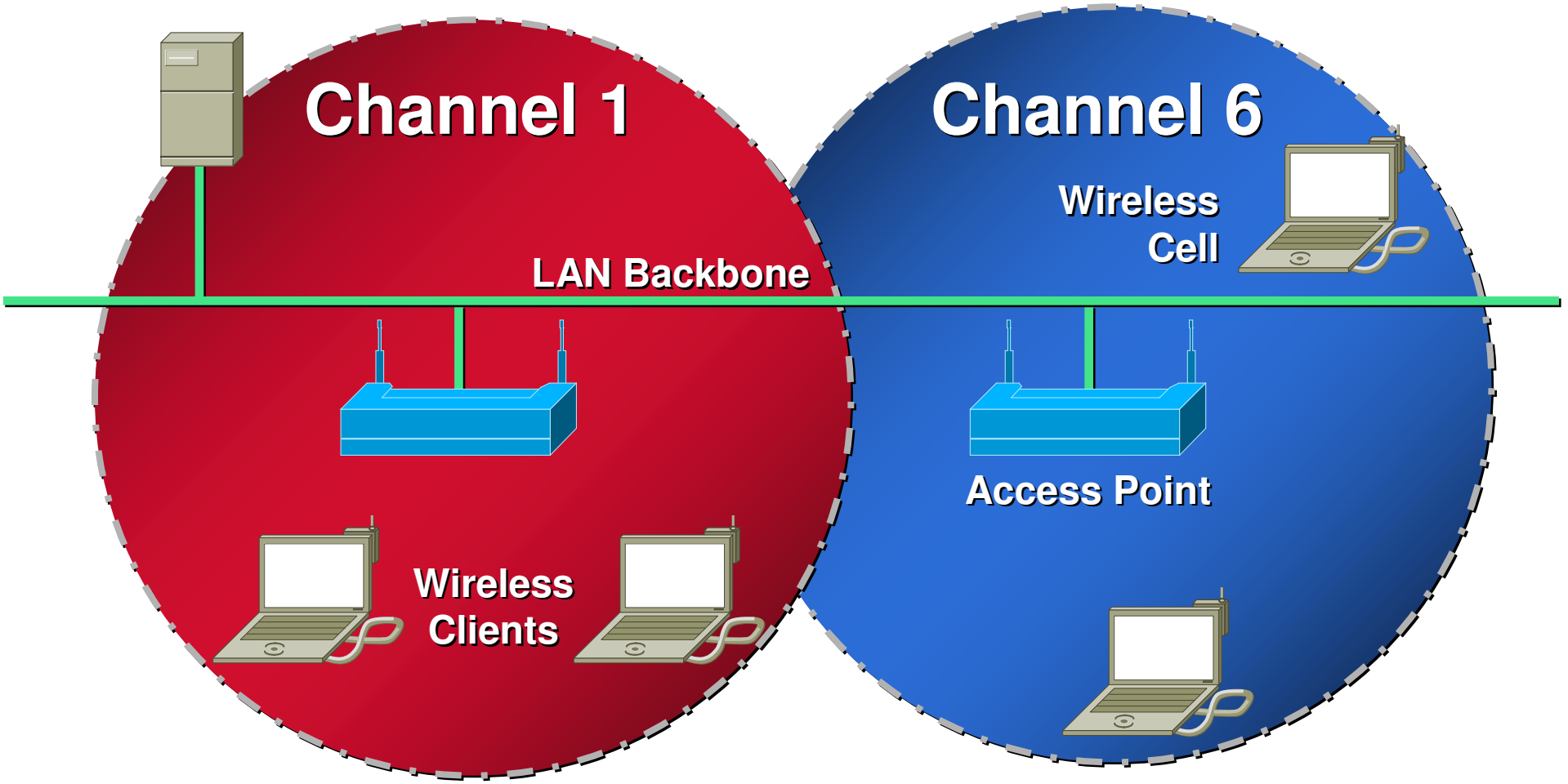
	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a,11b,11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Speed	< 1Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Pier-to-Pier Device-to-Device	Enterprise networks	Fixed, last mile access	PDAs, Mobile Phones, cellular access

Wireless Local Area Network (WLAN)

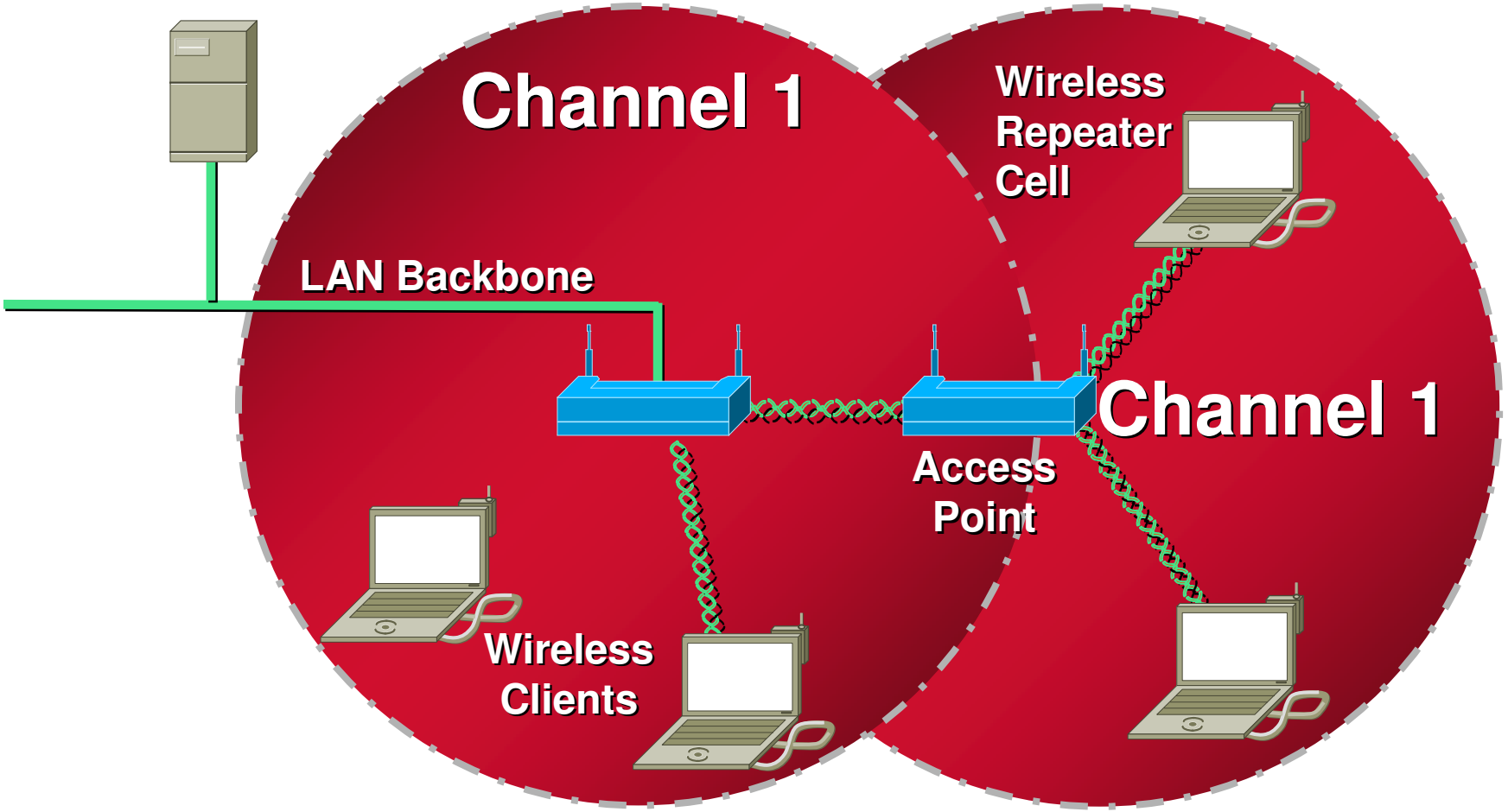


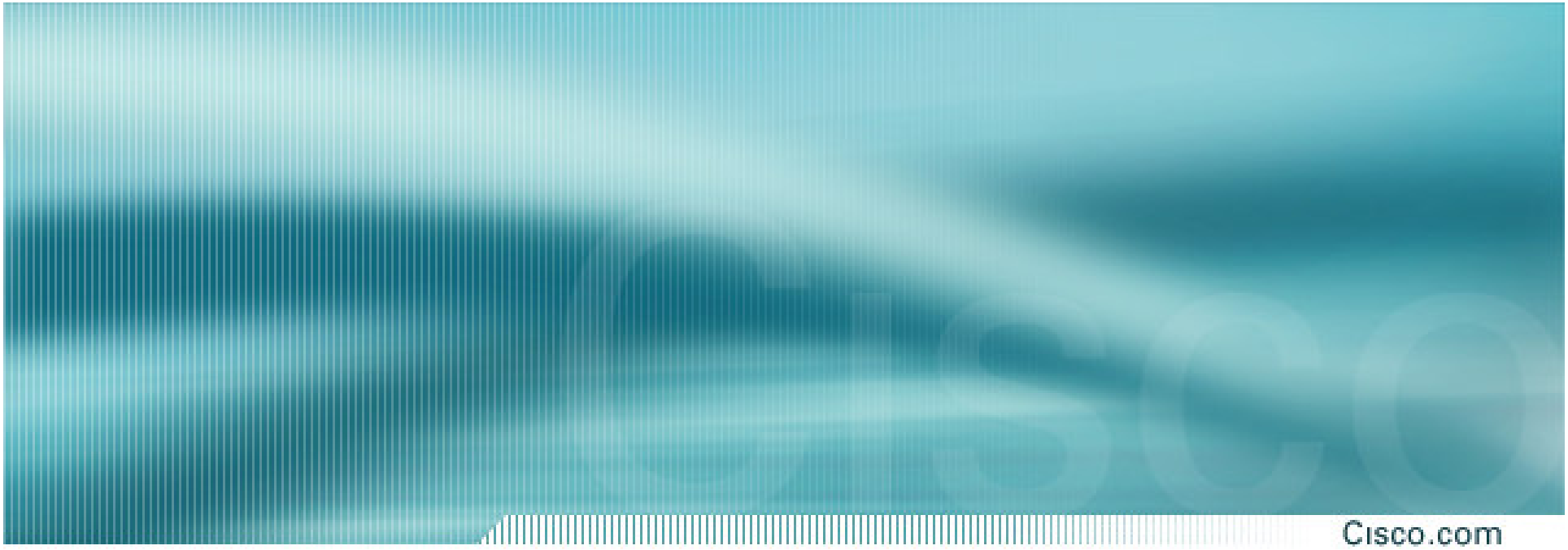
Typical Multicell Configuration

Cisco.com



Wireless Repeater





IEEE 802.11 Standards Update

Topics from A to X

IEEE 802.11 Standard Activities

- 802.11a—5GHz—Ratified in 1999
- 802.11b—11Mb 2.4GHz—ratified in 1999
- 802.11d—World Mode and additional regulatory domains—Ratified
- 802.11e—Quality of Service
- 802.11f —Inter-Access Point Protocol (IAPP)
- 802.11g—Higher Datarate (>20mBps) 2.4GHz
- 802.11h—Dynamic Frequency Selection and Transmit Power Control mechanisms
- 802.11i—Authentication and security

WLAN Standards Bodies

Primary Role →	*Develop Spec*	*Interoperability Testing*
Standard	**IEEE**	**Wi-Fi Alliance**
• 2.4 GHz, 11 Mbps	802.11b	802.11b
• 5 GHz, 54 Mbps	802.11a	802.11a
• Security	802.11i	WPA, WPA2(future)
• 2.4 GHz, 54 Mbps	802.11g	802.11g
• QoS	802.11e	Future
• 5 GHz Europe	802.11h+d	Future

802.11a

Cisco.com

- Ratified as Standard in Sept, 1999
- Provides similar technology to HylerLAN2
- Data rates to 54Mb defined
- Provides 8 indoor WLAN channel
- Regulation differ extensively across countries

802.11b
11Mb 2.4GHz Direct Sequence

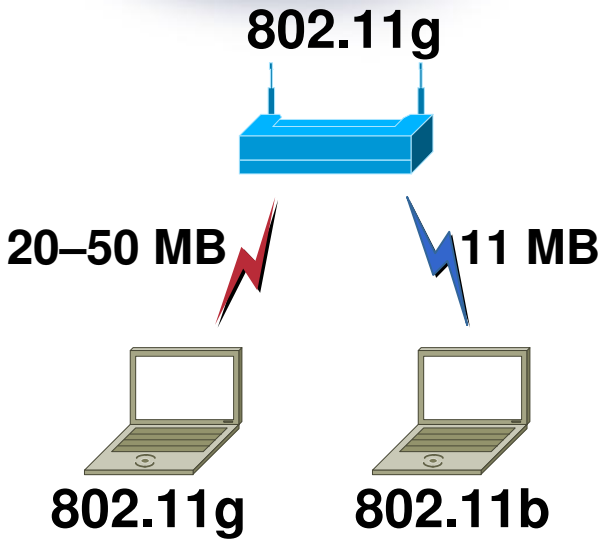
Cisco.com

- Ratified as Standard in Sept, 1999
- 11Mb 2.4Gz
- 11 US channels
- 13 ETSI channels
- 14 Japan Channels
- Power levels of 36dBm EIRP-FCC
  20dBm EIRP-ETSI
- Virtually approved for world wide use
- Modulation CCK (11Mb) and BPSK/QPSK (1 and 2Mb – 802.11)

IEEE802.11g

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

- Provides **higher data rates** @ 2.4 GHz
- **Similar speeds** as 802.11a
- **Similar distance** as 802.11b
- **Backward compatible** with 11 Mbps (802.11b)
- Same modulation as 802.11a—**OFDM**



802.11 Capacity Compared

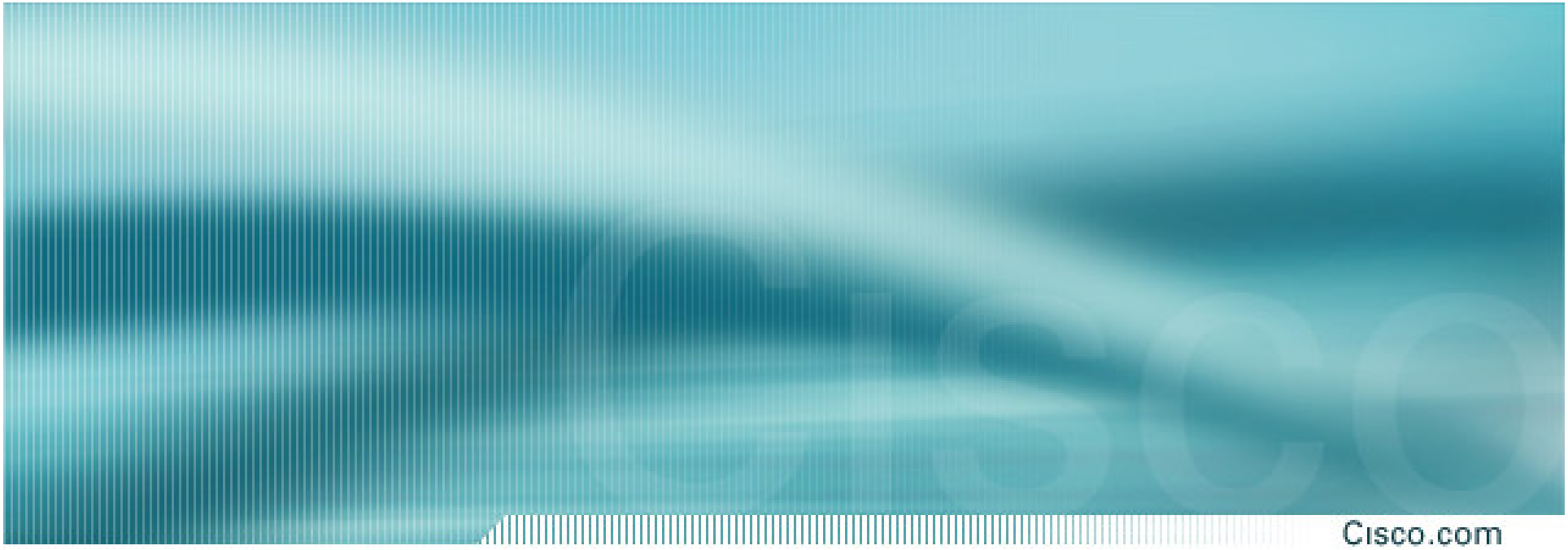
	Throughput (Mbps)	Channels	Capacity (Mbps)
802.11b	6	3	18
802.11g (Mixed Mode Operation)	8	3	24
802.11g (No Legacy Support)	22	3	66
802.11a	25	12	300
802.11a (with 802.11h Support)	25	24	600

- Even when not supporting 802.11b clients, 802.11g still provides a fraction of the network capacity provided by 802.11a
- Dual band infrastructure is the only way to achieve a high capacity wireless LAN

Deployment Considerations

Cisco.com

- **No reason not to begin migration to 802.11g**
  - –No additional cost, no 802.11b performance degradation
  - –New site survey not a necessity, most installed antennas supported
  - –Increased throughput, enhanced security, better 802.11b range
- **Dual-band 802.11a/g clients are the near term standard**
  - –Silicon Vendors, PC OEMs moving towards high-capacity clients
  - –Neither 802.11a nor 802.11g likely to exist as stand-alone client adapters for mainstream devices
- **Customers can start planning for a dual-band infrastructure**
  - –Cisco Aironet 1200 Series Access Point supports dual radios at time of purchase or as a field upgrade
  - –802.11a infrastructure capabilities can be added in as user count, client 802.11a capabilities and capacity requirements increase



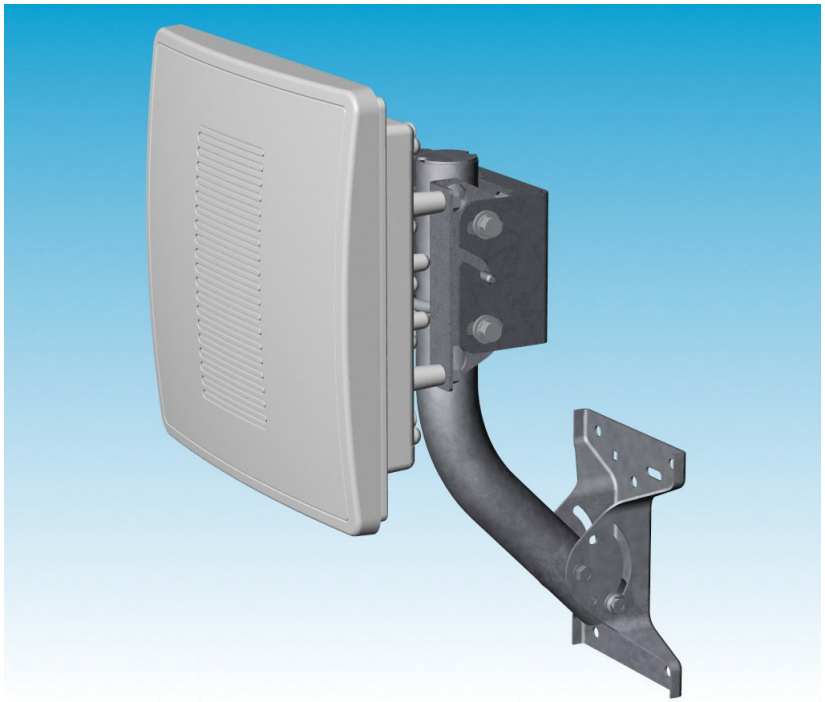
Wireless Bridges

Wireless Bridging – what and why?

- **What?**
  - **–Wireless line of sight infrastructure technology for connecting multiple networks in a metro area**
- **Why?**
  - **–Flexible, rapidly deployable, cost effective alternative to leased lines**

BR1410 Wireless Metro Bridge

- 5.8 GHz UNII-3 band
- 802.11a – 54 Mbps data rate
- Point-to-Point & Point-to-MultiPoint
- >5 mile range @ 54 Mbps P2P
  - –High throughput even at long ranges
- Outdoor weather-proof enclosure
  - –Designed for roof mount, tower mount, and mast mount
- 2 versions:
  - 1)With integrated 23 dBi patch antenna
  - 2)With connectors for remote antennas:
    - •9 dBi omni
    - •9.5 dBi sector
    - •28 dBi dish



High Performance

- Outdoor deployable radio maximizes performance by minimizing cable loss
- Data rates: 6 to 54 Mbps with industry leading receiver sensitivity
- Point to point range with integrated 22.5 dBi gain antennas:
  - –7.5 miles (12Km) at 54 Mbps
  - –16 miles (25Km) at 9 Mbps
- Point to point range with 28 dBi dish antennas:
  - –12 miles (20Km) at 54 Mbps
  - –23 miles (37Km) at 9 Mbps
- Point to multi-point range with 9 dBi omni hub antenna and 22.5 dBi gain antenna:
  - –2 miles (3Km) at 54 Mbps
  - –8 miles (13Km) at 9 Mbps
- VoIP circuits trunked – up to 24 over PtP links
- Excess processor and memory capacity for future SW/FW upgrades yielding higher throughputs and more VoIP circuits.

Agenda

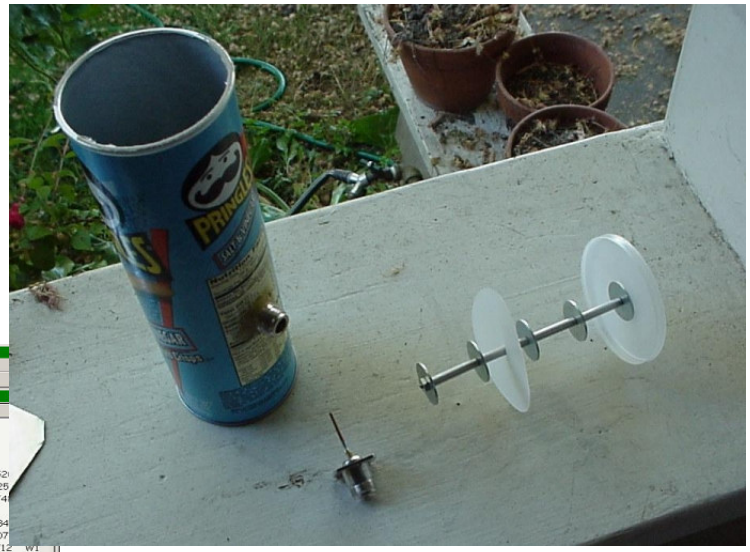
Cisco.com

- **WLAN Security**

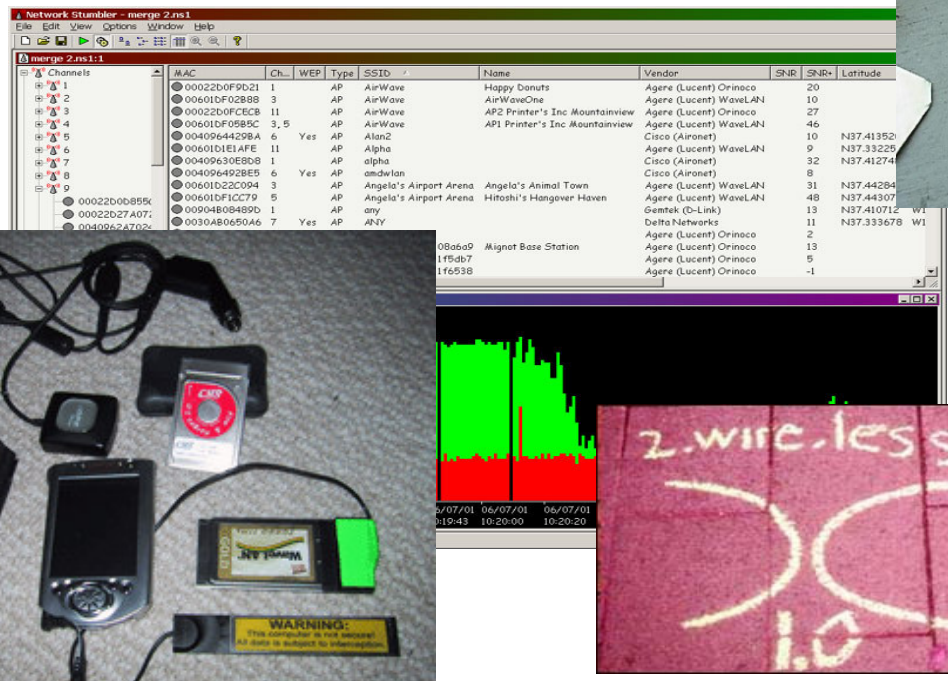
Pringles

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

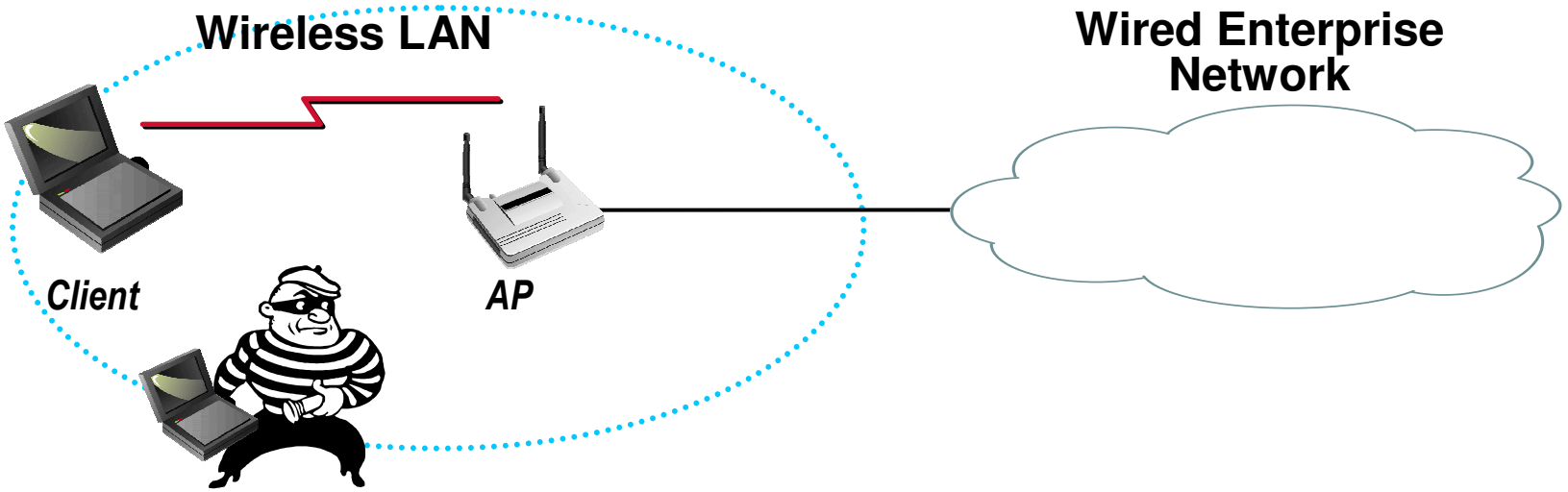
Fonte: Info Exame Junho/2002



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



WLAN Security



Issue

- Privacy - Wireless sniffer can view all WLAN data packets
- Authentication - Anyone in AP coverage area can get on WLAN and network

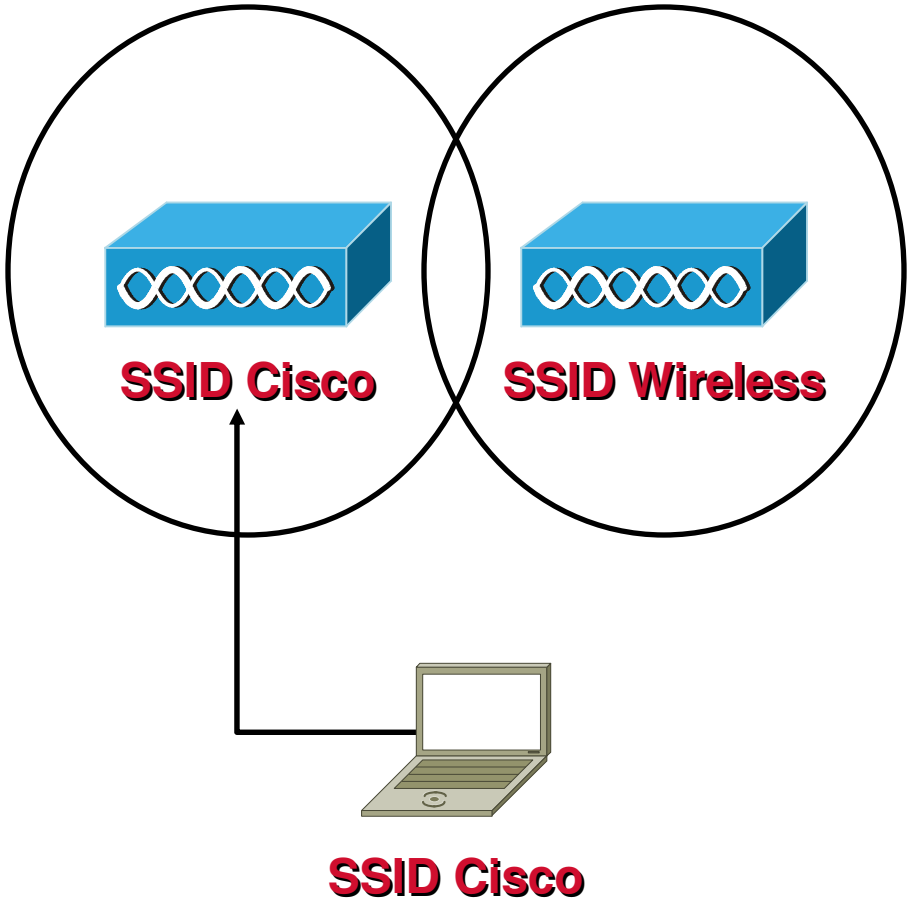
Possible Solutions

0. None
1. Static WEP (only 40 bit key required by WECA)
2. Dynamic WEP (LEAP / EAP-TLS)
3. VPN

Goal: Make WLAN security equivalent to wired LANs (WEP - Wired Equivalent Privacy)

The Service Set Identifier (SSID)

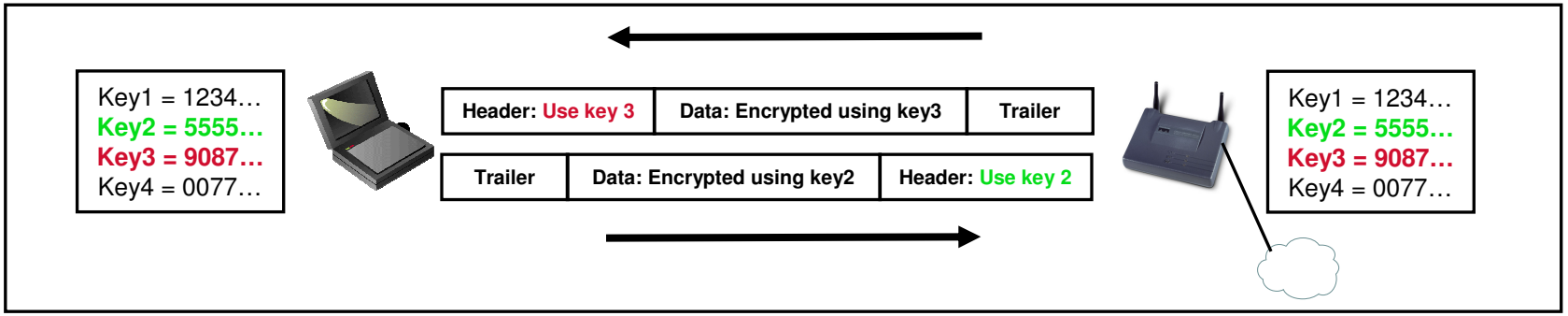
- Used to logically separate wireless LANs
- SSID is not a security mechanism!
- Disabling SSID broadcast in the beacons does not prevent an attacker from seeing them



MAC Authentication

- **MAC-based Authentication**
  - –Use with caution only when clients do not support VPNs or EAP
  - –Cisco supports centralized configuration and management of permitted MAC addresses in RADIUS database
  - –Can be easily spoofed
- **MAC Authentication is weak**
  - –MAC addresses are sent in the clear
  - –MAC addresses can be sniffed and spoofed

Static Wired Equivalent Privacy (WEP)
Enable Communication with Network



- **Knowledge of the WEP key is required in order to communicate on the WLAN**
- **Key needs to be changed frequently**
  - **–WEP encryption can be attacked**
  - **–If there is 1 laptop lost then every WEP key in the network has to change**
  - **–Keys need to change periodically to maintain security of authentication and privacy**
- **Key distribution and management problematic**
  - **–There is no method to "push" WEP keys to clients**
  - **–Impossible to scale securely**

Stream Ciphers (Cont.)

- To encrypt, XOR key stream with plain text
  - –Key stream ⊗ Plain Text => Cipher Text
- To decrypt, XOR key stream with cipher text
  - –Key Stream ⊗ Cipher Text => Plain Text

"WIRELESS" = 58495245C455353

Key Stream = 123456789ABCDEF XOR

4A7D043D6FBE9C

Key Streal = 123456789ABCDEF XOR

"WIRELESS" = 58495245C455353

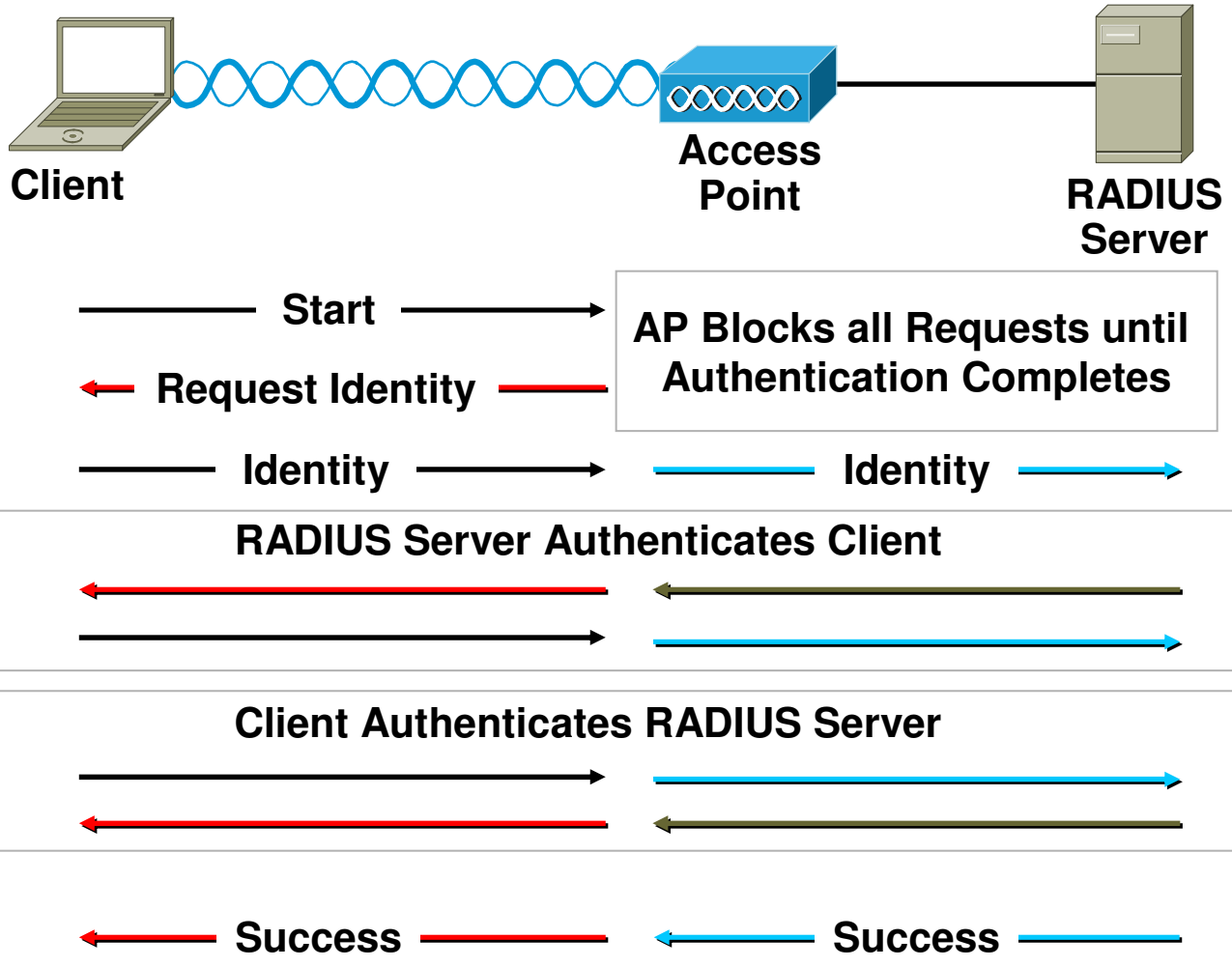
802.11 Security Summary

- The security mechanisms in the 1997 802.11 specification are flawed
  - –Open authentication
  - –Shared Key authentication
  - –WEP
- These will NOT secure your wireless LAN!!

802.1X for 802.11

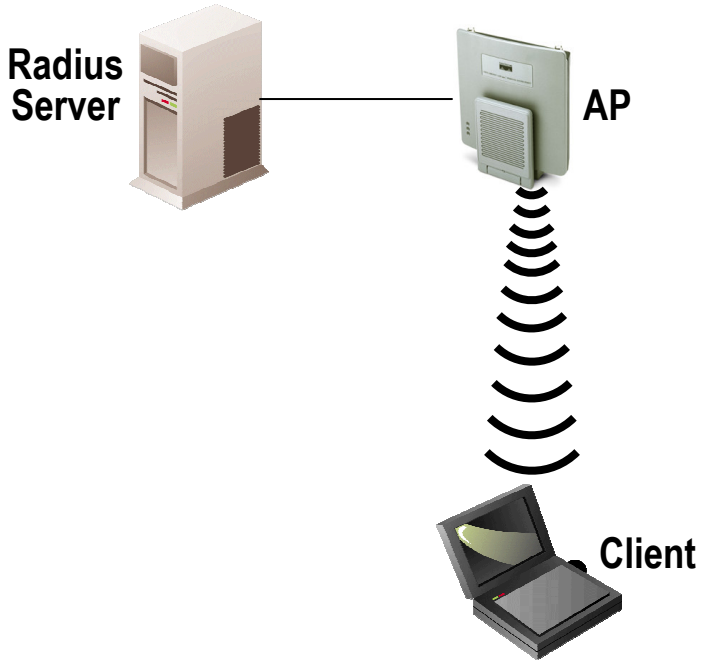
- Layer 2 link layer support for Extensible Authentication Protocol (EAP)
- Framework to facilitate authentication between client, AP, and AAA server
- Extensible authentication algorithms
  - –Password-based
  - –PKI-based
  - –Biometrics
  - –More to come…

802.1X Authentication Process



WLAN Security: 802.1X Authentication

- **Mutual Authentication**
- **LEAP**
  - –"Lightweight" EAP
  - –Nearly all major OS's supported:
    - •WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS
- **EAP-TLS**
  - –EAP-Transport Layer Security
  - –Mutual Authentication implementation
- **PEAP**
  - –"Protected" EAP
  - –Establishes secure tunnel (similar to VPN)
  - –Supported by Cisco, Microsoft, & RSA
  - –Option: One-Time Passwords ("OTP")



EAP-Cisco Authentication (LEAP)

- **Client Support**
  - –Windows 95-XP
  - –Windows CE
  - –Macintosh OS 9.X and 10.X
  - –Linux
- **Device Support**
  - – WGB 340 e 350
  - – BR350 series
  - –APs (340, 350, 1100, 1200)
- **RADIUS Server**
  - –Cisco ACS

Broadening Support for LEAP

Cisco has licensed LEAP to many companies:

- **LEAP support: RADIUS servers**
  - –**Funk Software:** Steel-Belted Radius Server
  - –**Interlink:** Secure.XS Radius Server
- **LEAP support: Client Devices**
  - –**Apple:** Powerbooks/iBooks
  - –**HP:** Print Servers
  - –**Symbol:** Handhelds
  - –**Intermec:** Handhelds
- **LEAP support: Client Software**
  - –**Funk Software:** Odyssey Client v.1.1
  - –**Meetinghouse:** Aegis Client v.1.3.6
- **LEAP support: Chipsets**
  - –**Intel** **TI**
  - –**Intersil** **Marvell**
  - –**Atheros** **Agere**
  - –**Atmel** **Broadcom**

EAP-TLS Authentication

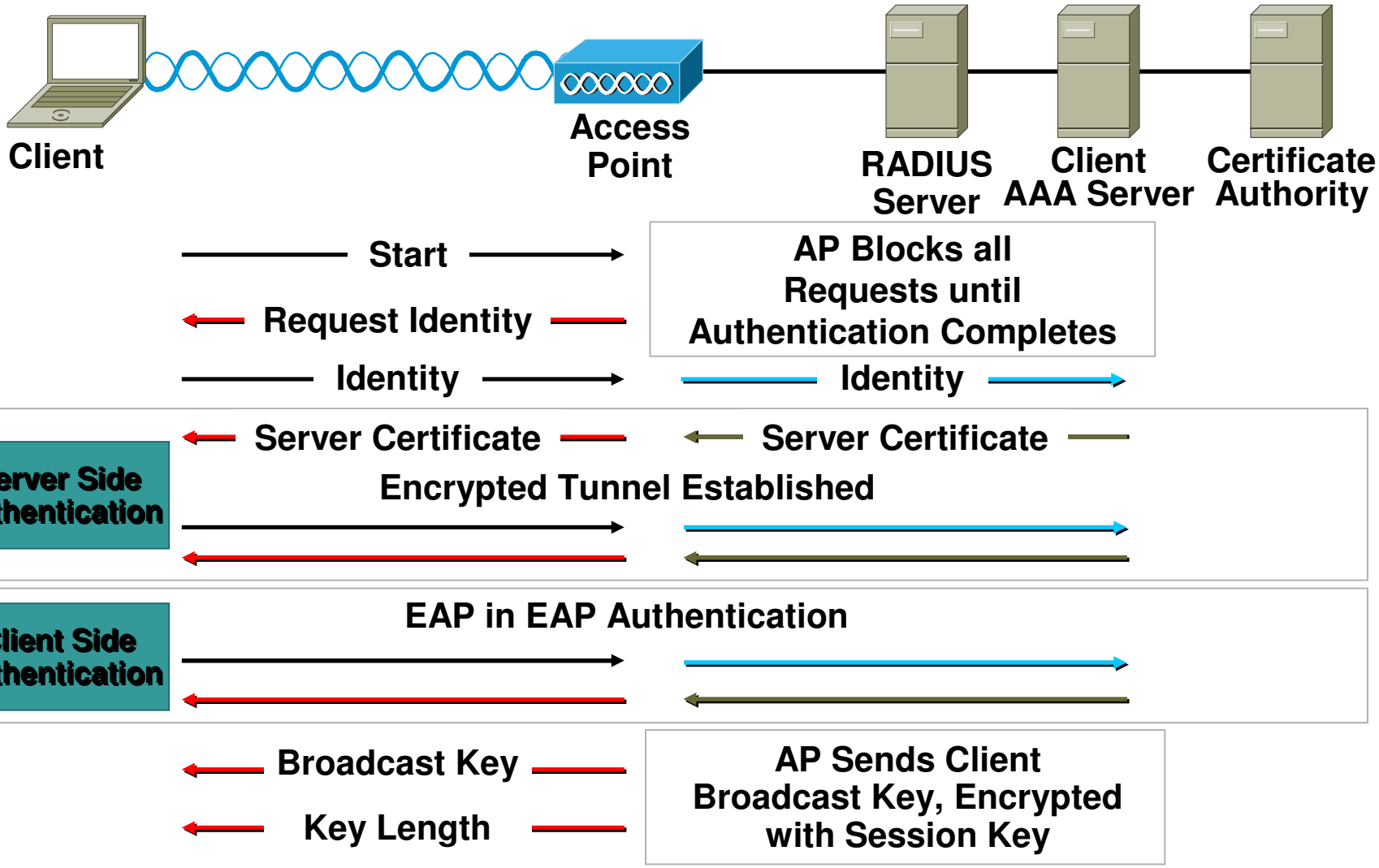
- **Client Support**
  - –Windows 2000, XP
  - –Clients require a local user or machine certificate
- **Infrastructure Requirements**
  - –EAP-TLS supported RADIUS server
    - •Cisco ACS, Cisco AR, MS IAS
    - •RADIUS server requires a server certificate
  - –Certificate Authority Server
    - •Windows 2000 Server

Hybrid Authentication

- **EAP-PEAP**
  - –Server side authentication with TLS
  - –Client side authentication with EAP authentication types (EAP-GTC, EAP-MD5, etc)
- **Require CA, as with EAP-TLS**
- **Clients do not require certificates**
  - –Simplifies end user/device management
- **Allows for one way authentication types to be used**
  - –One Time Passwords
  - –Proxy to LDAP, Unix, NT/AD, Kerberos, etc

EAP-PEAP Authentication

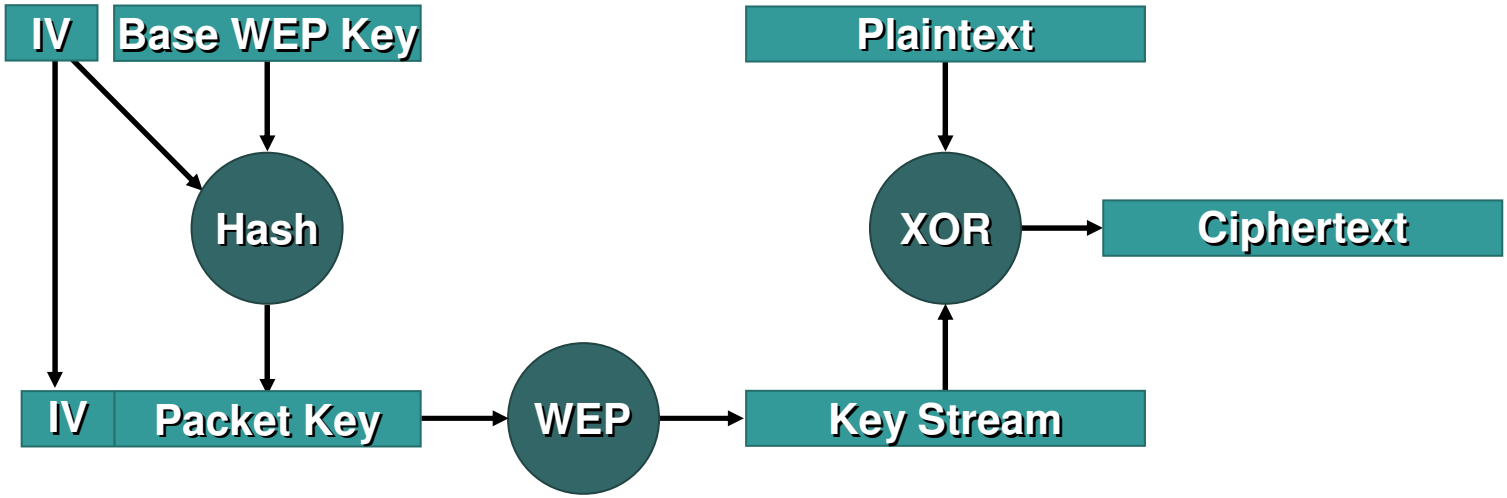
Cisco.com



Strong Encryption

- **Temporal Key Integrity Protocol (TKIP)**
  - –Enhances WEP encryption
  - –Per Packet Keying
  - –Message Integrity Check
- **AES**
  - –Advanced Encryption Standard
  - –The Gold Standard
  - –Hardware encryption vs. software encryption
- **VPN over Wireless**
  - –3DES encryption—Tried and true
  - –HMAC-SHA1 or HMAC-MD5 message authentication

Temporal Key Integrity Protocol (TKIP)
Per Packet Keying Operation



- IV Sequencing—IVs increment by one
- Per Packet IV is hashed with base WEP key
- Result is a new ‘Packet’ WEP key
- The Packet WEP key changes per IV

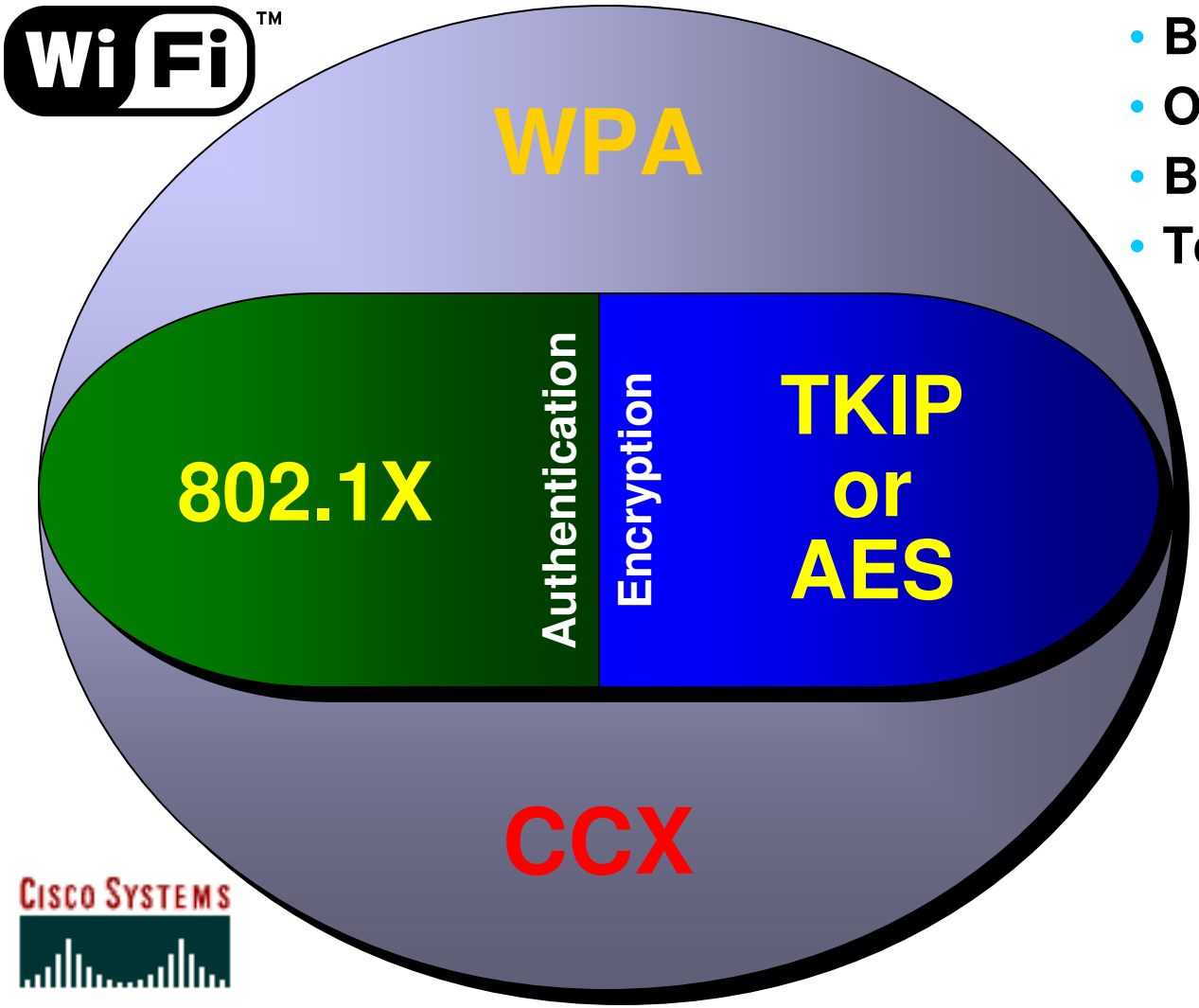
AES Encryption

- **Advanced Encryption Standard**
  - –3DES successor
  - –Sponsored by NIST
- **Rijndael Algorithm**
  - –Block Cipher
  - –128,192, and 256 bit key support
- **Optional in WPA**
  - –Probably required in future versions
- **Most probably requires Hardware upgrade**
  - –Available with Cisco 802.11g family

Broadcast Key Rotation

- Broadcast key is required in 802.1X environments
- Broadcast key is vulnerable to same attacks as static WEP key
- Broadcast key needs to rotate, as with unicast key

Enterprise-Class WLAN Security: The Cisco Wireless Security Suite



- **Built on Standards**
- **Optimized for Enterprise**
- **Broad Adoption**
- **Tested for Interoperability**

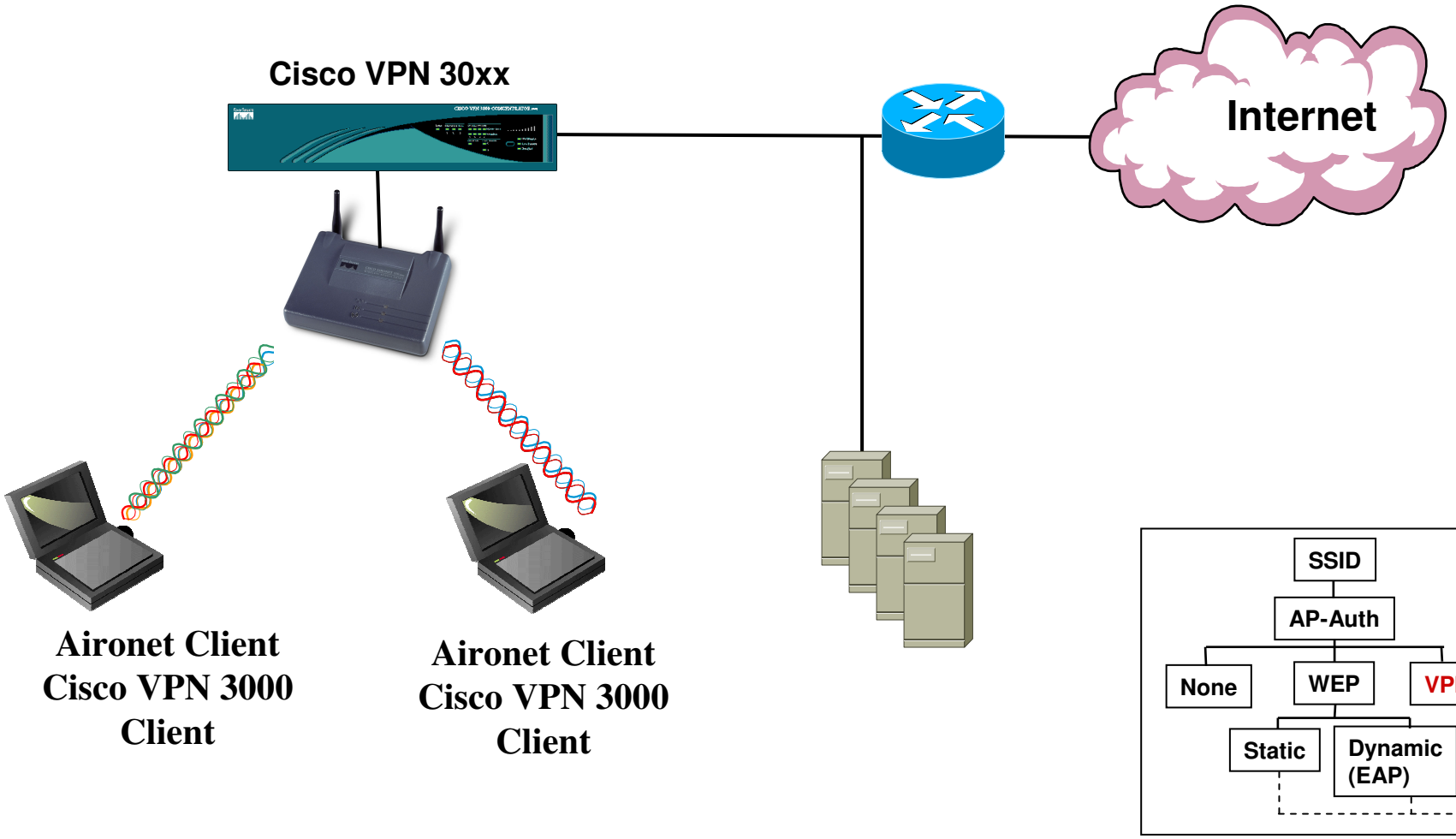
WPA
Wi-Fi Protected Access

TKIP
Temporal Key Integrity Protocol

AES
Advanced Encryption Standard

CCX
Cisco Compatible eXtensions

Remote Access Wireless VPN



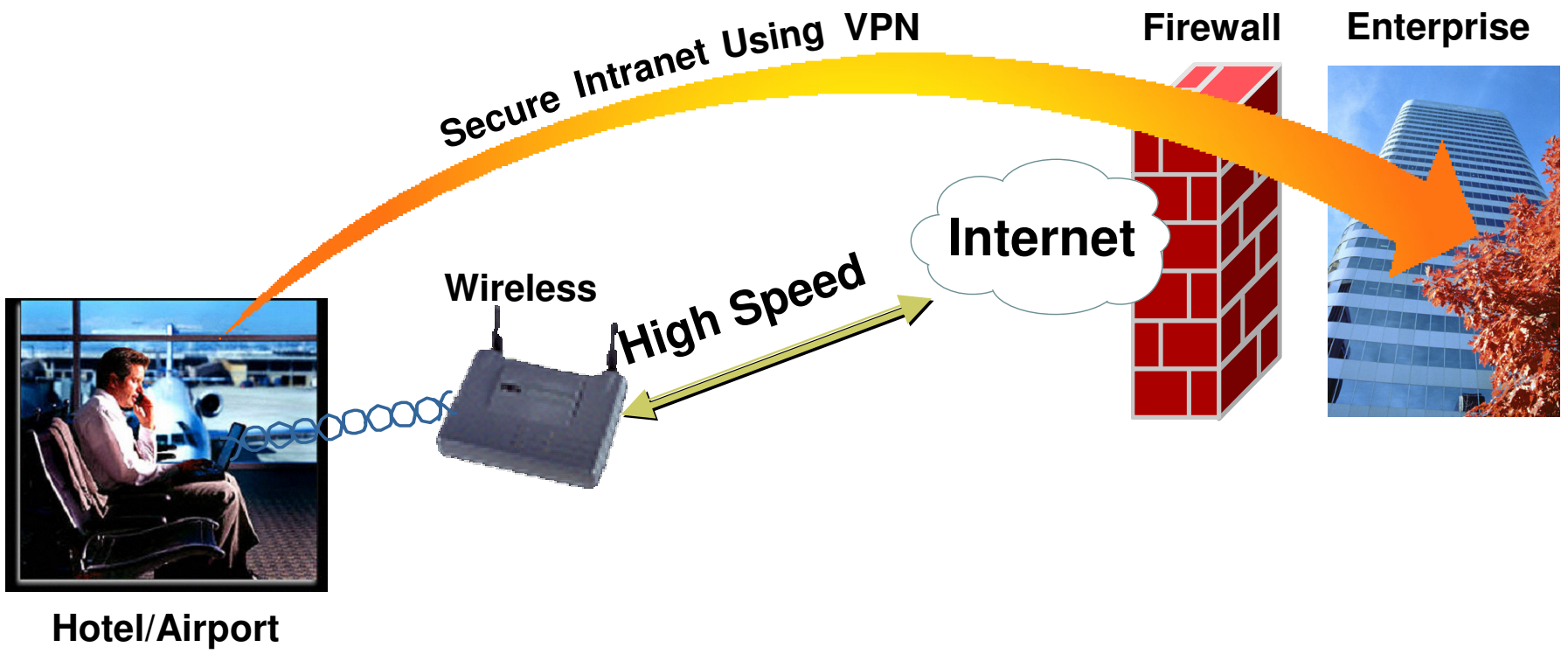
VPN over 802.11—Issues

Cisco.com

- Average of 30% to 40% performance impact
- Client throughput may require multiple concentrators
- Support for IP unicast exclusively
  - –No support for IPX, AppleTalk
  - –No support for multicast
- 802.11e QoS enhancements useless for VPN WLAN clients
  - –All traffic is IP/ESP encapsulated

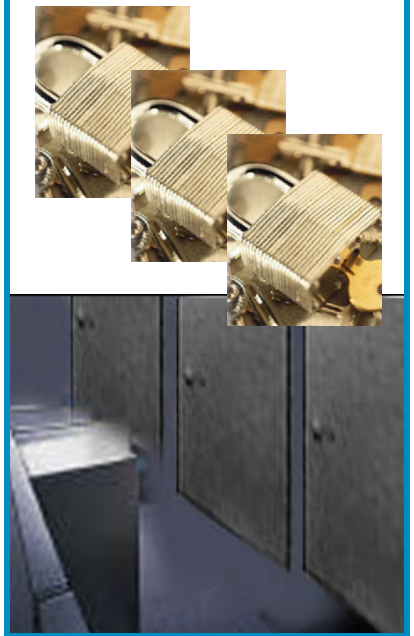
Remote Access Security Using VPN

Cisco.com



First Generation WLAN Security : Not appropriate for Enterprise Deployment

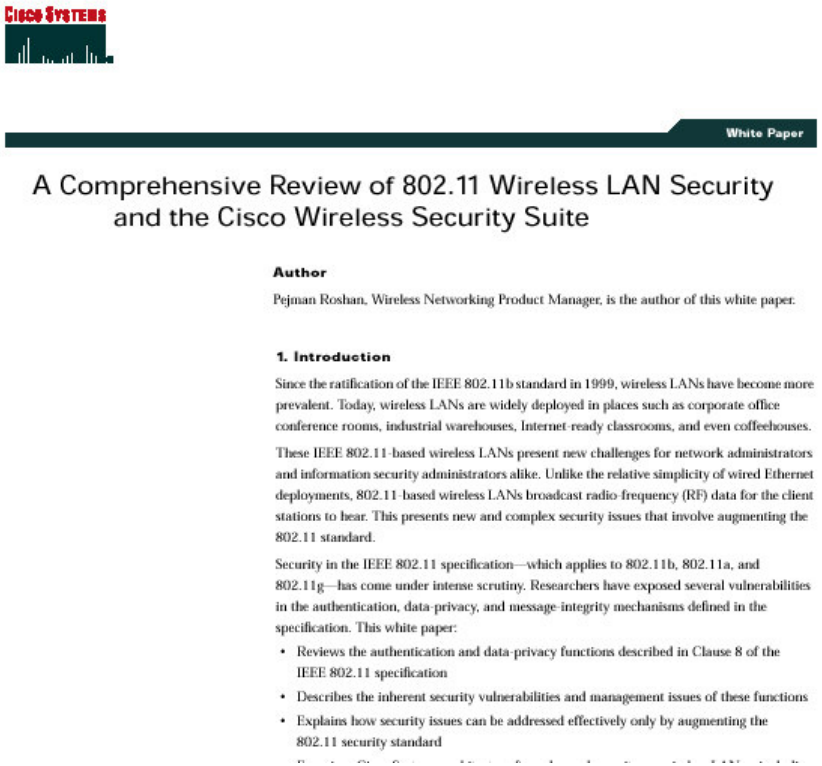
Cisco.com

No Security	Basic Security	Enhanced Security	VPN Security
No WEP and Broadcast Mode	Wi-Fi 40-bit, 128-bit Static WEP	Dynamic Key Management System, Mutual Authentication, and 802.1x via EAP	End-to-end security using VPN
			
Public Access	Telecommuter and Small Business	Mid-Market and Enterprise	Special Apps./ Business Traveler

WLAN Security White Papers

Cisco.com

Wireless LAN Security & the Cisco Wireless Security Suite



Cisco Systems

White Paper

A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite

Author

Pejman Roshan, Wireless Networking Product Manager, is the author of this white paper.

1. Introduction

Since the ratification of the IEEE 802.11b standard in 1999, wireless LANs have become more prevalent. Today, wireless LANs are widely deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses.

These IEEE 802.11-based wireless LANs present new challenges for network administrators and information security administrators alike. Unlike the relative simplicity of wired Ethernet deployments, 802.11-based wireless LANs broadcast radio-frequency (RF) data for the client stations to hear. This presents new and complex security issues that involve augmenting the 802.11 standard.

Security in the IEEE 802.11 specification—which applies to 802.11b, 802.11a, and 802.11g—has come under intense scrutiny. Researchers have exposed several vulnerabilities in the authentication, data-privacy, and message-integrity mechanisms defined in the specification. This white paper:

- Reviews the authentication and data-privacy functions described in Clause 8 of the IEEE 802.11 specification
- Describes the inherent security vulnerabilities and management issues of these functions
- Explains how security issues can be addressed effectively only by augmenting the 802.11 security standard

www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml

SAFE for Wireless

(recently updated Mar.'03)

Cisco Systems

White Paper

SAFE:
Wireless LAN Security in Depth

Authors

Sean Convery (CCIE #4232) and Darrin Miller (CCIE #6447) are the primary authors of this white paper. Mark Doering, Pej Roshan, and Sri Sundaralingam provided significant contributions to this paper and are the lead architects of Cisco's reference implementation in San Jose, CA USA. All are network architects focusing on wireless LAN, VPN, or security issues.

Abstract

This paper provides best-practice information to interested parties for designing and implementing wireless LAN (WLAN) security in networks utilizing elements of the SAFE blueprints. All SAFE white papers are available at the SAFE Web site: http://www.cisco.com/go/safe. These documents were written to provide best-practice information on network security and virtual-private-network (VPN) designs. Although you can read this document without having read either of the two primary security design documents, it is recommended that you read either "SAFE Enterprise" or "SAFE Small, Midsize and Remote-User Networks" before continuing. This paper frames the WLAN implementation within the context of the overall security design. SAFE represents a system-based approach to security and VPN design. This type of approach focuses on overall design goals and translates those goals into specific configurations and topologies. In the context of wireless, Cisco recommends that you also consider network design elements such as mobility and QoS when deciding on an overall WLAN design. SAFE is based on Cisco products and those of its partners.

This document begins with an overview of the architecture, and then details the specific designs under consideration. Because this document revolves around two principal design variations, these designs are

www.cisco.com/application/pdf/en/us/guest/netsol/ns128/c654/ccmigration_09186a008009c8b3.pdf