BENELUX FORUM 2005

Empowering Teachers and the Strength of Their Connections

Cisco Systems

Cisco Systems

Cisco On Cisco

WiFi Wireless Networks an addiction

Harm Klaassen
Hklaasse@cisco.com
Systems Engineer Education
netherlands

Agenda

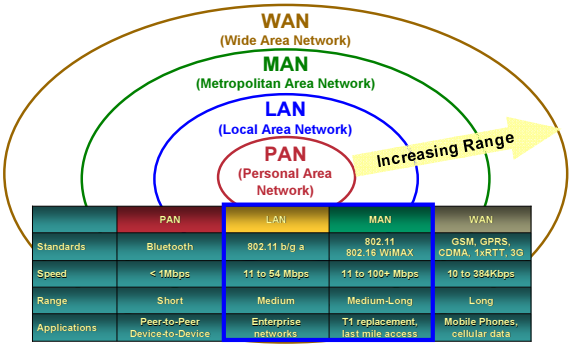
Empowering Teachers and the Strength of Their Connections

Cisco.com

- Wireless standards and trends.
- Wireless security.
- Structured Wireless-Aware Network SWAN.
- Summary.

Wireless Technologies

Cisco.com



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11 b/g a	802.11 802.16 WiMAX	GSM, GPRS, CDMA, 1xRTT, 3G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	Mobile Phones, cellular data

Momentum is Building in Wireless LANs

Cisco.com

- Wireless LANs are an "addictive" technology
- Strong commitment to Wireless LANs by technology heavy-weights
  - –Cisco, IBM, HP, Intel, Microsoft, Dell
- Embedded market is growing
  - –Laptop PC's with "wireless inside"
  - –Also PDA's, phones, printers, etc.
- The WLAN market is expanding from Industry-Specific Applications, to broad-based applications in Universities, Homes, & Offices

Evolution of the WLAN Business

WLAN Industry Has Been Around For Over 15 Years

Cisco.com

Early Adopters

Specific Industries
Hotels Hospitals
Retail Manufacturing

Education
Universities/Libraries

Mainstream

Home

Office WLANs

Outdoor Wireless Bridging

Next Wave

Public Access "Hotspots"
Airports Restaurants
Hotels Coffee Shops
Entire Towns Convention Centers

New Applications
Voice over WLAN
Buses, Sports Events, Construction Sites
Public Safety (Police, Ambulances)

WLAN Standards Activities (The "Alphabet Soup")

Wi Fi™

Cisco.com

Standard	Develop Spec IEEE	Interoperability Testing Wi-Fi Alliance
5 GHz, 54 Mbps	802.11a	802.11a
2.4 GHz, 11 Mbps	802.11b	802.11b
Multiple regulatory domains	802.11d	
Quality of Service (QoS)	802.11e	WME
Inter-Access Point Protocol	802.11f	
2.4 GHz, 54 Mbps	802.11g	802.11g
DFS & TPC	802.11h	
Security	802.11i	WPA, WPA2
Japan 5 GHz Channels	802.11j	
Measurement	802.11k	
Maintenance	802.11m	
High-Speed	802.11n	

The 802.11g Standard

Cisco.com

- 802.11g standard ratified by IEEE in June '03
  - Wi-Fi 802.11g interoperability testing began July '03
  - Worldwide usage
- Operates in the same 2.4 GHz band as 802.11b
  - Uses the same three non-overlapping channels
- Full backward compatibility with 802.11b
  - Investment protection
  - Conceptually similar to Ethernet vs. Fast Ethernet
  - .11g throughput is reduced in "mixed cells" with both .11b & .11g clients due to backward compatibility constraints; however, with the recently implemented "RTS-to-Self" default on the AP, mixed cell throughput has been improved.
- Uses OFDM for 802.11g data rates, CCK for 802.11b
  - OFDM: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps
  - CCK: 11, 5.5, 2 & 1 Mbps

802.11a/b/g Comparison: Throughput

Cisco.com

	Data Rate (Mbps)	Throughput (Mbps)	Throughput as a % of 802.11b Throughput
802.11b	11	6	100%
802.11g (with .11b clients in cell)	54	14	233%
802.11g (no .11b clients in cell)	54	22	367%
802.11a	54	25	417%

802.11g throughput is reduced in "mixed cells" with both .11b & .11g clients due to backward compatibility constraints; however, with the recently implemented "RTS-to-Self" default on the AP, mixed cell throughput has been improved.

Wireless LAN Technology Spreading Throughout Cisco Product Line

Cisco.com

- Access Points, Client Cards, Outdoor Bridges and Antennas
- Switches – Catalyst 6500 Services modules.
- Management – CiscoWorks WLSE
- Security – ACS, Access Registrar
- Mobile Access – MAR3200 Mobile Router
- Voice – 7920, Soft-phone Clients
- Public Access – SIM-authentication
- Secure Guest Access – BBSM and SSG
- Home – Linksys

Debate: 2.4 GHz 802.11g vs. 5 GHz 802.11a

Cisco.com

Q: Which is better?

A: Both!

- Home Environment ⟶ .11g
- Business Environment ⟶ .11a/b/g

- Silicon Vendors focusing on .11a/b/g chipsets
- *"Dual-Band .11a/b/g is the Future"*
  - –Gartner Group
  - –META Group

802.11a & g Deployment Considerations

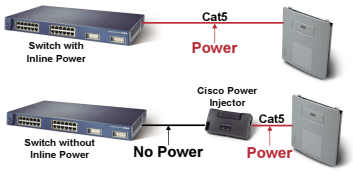
Cisco.com

- No reason not to begin migration to 802.11g
  - For Cisco, .11g APs same cost as .11b, 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 becoming mainstream
  - .11a/g chipsets are now commonplace from the leading silicon vendors
- 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 AP radios can be added in response to increases in number of users, WLAN traffic, and % of clients that are 802.11a-capable

All Cisco AP's Have In-Line Power to Reduce Installation Costs

Cisco.com

- In-Line Power on 1100, & 1200 Series AP's
- 48 Volt DC power supplied over Cat 5 cable
- Eliminates cost of installing AC power
- AP1100/AP1200 offer choice of in-line power or separate AC power
- Catalyst inline-powered switches support device discovery mode



Ethernet In-line Power Sources:
- Cisco Aironet Power Injectors
- Catalyst 3560-24PWR Switch
- Catalyst 4500 and 6500 Series Switches
- Cisco 2600, 3600/3700 and the News ISR 2800, 3800,
- Inline Powered EtherSwitch Modules
- 48 Port Power Patch Panel

1300 Series 802.11g Outdoor AP & Wireless Bridge

Cisco.com

- 54 Mbps max. data rate, 28 Mbps throughput
- Outdoor weather-proof housing
- 2 versions:
  - With integrated 13 dBi patch antenna
  - With connectors for remote antenna
- Cisco IOS Software
- Same WLAN security capabilities as AP1200
- Can operate as an "outdoor AP" or wireless bridge
- Point-to-Point & Point-to-Multipoint configurations
- Full line of of 2.4 GHz antennas supported:
  - 9 dBi patch
  - 5.2 dBi omnidirectional
  - 13.5 dBi Yagi
  - 21 dBi dish
  - 13 dBi patch (integrated)
  - 12 dBi omnidirectional
  - 14 dBi sector

1300 Series Outdoor AP/Bridge with integrated 13 dBi patch antenna

Agenda

Empowering Teachers and the Strength of Their Connections

Cisco.com

- Wireless standards and trends.
- Wireless security.
- Structured Wireless-Aware Network SWAN.
- Summary.

Wireless LAN Security: Vulnerabilities & Lessons

Cisco.com

Vulnerabilities:

Hackers


THE WALL STREET JOURNAL.

Hackers Can Penetrate Wireless Network

Employees

"War Driving"

Lessons:
- Don't rely on basic WEP encryption; Always use strong passwords
- Security must be turned on (part of the installation process)
- Employees will install WLAN equipment on their own (compromises security of your entire network)

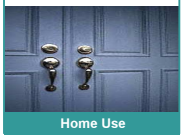
WLAN Security Hierarchy

Cisco.com

Open Access
No Encryption, Basic Authentication

Public "Hotspots"

Basic Security
40-bit or 128-bit Static WEP Encryption



Home Use

Enhanced Security
802.1X, 802.11i TKIP/WPA Encryption, Mutual Authentication, Scalable Key Mgmt., etc.

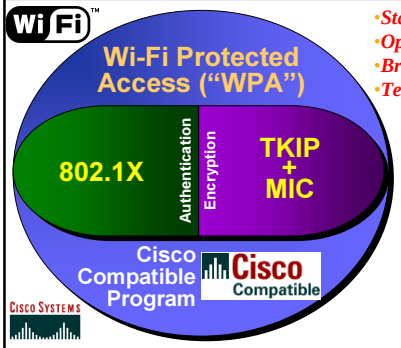
Business

Remote Access
Virtual Private Network (VPN)

Business Traveler, Telecommuter

Enterprise-Class WLAN Security

Cisco.com



- *Standardized*
- *Optimized for Enterprise*
- *Broad Adoption*
- *Tested for Interoperability*

Wi-Fi Protected Access:
- Mandates TKIP Encryption + MIC + 802.1X Authentication
- Required as of Aug.'03

Encryption: TKIP + MIC
- Temporal Key Integrity Protocol
- Message Integrity Check
- Successor to WEP encryption

Cisco Compatible Program:
- Cisco Compatible eXtensions
- Ensures interoperability for a variety of 802.1X authentication types, including LEAP & PEAP

WLAN Encryption: 3 Choices

Cisco.com

- **WEP** ("Wired Equivalent Privacy")
  - Original standard for WLAN encryption
  - A determined hacker can break static WEP keys
  - OK for home use; Not adequate for business use

802.11i Standard:
- Ratified June '04
- 2 Encryption Modes Supported:
  - TKIP + MIC
  - AES

- **802.11i/WPA: TKIP Encryption with Message Integrity Check**
  - Cisco's pre-standard TKIP (a.k.a. "CKIP") began shipping Dec.'01
  - All Cisco Aironet WLAN products (except BR350 & WGB352) now support 802.11i-standard TKIP (part of WPA standard)
  - WPA ("Wi-Fi Protected Access") delivers enterprise-class security consistent with 802.11i spec
  - WPA is mandatory for all new Wi-Fi products introduced since Aug.'03
- **802.11i/WPA2: AES Encryption**
  - AES is the "Gold Standard" of encryption
  - WPA2 standard will include both TKIP & AES (per 802.11i spec)
  - WPA2 interoperability testing begins Fall '04; won't be mandatory until Spring 2006
  - Cisco will implement AES in hardware, not software, to ensure good security and good performance
  - Cisco's 802.11g radios, and 2nd-generation 802.11a radios, will support AES (Cisco's 802.11b radios will not support AES)

WLAN Encryption: How To Decide What To Use?

Cisco.com

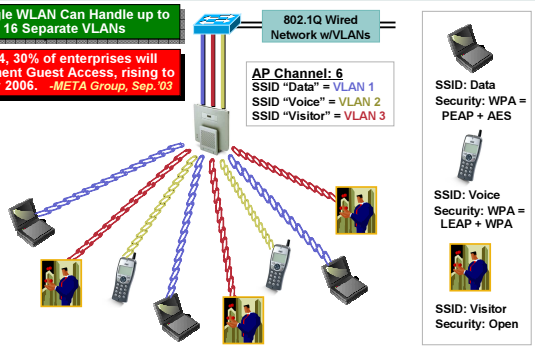
- **Devices**
  - Most WLAN devices can support WPA/TKIP
  - At present, AES is not widely supported (but this will evolve over the next few years as more new devices are shipped that can support AES)
- **Applications**
  - AES is appropriate for some critical apps (healthcare, financial, national security)
  - For most mainstream office apps, WPA/TKIP is more than sufficient (WPA/TKIP has never been broken)
- **Interoperability**
  - Between WPA testing and Cisco Compatible testing, a large number of devices have been tested for WPA/TKIP interoperability
  - AES/WPA2 interoperability testing will begin Fall '04, but existing products in the market do not need to go through this testing
- **VLANs**
  - You can "mix & match" security on your WLAN by using VLANs
  - VLAN-1: For devices that can handle AES, and applications that require AES
  - VLAN-2: For all other devices that can handle WPA/TKIP
  - VLAN-3: For application-specific or legacy devices that only support WEP
    (WEP is insecure and puts the network at risk)

VLANs: For Security, Voice, Guest Access, etc.

Cisco.com

A Single WLAN Can Handle up to 16 Separate VLANs

By 2004, 30% of enterprises will implement Guest Access, rising to 50% by 2006. *-META Group, Sep.'03*



WLAN Security: Best Practices

Cisco.com

- Mutual Authentication is vital for WLANs
- Use VPNs for remote access
- Strong Passwords are your best defense against dictionary attacks
  - Prompt users to select new passwords every 3-6 months
  - Characteristics of a Strong Password:
    - At least 10 characters long
    - Use both upper & lower case letters
    - Use 1 or more symbols (! @ # $)
    - Password should not contain real words (in any language)
- Create a WLAN Policy for your organization
  - Employees should not install rogue AP's at work
  - Remind users to enable security on their home AP's (even basic WEP is better than nothing)
- For further information, check out Cisco WLAN White Papers at www.cisco.com/go/aironet/security

Agenda

Empowering Teachers and the Strength of Their Connections

Cisco.com

- Wireless standards and trends.
- Wireless security.
- Structured Wireless-Aware Network SWAN.
- Summary.

Cisco's Wireless LAN Strategy

Cisco.com

Benefits of Integrating Wired and Wireless

- Seamless management of wired and wireless
- Synergy with wired functions
- Future proof your technology investment
- Performance and Scalability
- Functionality

. . . Driving to Minimize TCO

Cisco SWAN: Integrated Wired/Wireless Framework

Cisco.com

Provides:

Security
AND
Scalability
AND
Ease of Deployment
AND
Network Management
AND
Low Operating Costs
AND
Voice + Data
AND
Mobility

ALL AT THE SAME TIME!
NO TRADEOFFS!

Cisco Structured Wireless-Aware Network Key Benefits

Cisco.com

- **Scalable WLAN Management**
  - Managing 50/100 AP up to 2500 APs is as easy as managing a few APs
  - Easily update software on all APs
- **Enhances Security**
  - WLAN IDS: Rogue AP Detection, Location and Suppression
  - WLAN IDS: AP Scan Only Mode
  - Fast Secure Layer 3 Roaming
  - WAN Link Survivability with Local Authentication Service
  - Security Policy Monitoring
- **Simplified WLAN Deployment & Operations**
  - Assisted Site Surveys
  - Interference Detection and Mitigation
- **Effective Troubleshooting and Diagnostic Tools**
  - Self-healing WLANs
  - Proactive performance and fault monitoring

Extends the security and reliability of the wired LAN to the wireless LAN

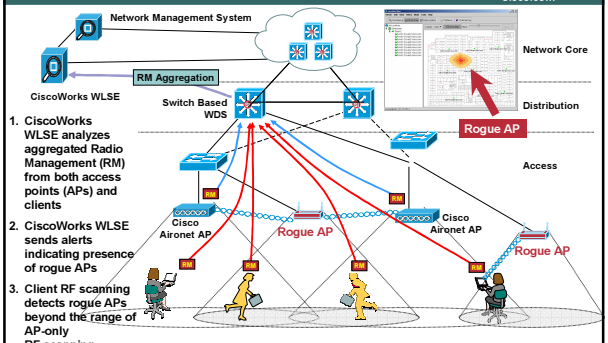
CiscoWorks WLSE 2.11 or Express

Cisco.com

- **Radio Management Enhancements:**
  - Self Healing WLANs
  - Automated Re-Site Survey
  - XML API for Radio Management
  - .11a and .11g Radio Management support
  - Rogue AP Suppression through switch port shut-down
- **Support for 802.11g and 802.11a/g Access Points**
- **CiscoWorks WLSE Express up to 100 AP the SMB and Secundary/ Primairy school solution**
- **Real-time reports for troubleshooting**
- **WDS based client tracking to look up associated AP**

Cisco SWAN - Rogue Access Point Detection
Access Point and Client-Assisted RF Scanning

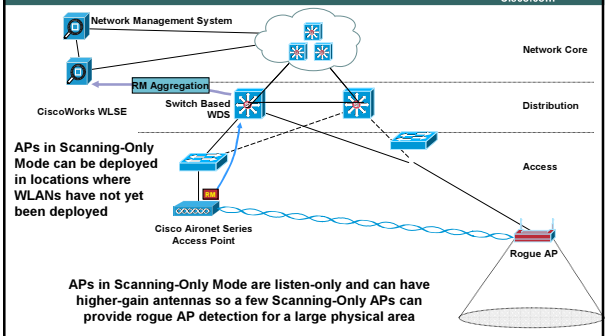
Cisco.com



1. CiscoWorks WLSE analyzes aggregated Radio Management (RM) from both access points (APs) and clients
2. CiscoWorks WLSE sends alerts indicating presence of rogue APs
3. Client RF scanning detects rogue APs beyond the range of AP-only RF scanning

Cisco SWAN - Rogue Access Point Detection
Access Point Scanning-Only Mode

Cisco.com

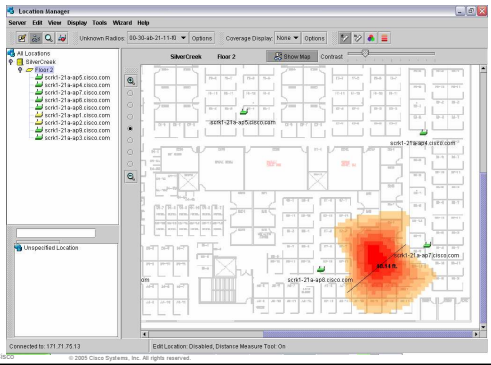


APs in Scanning-Only Mode are listen-only and can have higher-gain antennas so a few Scanning-Only APs can provide rogue AP detection for a large physical area

Cisco on Cisco

CiscoWorks WLSE Location Manager

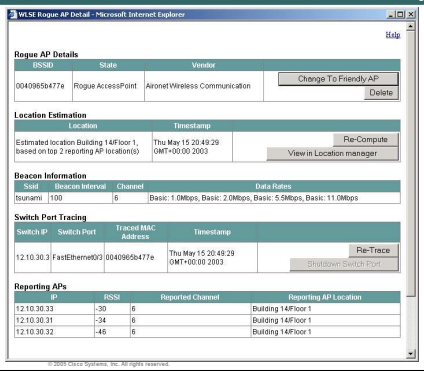
Cisco.com



Cisco on Cisco

CiscoWorks WLSE
Rogue AP Details Screen

Cisco.com

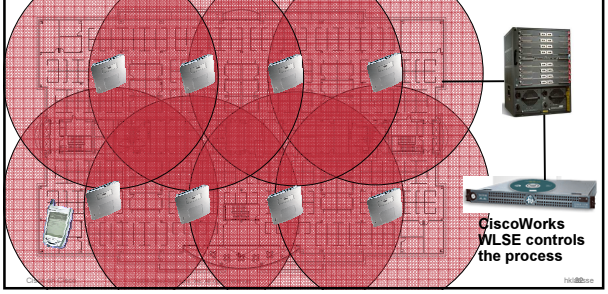


Cisco on Cisco

Cisco SWAN
Out of Box Deployment - Assisted Site Survey

Cisco.com

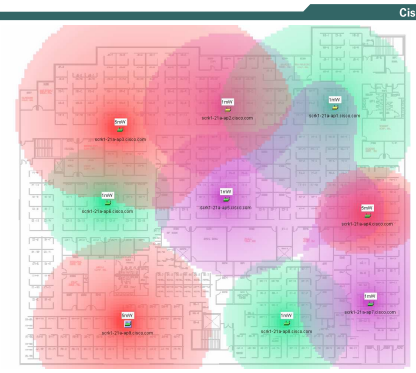
1. CiscoWorks WLSE instructs APs to measure and report the Radio Frequency (RF) environment and pushes optimal RF configurations to APs
2. CiscoWorks WLSE uses measurements from a client as it walks the perimeter of the coverage area to further fine-tune RF coverage



CiscoWorks WLSE controls the process

CiscoWorks WLSE Screen Shot: RF Map

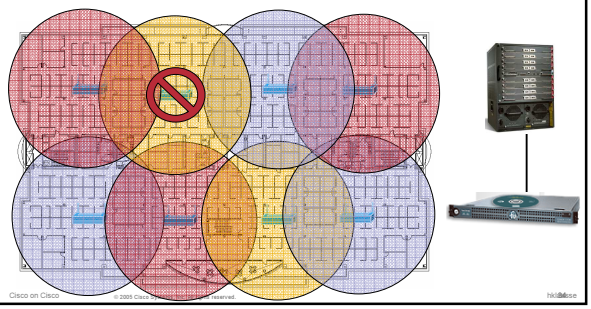
Cisco.com



Self Healing WLANs

Cisco.com

1. Timely response to loss of AP/Radio
2. Stable mechanism



Agenda

Empowering Teachers and the Strength of Their Connections

Cisco.com

- Wireless standards and trends.
- Wireless security.
- Structured Wireless-Aware Network SWAN.
- Summary.

Why Wireless with Cisco?

Cisco.com

- *We know networking, and are committed to wireless*
  - Wireless networking is complicated and evolving
  - An extension of the wired network
  - No ambitions for devices
- *We are committed to an open, standards-based approach*
  - Required to grow the overall market
  - Can't do it all ourselves, even if we wanted to
  - We have many successful multi-vendor deployments in retail
  - Proven partnering program with a broad range of solutions
- *We have a proven architecture, and a system cost advantage*
  - Lower overall total cost of ownership, lower risk
- *We have a leading security offering*
  - WPA, 802.1X, Multiple EAP-types, VPN
- *We have a broad, integrated product offering*
  - Significant R&D devoted to wireless at Cisco, beyond APs
  - Support for a variety of wireless applications (voice/video, guest access, IP surveillance, etc.)