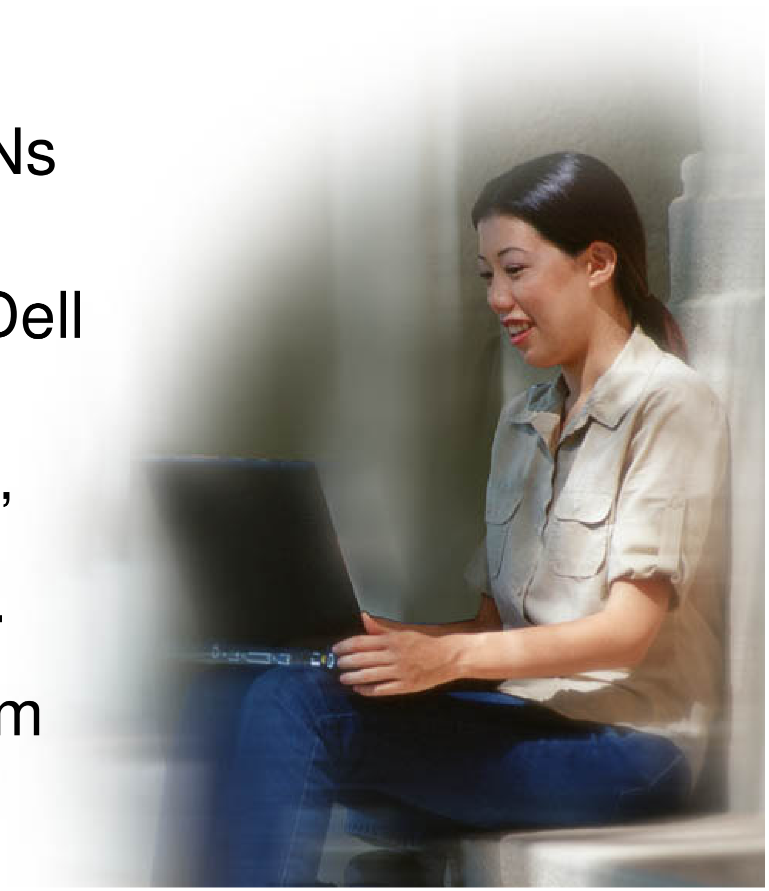
Wireless Mobilization of the Adaptive Enterprise through Intelligent Networking

Sri Sundaralingam

Technical Marketing Manager
Cisco Systems, Inc.

Momentum is Building in Wireless LANs

- 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



Agenda

- **Deployment Criteria**
- Cisco's SWAN Solution
- 802.11a/b/g Technologies
- Centralized Network and RF (i.e. "Air") Management
- 802.11 Security
- Wired/Wireless Integration
- Summary

Deployment Criteria

- End-to-End Security
  - Layer-2 based user authentication and data confidentiality
  - Integrated wired/wireless security
- Centralized Network and RF Management
  - Scalable deployment model for network growth
  - Single point of control for WLAN infrastructure device configuration and SW revisions
- End-to-End Mobility
  - Within buildings, between buildings, etc
- Quality of Service (QoS)
  - End-to-end prioritization for applications such as voice and video

Deployment Criteria

- Minimized Total cost of ownership
  - Integrate with existing wired network
  - Minimize operational costs of deploying and managing the WLAN network
- Investment protection
  - Support for future 802.11 standards
  - Avoid overhaul of WLAN infrastructure as the 802.11 technology matures...

Agenda

- Deployment Criteria
- **Cisco’s SWAN Solution**
- 802.11a/b/g Technologies
- Centralized Network and RF (i.e. “Air”) Management
- 802.11 Security
- Wired/Wireless Integration
- Summary

Cisco's SWAN* Solution

3

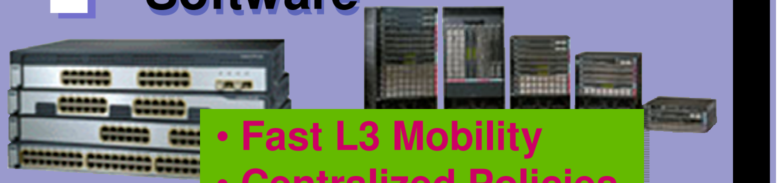
Cisco client adapters

Cisco Compatible client devices

- Expanded Security Options
- Granular Site Surveys

4

Cisco switches and routers with wireless-aware Cisco IOS® Software



- Fast L3 Mobility
- Centralized Policies
- High Availability

2

Cisco Network Management - CiscoWorks WLSE 802.1X AAA Server

- Simplified Deployment / Management
- Rogue AP Detection / Suppression

1

Cisco IOS Software APs

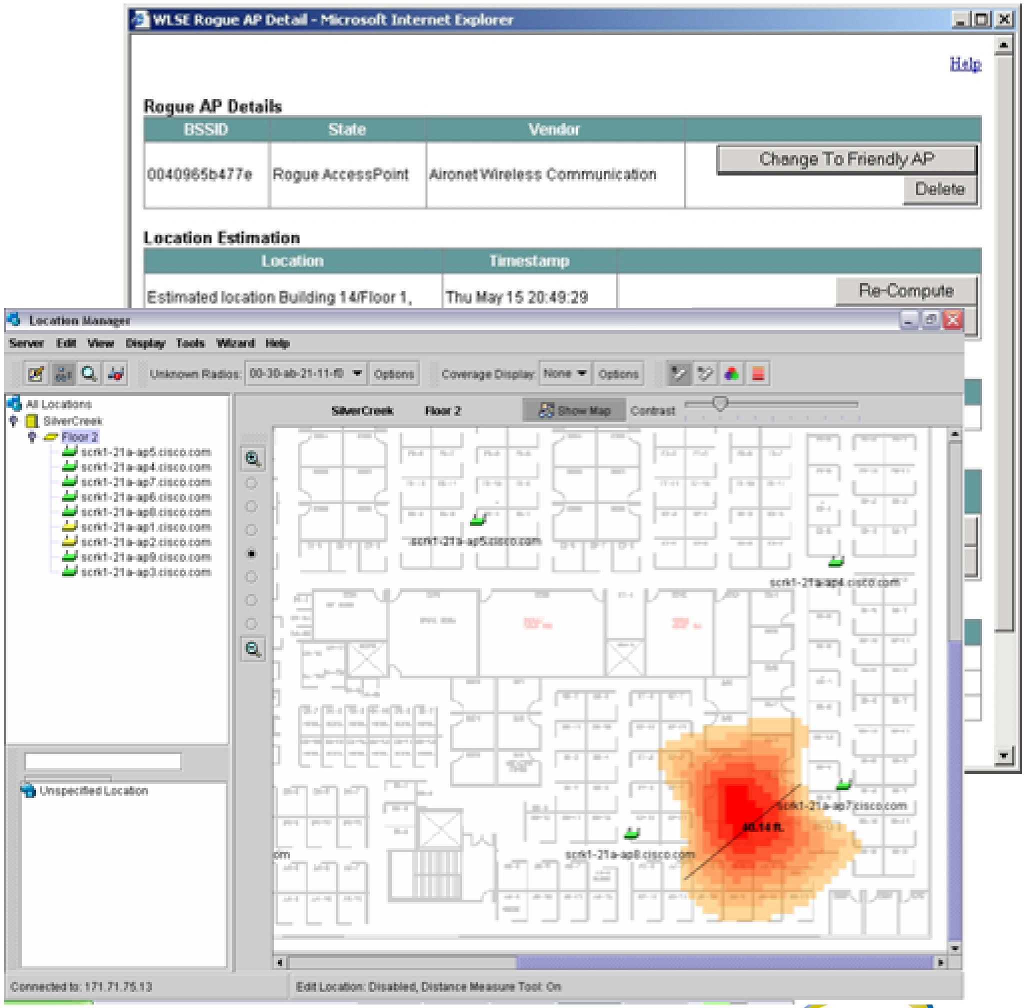
Wi-Fi Client Adapters

- Best in Class APs

*Note: SWAN = Structured Wireless-Aware Network

Cisco SWAN Provides for Next Generation Features

- Rogue AP detection
- Interference location assistance
- Intrusion detection
- RF network visualization and reporting
- Fast and secure roaming
- Site survey assistance
- Self healing capabilities



Rogue AP Details

BSSID	State	Vendor	
0040965b477e	Rogue AccessPoint	Aironet Wireless Communication	Change To Friendly AP Delete

Location Estimation

Location	Timestamp	
Estimated location Building 14/Floor 1,	Thu May 15 20:49:29	Re-Compute

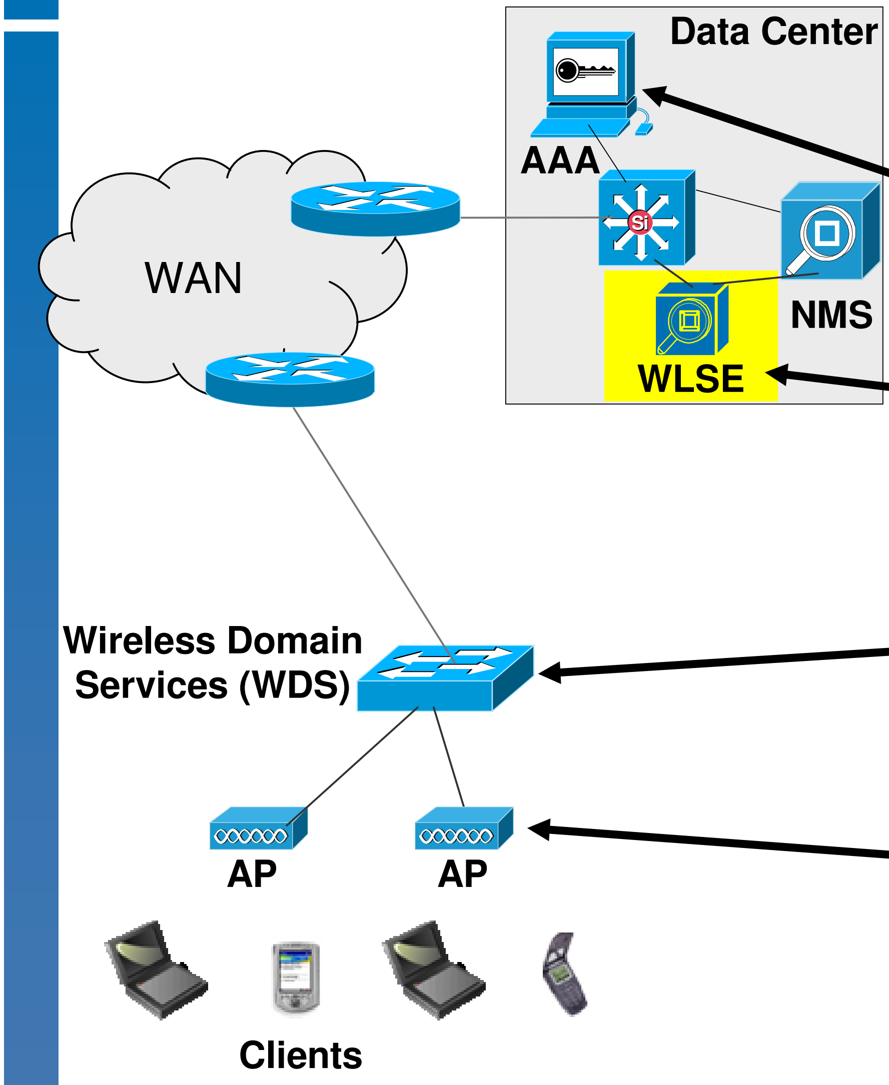
Unknown Radios: 00-30-ab-21-11-f0

Coverage Display: None

Connected to: 171.71.75.13

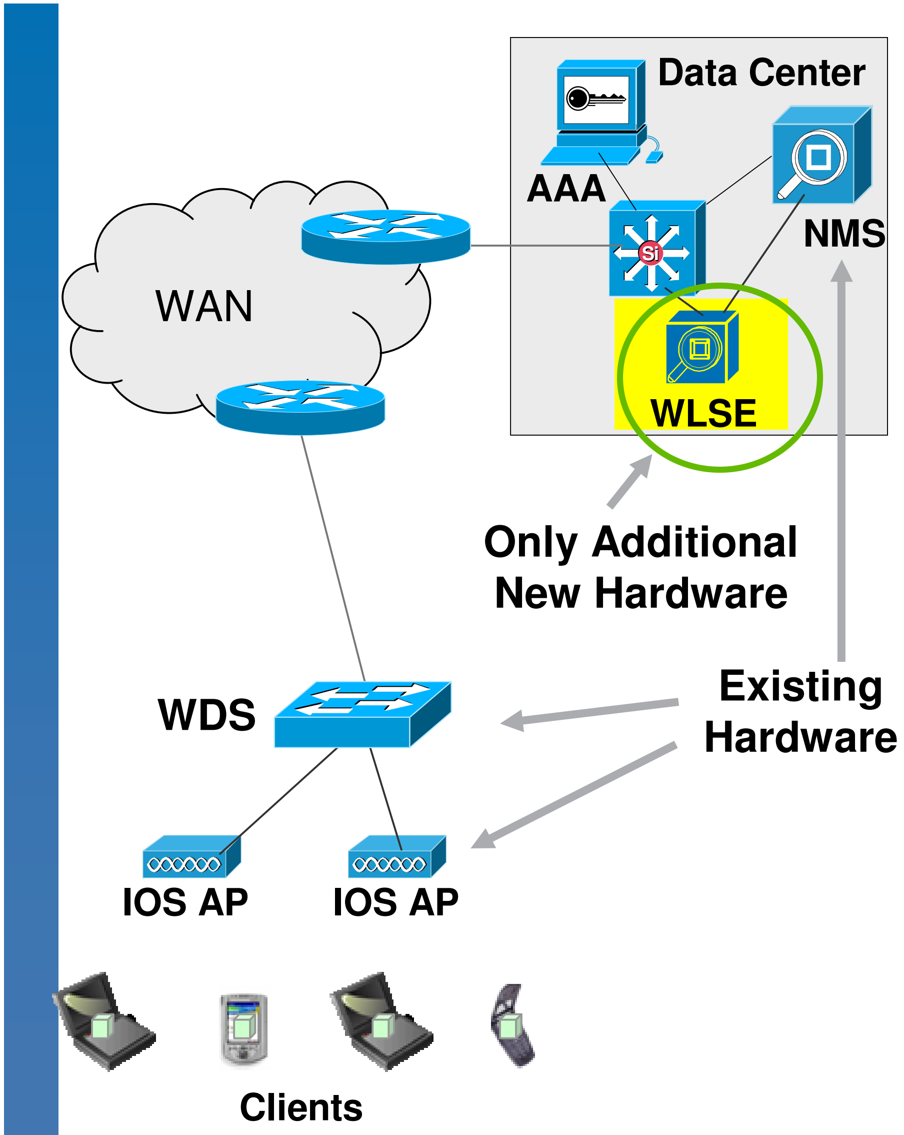
Edit Location: Disabled, Distance Measure Tool: On

Cisco SWAN’s Hybrid Approach



- Places intelligence where needed for specific application requirements
  - Centralized security policy management for WLAN user authentication
  - Centralized network/RF management and monitoring for network-wide visibility, enterprise scalability
  - Localized WLAN user data and control data aggregation to enable security, QoS, and Mobility services
  - 802.1x/security access control, 802.11i/WPA encryption, and packet prioritization at the wireless edge to enable end-to-end Security and QoS

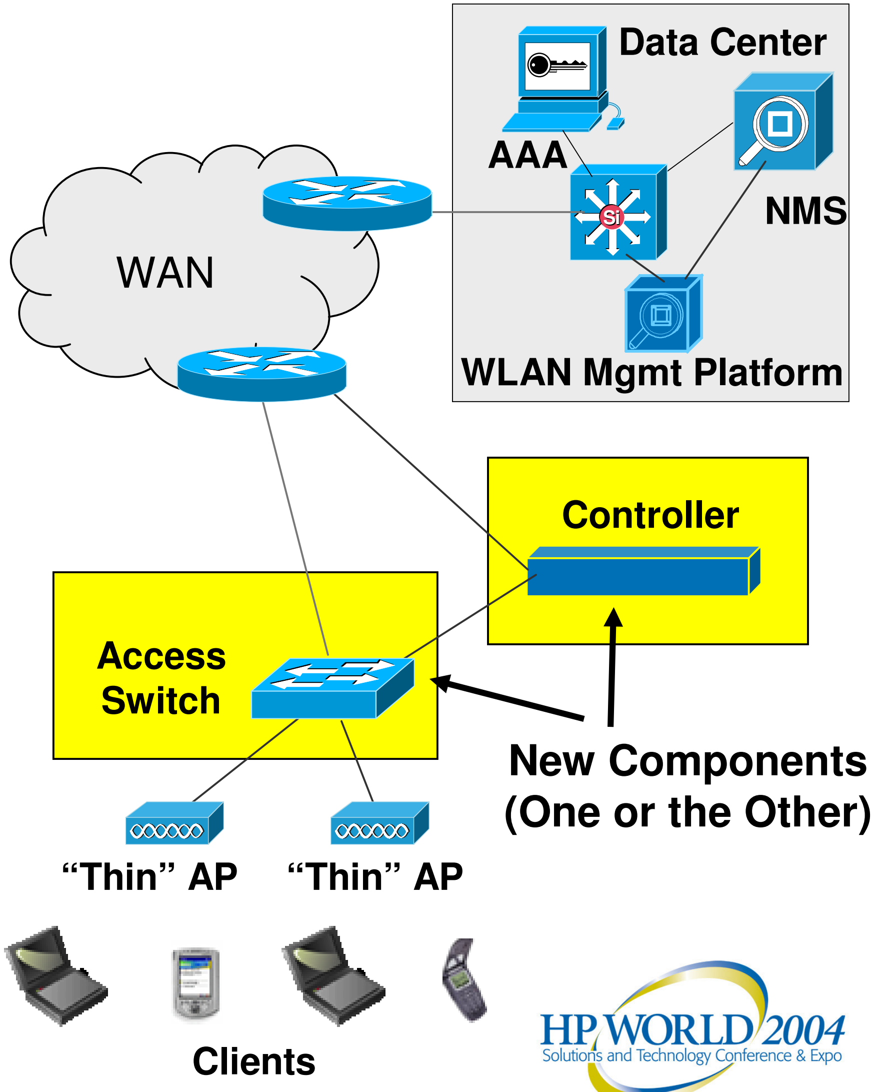
Cost Effectiveness of the Cisco Structured Wireless-Aware Network



- Flexible framework supports differing applications, network sizes, deployment stages, etc.
  - Scales up to enterprise campuses, down to small branch offices
  - More linear cost structure, pay as you scale
- Integrates wireless into existing networks
  - Uses existing AP350, AP1200 or AP1100 access points

The Wireless Switch/Thin AP Architecture

- Architectures vary by vendor but key similarities exist
- Wireless “switch” is really a controller
  - –Low port density, often single ingress/egress upstream port
  - –Minimal wired security and QoS features
- “Thin” AP wholly dependent upon controller
  - –Typically just a standard SOHO AP
- AP is a logical controller port
  - –AP has no user interface, no stored image
  - –AP used to pass packets; Unauthorized traffic is tunneled to the controller!
  - –No intelligent packet filtering performed in AP



HP WORLD 2004 Solutions and Technology Conference & Expo

Agenda

- Deployment Criteria
- Cisco’s SWAN Solution
- **802.11a/b/g Technologies**
- Centralized Network and RF (i.e. “Air”) Management
- 802.11 Security
- Wired/Wireless Integration
- Summary

802.11 a/b/g: Frequently Asked Questions

- 802.11a/b/g: Which one to pick?
- Single-band clients Vs Dual-band Clients?
  - Note: Single-band means 2.4 GHz (i.e. 802.11b/g) OR 5 GHz (802.11a); Dual band would mean both 2.4 GHz and 5 GHz bands.
- 802.11b for voice and 802.11a for data? **OR** 802.11a for voice and 802.11b for data?
- WLAN cell design: How many clients per cell? i.e. Bandwidth/Capacity per client?

802.11b Overview

- Ratified in 1999
  - Two years after initial 802.11 standard
  - Same time as 802.11a
- Defined data rates up to 11Mbps
- Operates in 2.4GHz band
  - Similar frequencies and regulations around the world
- Three non-overlapping operating channels

802.11b Data Rates

- Low order, robust modulation schema support lower data rates
- Higher order modulation schema support higher data rates

Modulation	Transmission Type	Data Rate
BPSK	DSSS	1Mbps
QPSK	DSSS	2Mbps
CCK	DSSS	5.5Mbps
CCK	DSSS	11Mbps

HP WORLD 2004
Solutions and Technology Conference & Expo

802.11a

- Ratified as standard in September 1999
- Data rates to 54 Mbps defined
- Provides twelve WLAN channels today
  - More channels forthcoming
- Regulations currently differ extensively across countries

802.11a Data Rates

Modulation	Transmission Type	Bits per Subchannel (Kbps)	Total Data Rate (Mbps)
BPSK	OFDM	125	6
BPSK	OFDM	187.5	9
QPSK	OFDM	250	12
QPSK	OFDM	375	18
16-QAM	OFDM	500	24
16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

802.11a Issues

- Eight channels (UNII 1 and UNII 2 combined)
  - Avoid the use of adjacent channels in adjacent cells due to sidebands
- Antenna limitations
  - UNII 1—Indoor usage and limited to permanently attached antennas in the U.S.
  - UNII 2—Indoor/outdoor and may use external antennas
  - UNII 3—Typically outdoor with external antennas, but can be used indoors
- Not qualified in many countries
  - Tx power control and dynamic frequency selection required (802.11h)

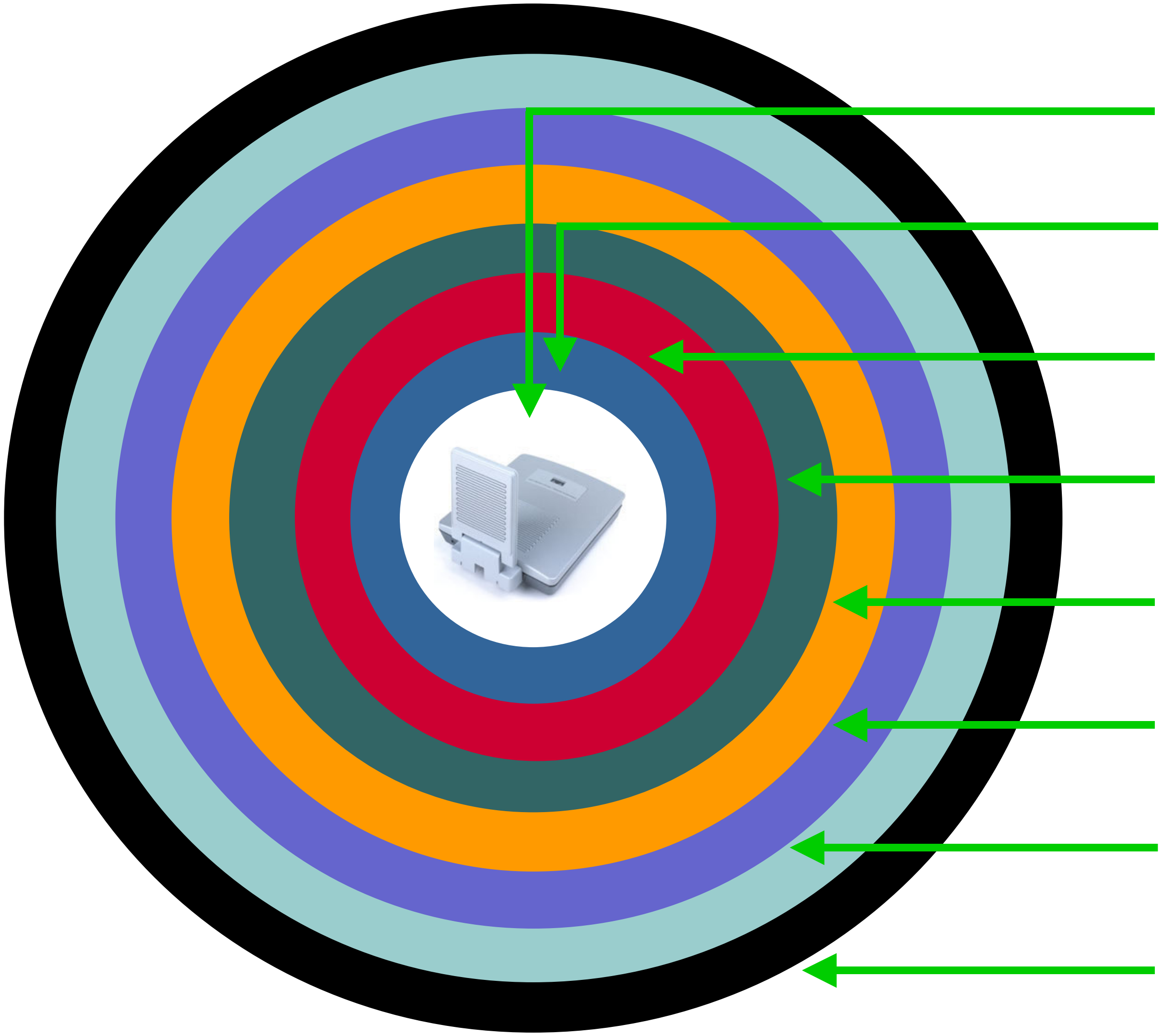
The 802.11g Standard

- 802.11g standard ratified in June 2003
- Operates in the same 2.4-GHz band as 802.11b
  - Uses the same three nonoverlapping channels
- Full backward compatibility with 802.11b
  - Conceptually similar to Ethernet and fast Ethernet
- Uses OFDM for 802.11g data rates, DSSS for 802.11b data rates
  - Employs various modulation schemes for a variety of data rates
  - 54, 48, 36, 24, 18, 12, 9, and 6 Mbps via OFDM
  - 11, 5.5, 2, and 1 Mbps via DSSS

802.11g Data Rates

Modulation	Transmission Type	Bits per Subchannel (Kbps)	Data Rate (Mbps)
BPSK	DSSS	NA	1
QPSK	DSSS	NA	2
CCK	DSSS	NA	5.5
BPSK	OFDM	125	6
BPSK	OFDM	187.5	9
CCK	DSSS	NA	11
QPSK	OFDM	250	12
QPSK	OFDM	375	18
16-QAM	OFDM	500	24
16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

802.11 Access Point Coverage



54 Mbps

48 Mbps

36 Mbps

24 Mbps

18 Mbps

12 Mbps

9 Mbps

6 Mbps

Aggregate and Per-User Throughput

- 802.11, like Ethernet, is a shared medium
- Aggregate throughput is the total bandwidth shared by all users in a cell
- Generally, the larger the cell, the more users in the cell
  - Greater per user throughput means smaller cells and more access points for a given area
- How many users per access point?
  - What’s the aggregate throughput of the access point?
  - On average, what amount of per user throughput do you want to provide?

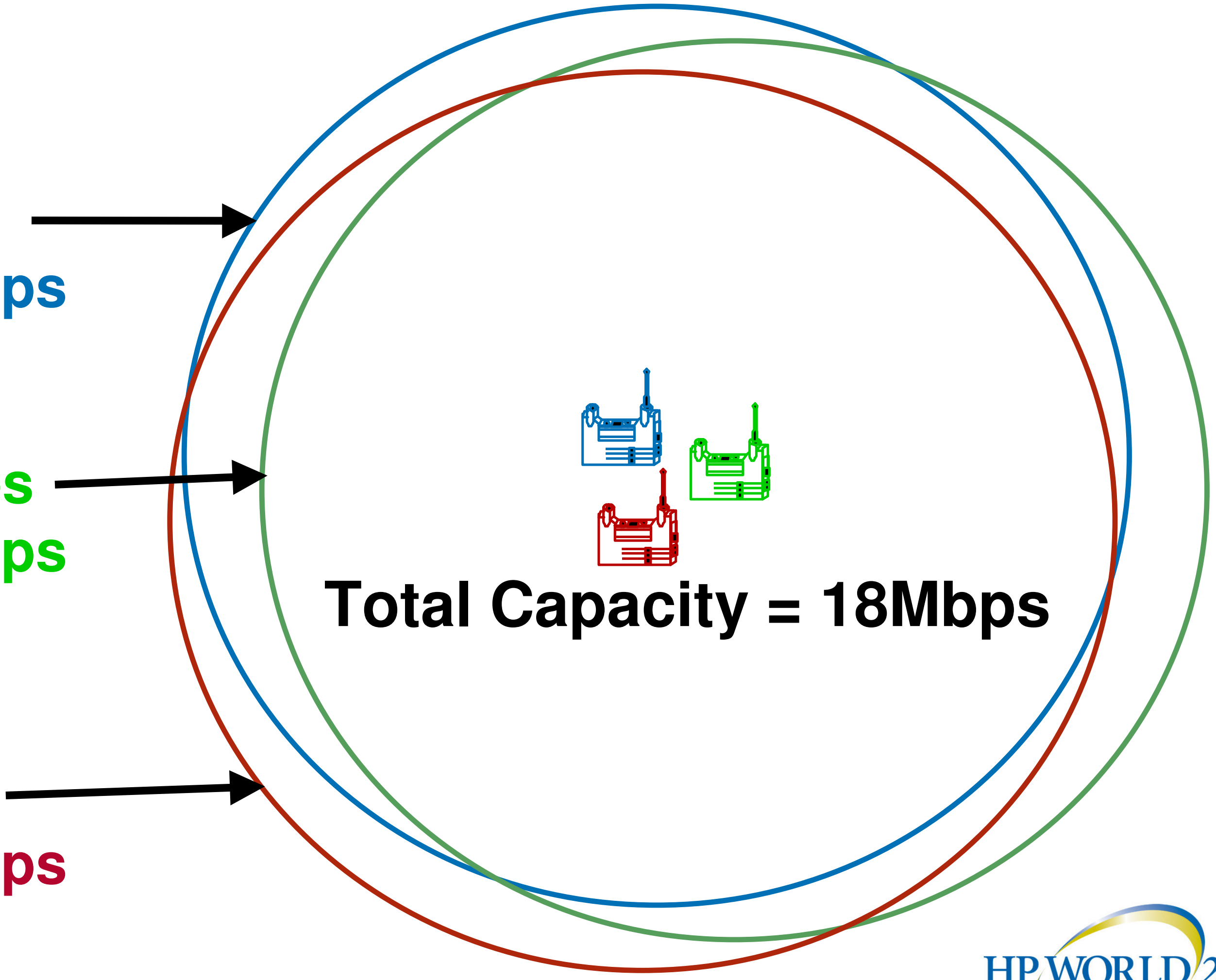
Per-User Throughput Examples

Technology	Data Rate (Mbps)	Aggregate Throughput (Mbps)	Example User Count	Average per user Throughput
802.11b	11	**6**	**10**	**600Kbps**
802.11b	11	**6**	**20**	**300Kbps**
802.11b	11	**6**	**30**	**200Kbps**
802.11g	54	**14**	**10**	**1.4Mbps**
802.11g	54	**14**	**20**	**700Kbps**
802.11g	54	**14**	**30**	**467Kbps**
802.11a	54	**25**	**10**	**2.5Mbps**
802.11a	54	**25**	**20**	**1.25Mbps**
802.11a	54	**25**	**30**	**833Kbps**

Capacity

- Capacity is throughput multiplied by available, non-overlapping channels
  - –802.11b and 802.11g operate in the same band, use the same three channels
    - •Any 802.11g capacity increase is from throughput alone
- 802.11a currently provides 12 channels in much of the world today, 23 channels in most of the world in 2005
  - –While throughput might be similar to 802.11g, channels are not, neither then is capacity
- In theory, access points set to non-overlapping channels may be co-located to provide all available capacity in a single coverage area
  - –More commonly, it’s an expression of total throughput across a network or facility

802.11b Scalability



Blue = 11Mbps Data Rate, 6Mbps Throughput

Green = 11Mbps Data Rate, 6Mbps Throughput

Red = 11Mbps Data Rate, 6Mbps Throughput

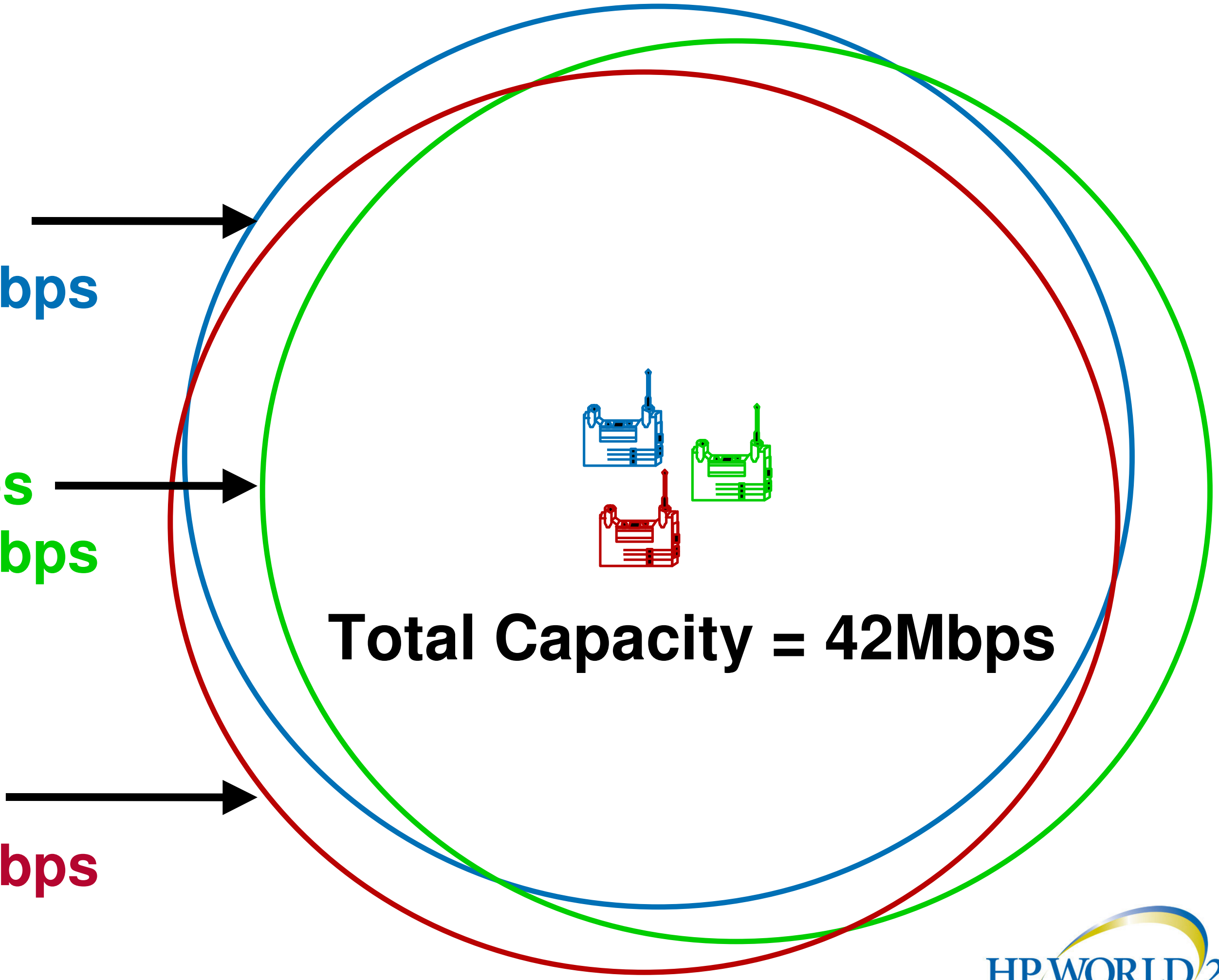
Total Capacity = 18Mbps

802.11g Scalability

Blue = 54Mbps Data Rate, 14Mbps Throughput

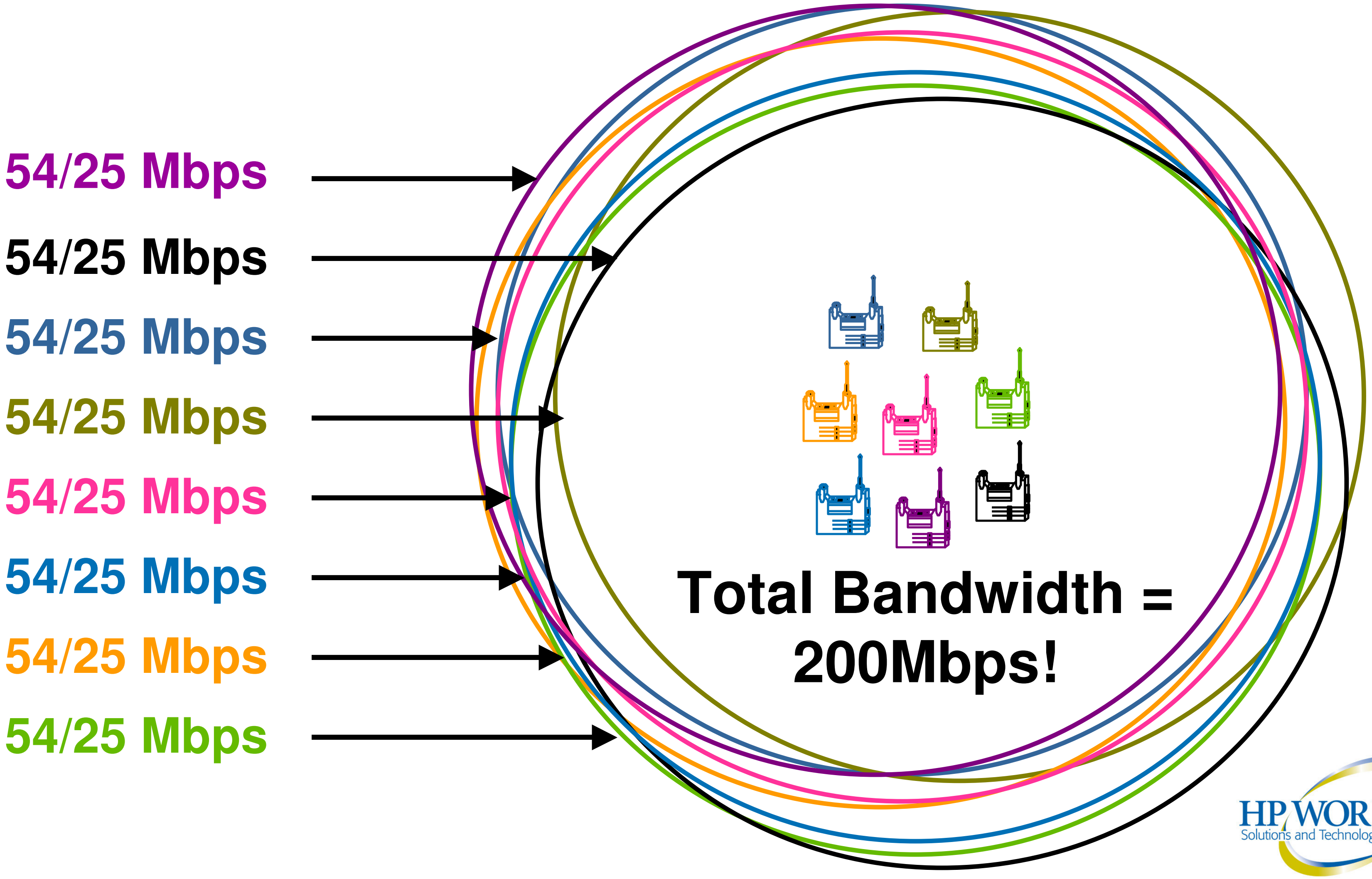
Green = 54Mbps Data Rate, 14Mbps Throughput

Red = 54Mbps Data Rate, 14Mbps Throughput



Total Capacity = 42Mbps

802.11a Scalability (Indoor UNII-1 and UNII-2)



54/25 Mbps

54/25 Mbps

54/25 Mbps

54/25 Mbps

54/25 Mbps

54/25 Mbps

54/25 Mbps

54/25 Mbps

Total Bandwidth = 200Mbps!

802.11 Capacity Compared

	Max. Data Rate (Mbps)	Throughput (Mbps)	Channels	Capacity (Mbps)
802.11b	**11**	**6**	**3**	**18**
802.11g (mixed mode, RTS/CTS)	**54**	**8**	**3**	**24**
802.11g (mixed mode, CTS to self)	**54**	**14**	**3**	**42**
802.11g (no legacy support)	**54**	**22**	**3**	**66**
802.11a (UNII-1 and UNII2)	**54**	**25**	**8**	**200**
802.11a (all UNII bands)	**54**	**25**	**12**	**300**
802.11a (with 802.11h support)	**54**	**25**	**23**	**575**

Cisco’s Current WLAN AP, Bridges, and Clients

Access Points & Bridges

1100 Series	(802.11b/g)
1200 Series	(802.11a/b/g Dual-Band)
1300 Series	(802.11b/g)
1400 Series	(802.11a, P2P & P2MP)
BR350	(802.11b, P2P & P2MP)
WGB352	(802.11b, Workgroup Bridge)
MAR3200	(802.11b/g Mobile Access Router)

Clients

7920	(802.11b, Phone)
CB21AG	(802.11a/bg CardBus)
PI21AG	(802.11a/b/g PCI)
CB20A	(802.11a, Cardbus)
PCM352	(802.11b, PCMCIA)
LMC352	(802.11b, PCMCIA, no antenna)
PCI352	(802.11b, PCI Adapter)

Agenda

- Deployment Criteria
- Cisco's SWAN Solution
- 802.11a/b/g Technologies
- **Centralized Network and RF (i.e. "Air") Management**
- 802.11 Security
- Wired/Wireless Integration
- Summary

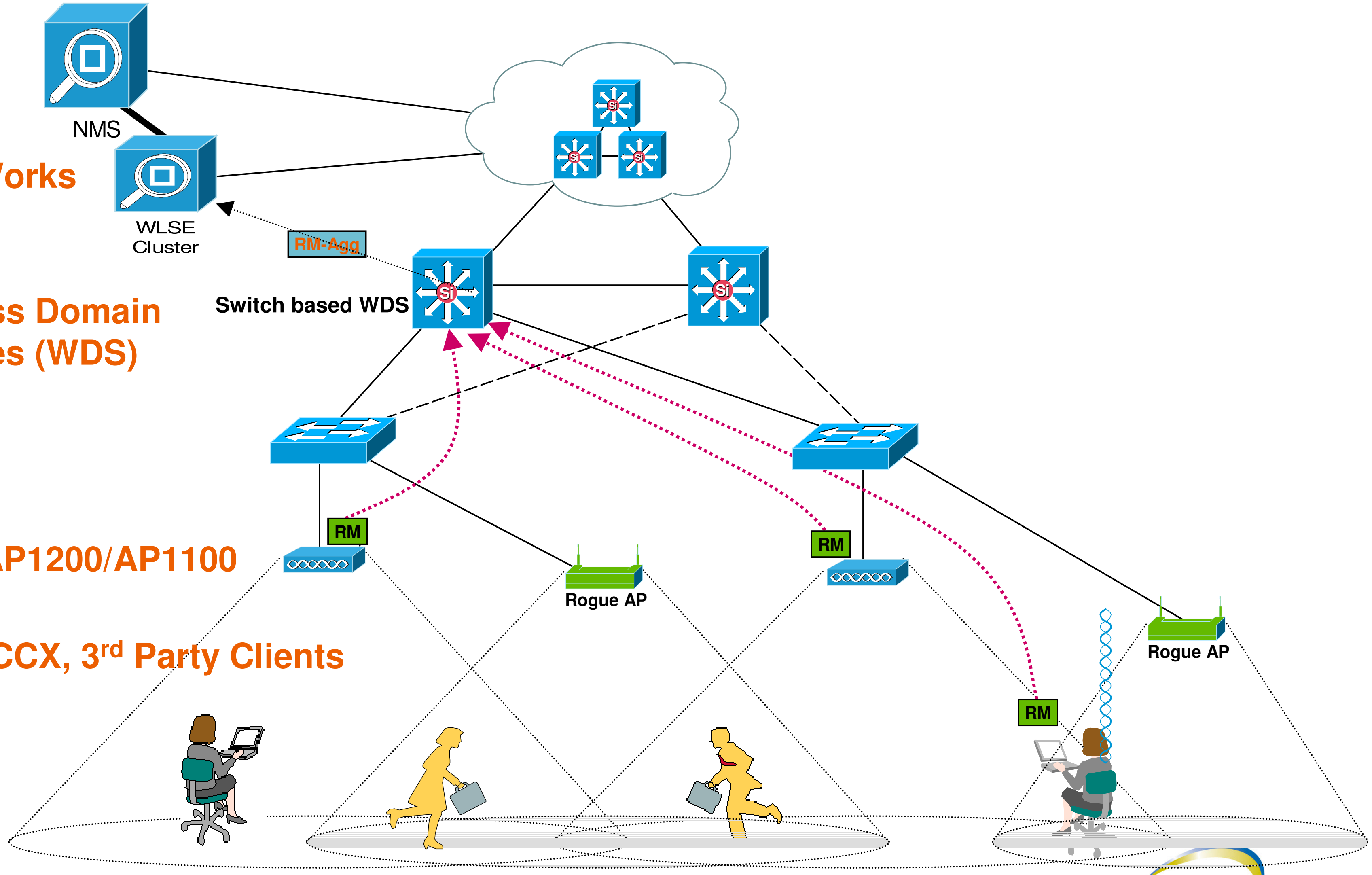
Cisco SWAN Solution: Centralized Network and RF Management

CiscoWorks WLSE

Wireless Domain Services (WDS)

Cisco AP1200/AP1100

Cisco, CCX, 3^{rd} Party Clients



CiscoWorks Wireless LAN Solution Engine

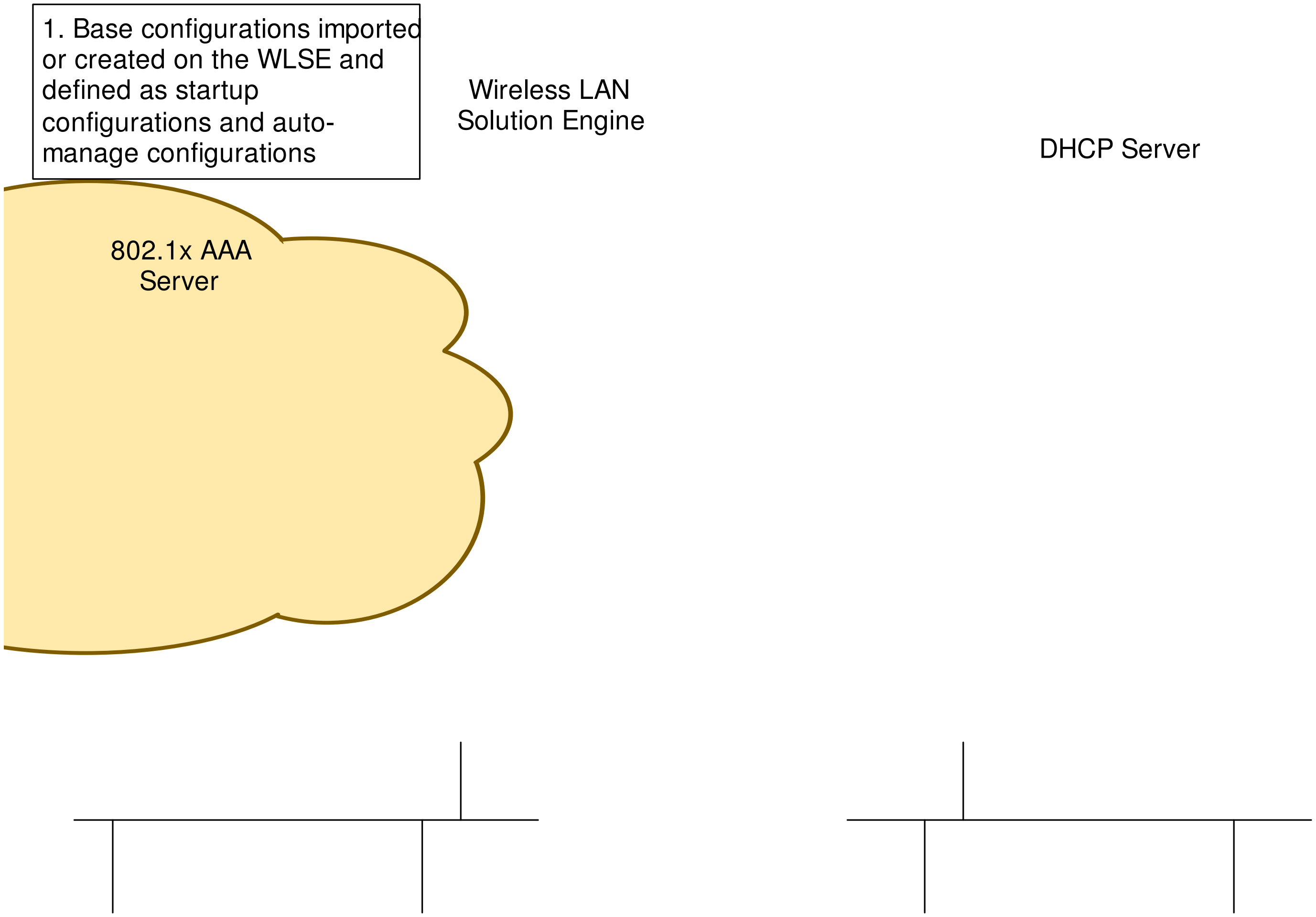
- Centralized WLAN Network and RF Management
- Supports up to 2500 AP's from a single CiscoWorks WLSE server (1 RU rack mountable server)
- Supports 802.11a, b, & g

- Features – Deployment:
  - Assisted Site Survey
  - Auto configuration of Cisco AP's "out-of-the-box"
  - Bulk configuration of AP's with user-defined groups
- Features – Operations:
  - Fault & Performance Monitoring
  - AP Scan Only Mode for Wireless Intrusion Detection
  - Rogue AP Detection, Location, & Suppression
  - Auto Re-Site Survey
  - Self-Healing
  - Real-time Active Client Tracking

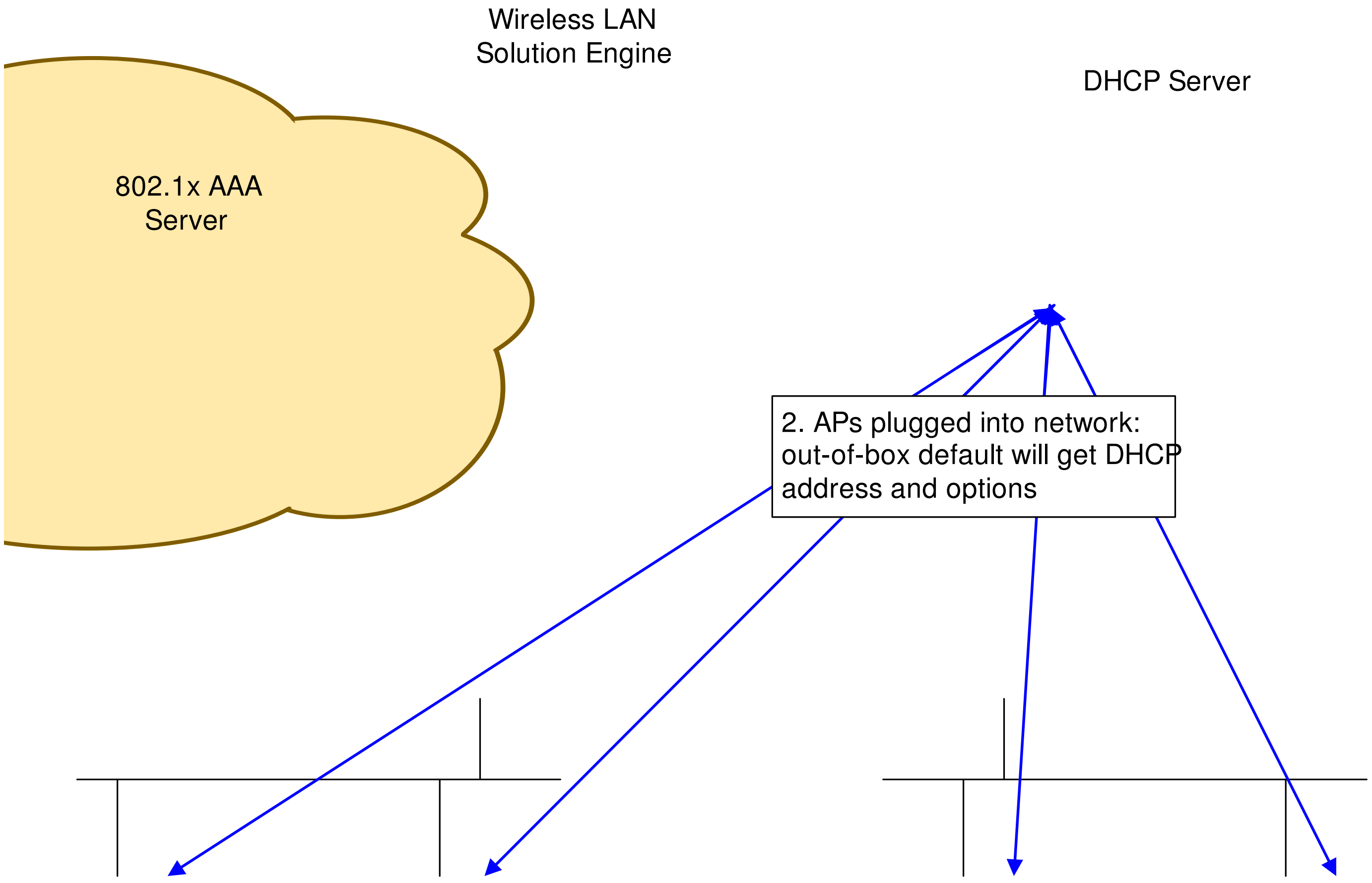
SWAN Out-of-Box Deployment
Taking the Pain Out of Deployment

- Startup template defines just enough information for WLSE to discover access points
- More complete configuration subsequently applied to access points via auto-manage or later via standard configuration job

Cisco SWAN: Out-of-Box Deployment

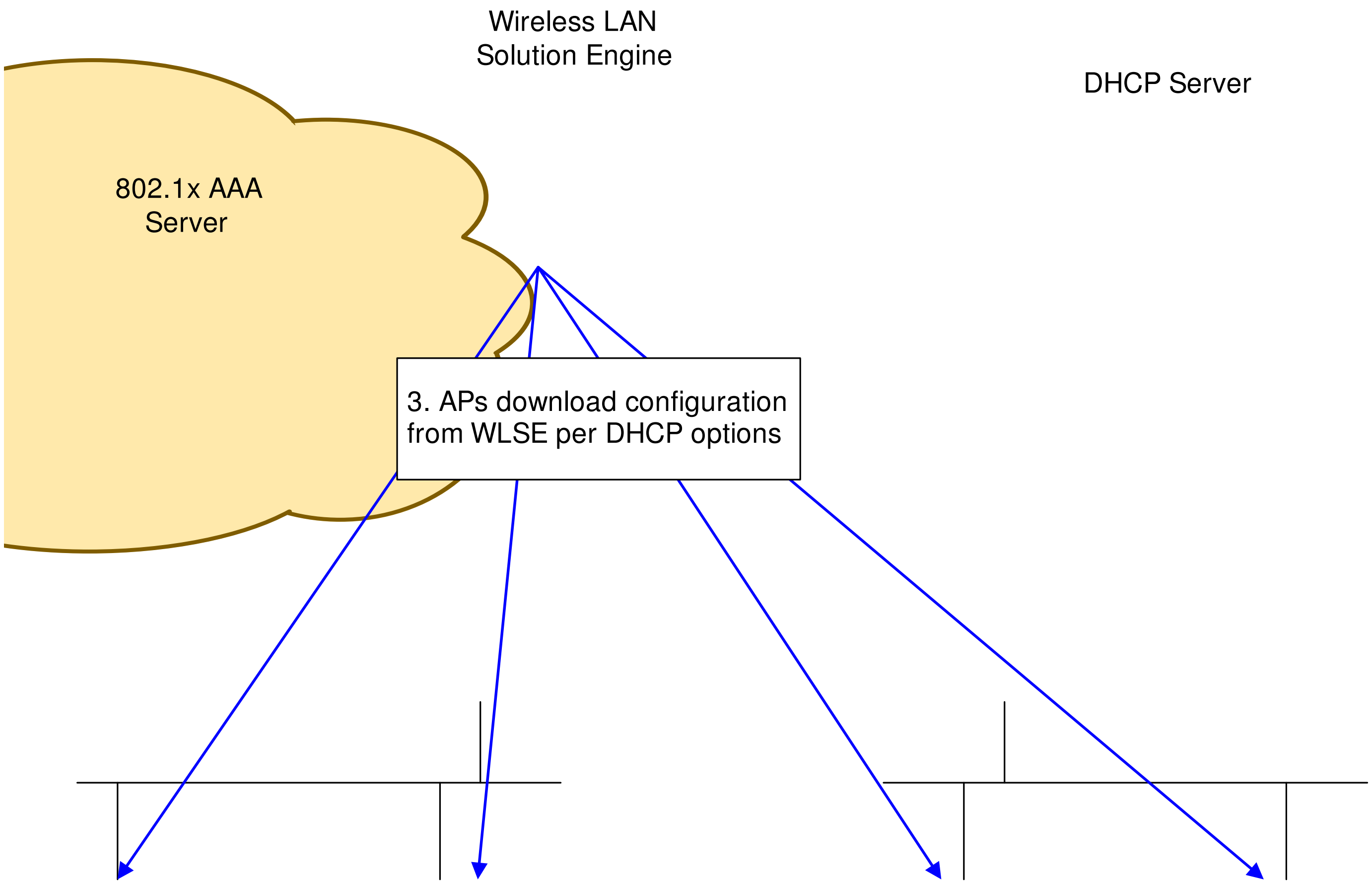

1. Base configurations imported or created on the WLSE and defined as startup configurations and auto-manage configurations

Cisco SWAN: Out-of-Box Deployment



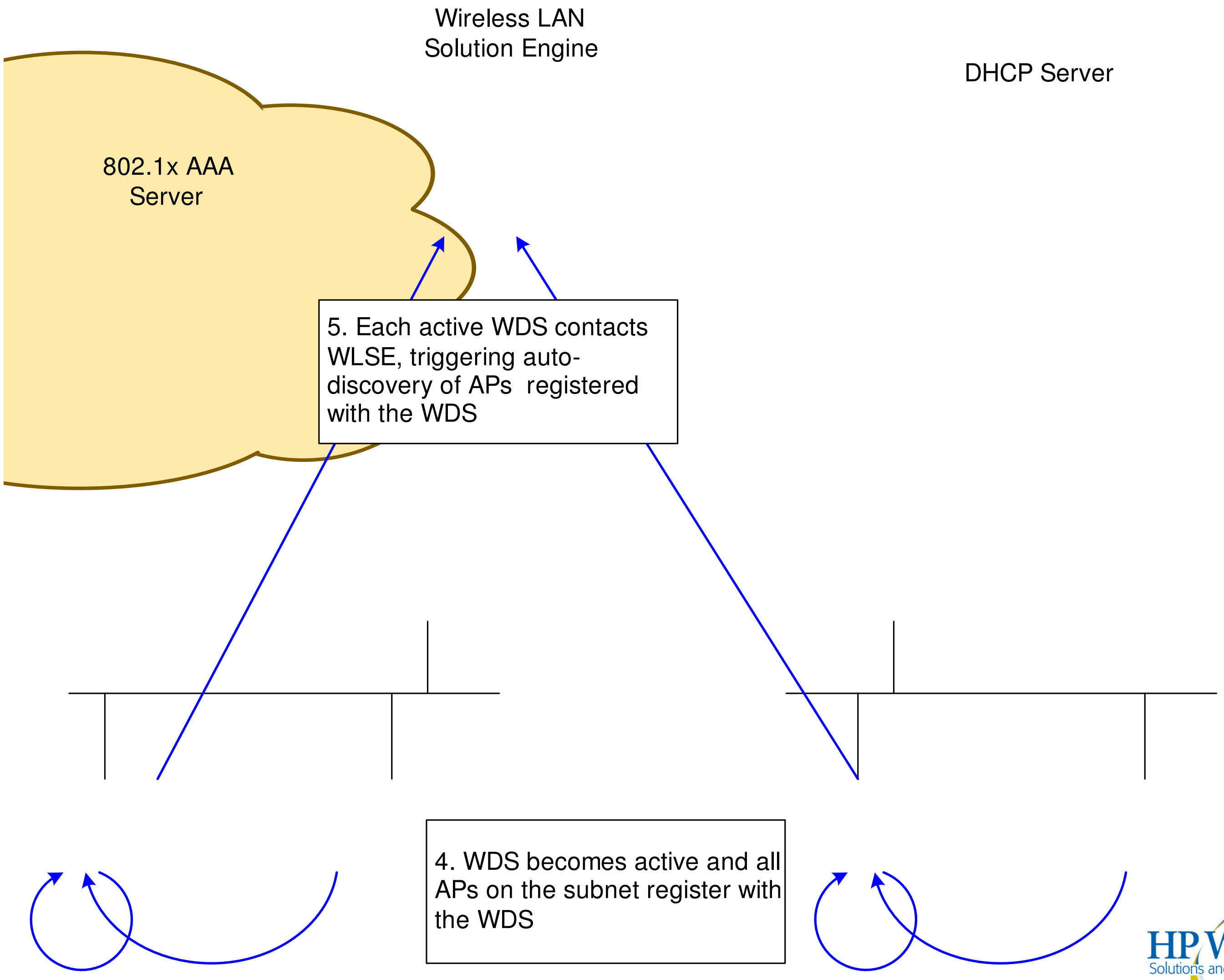
2. APs plugged into network: out-of-box default will get DHCP address and options

Cisco SWAN: Out-of-Box Deployment



3. APs download configuration from WLSE per DHCP options

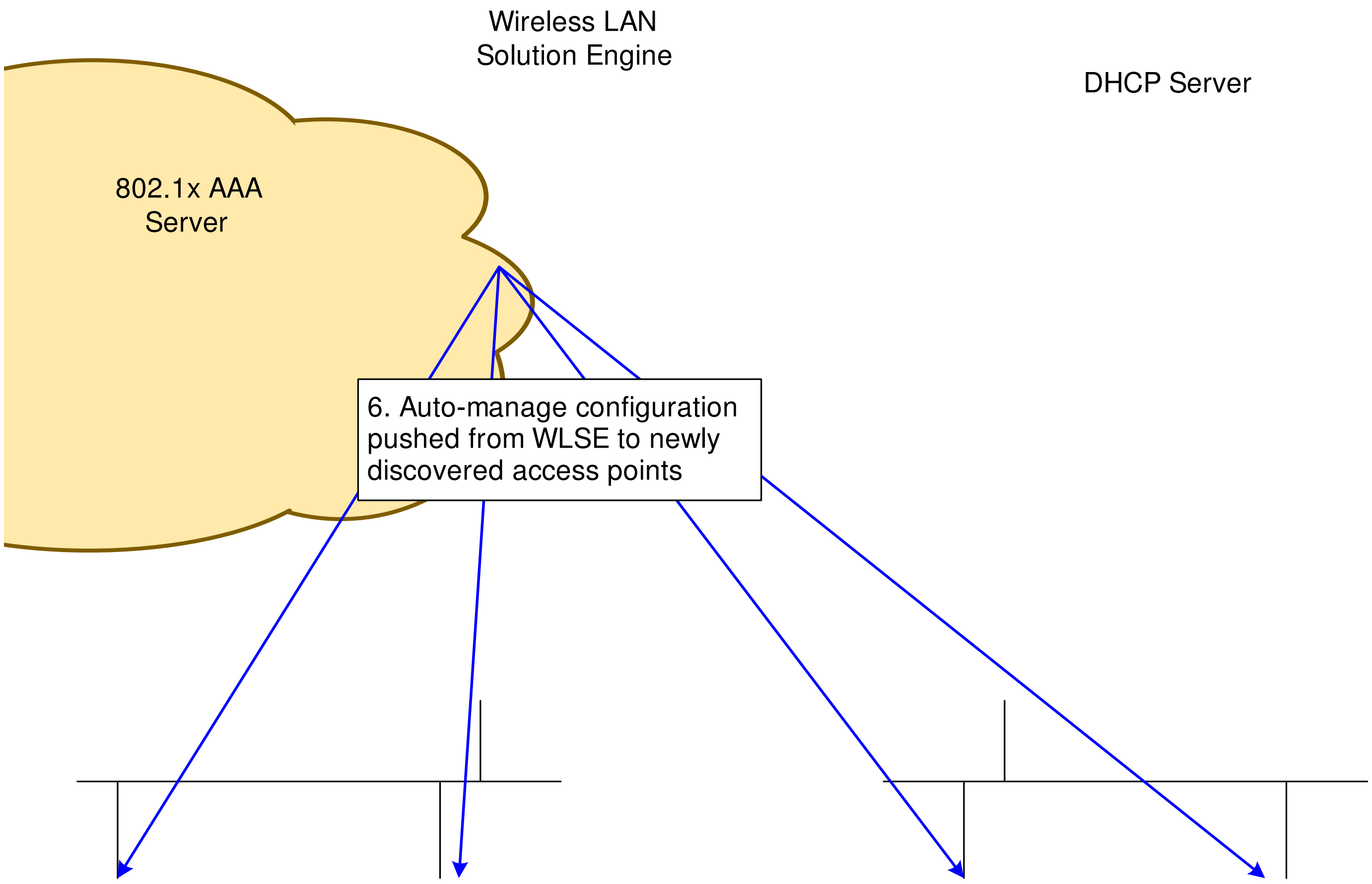
Cisco SWAN: Out-of-Box Deployment



5. Each active WDS contacts WLSE, triggering auto-discovery of APs registered with the WDS

4. WDS becomes active and all APs on the subnet register with the WDS

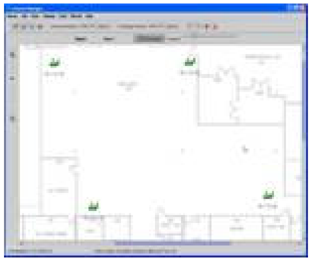
Cisco SWAN: Out-of-Box Deployment



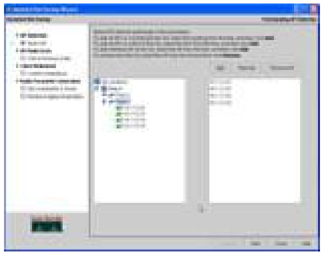
6. Auto-manage configuration pushed from WLSE to newly discovered access points

RF Management: Application Features

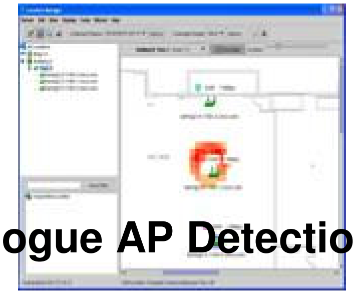
- CiscoWorks WLSE Tools for RF Management:



Location Manager

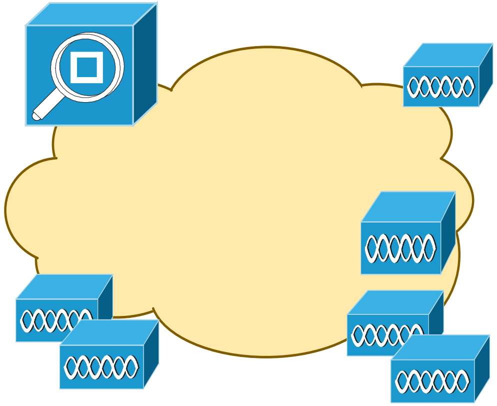


Assisted Site Survey



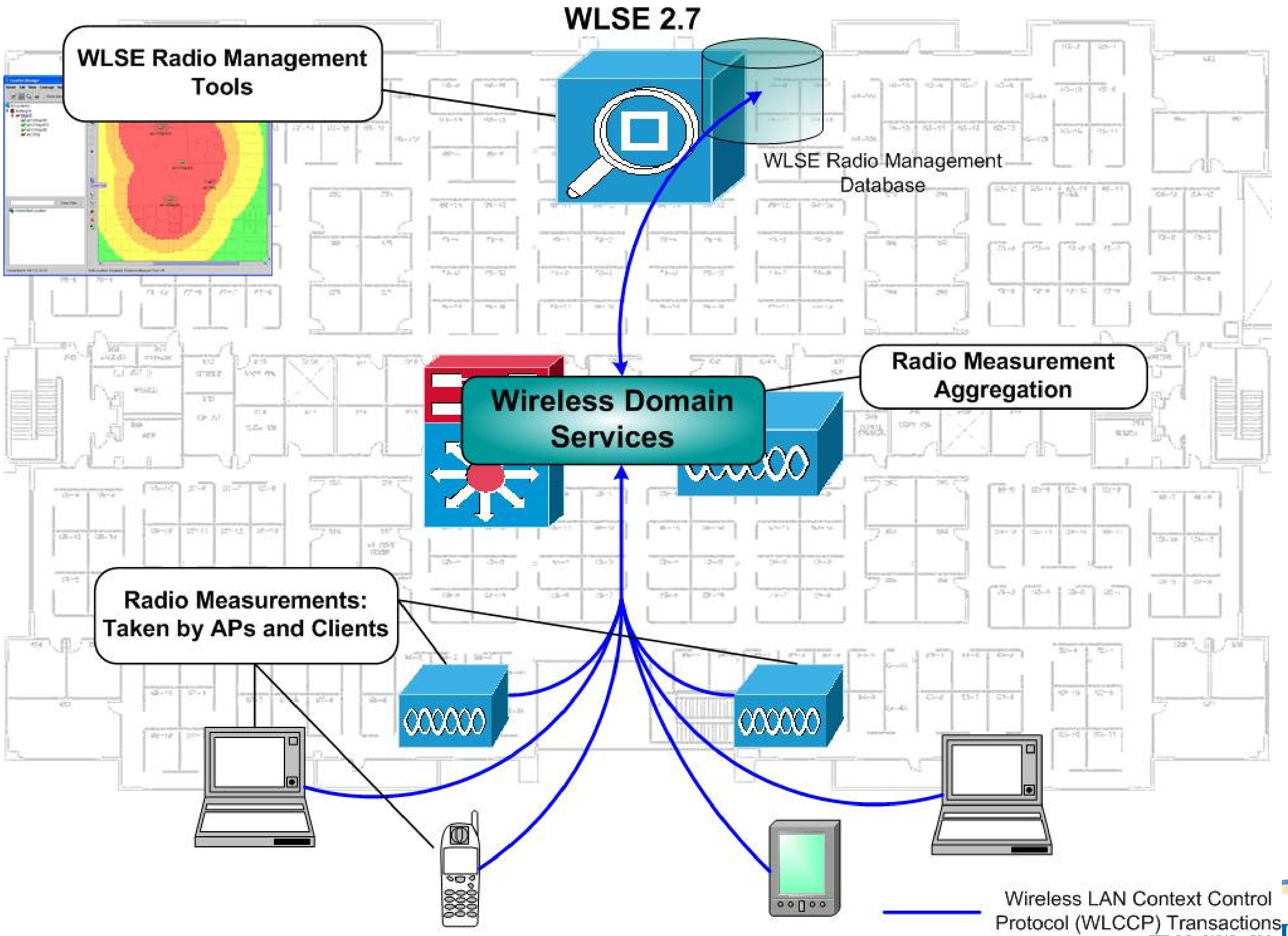
Rogue AP Detection

Radio Network Reports



Radio Interference Detection

Cisco RF Management: Overview



WLSE 2.7

WLSE Radio Management Tools

WLSE Radio Management Database

Radio Measurement Aggregation

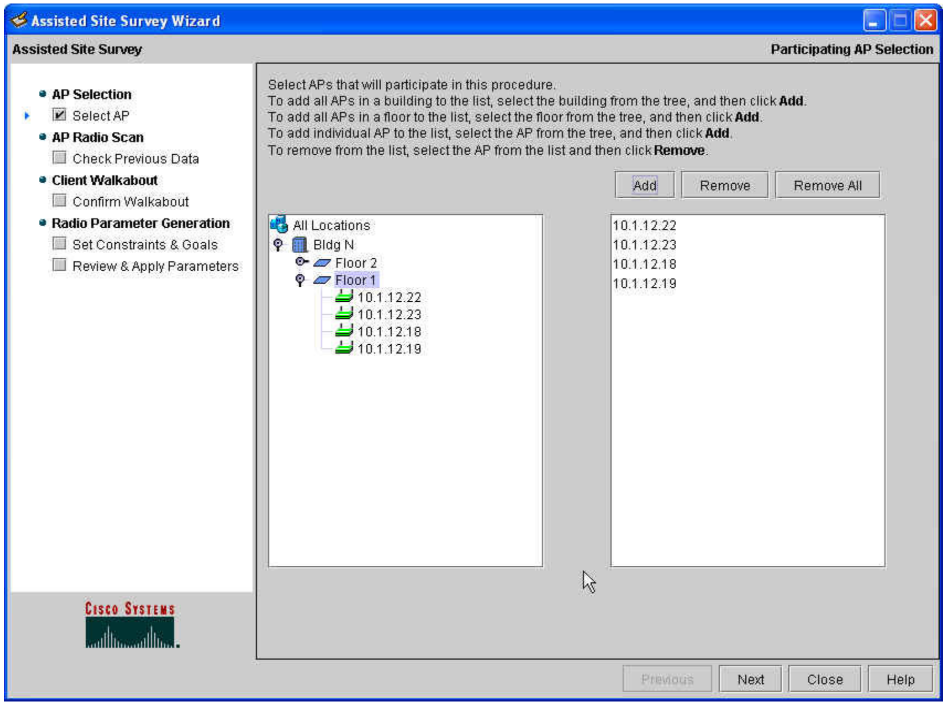
Wireless Domain Services

Radio Measurements: Taken by APs and Clients

Wireless LAN Context Control Protocol (WLCCP) Transactions

Assisted Site Survey

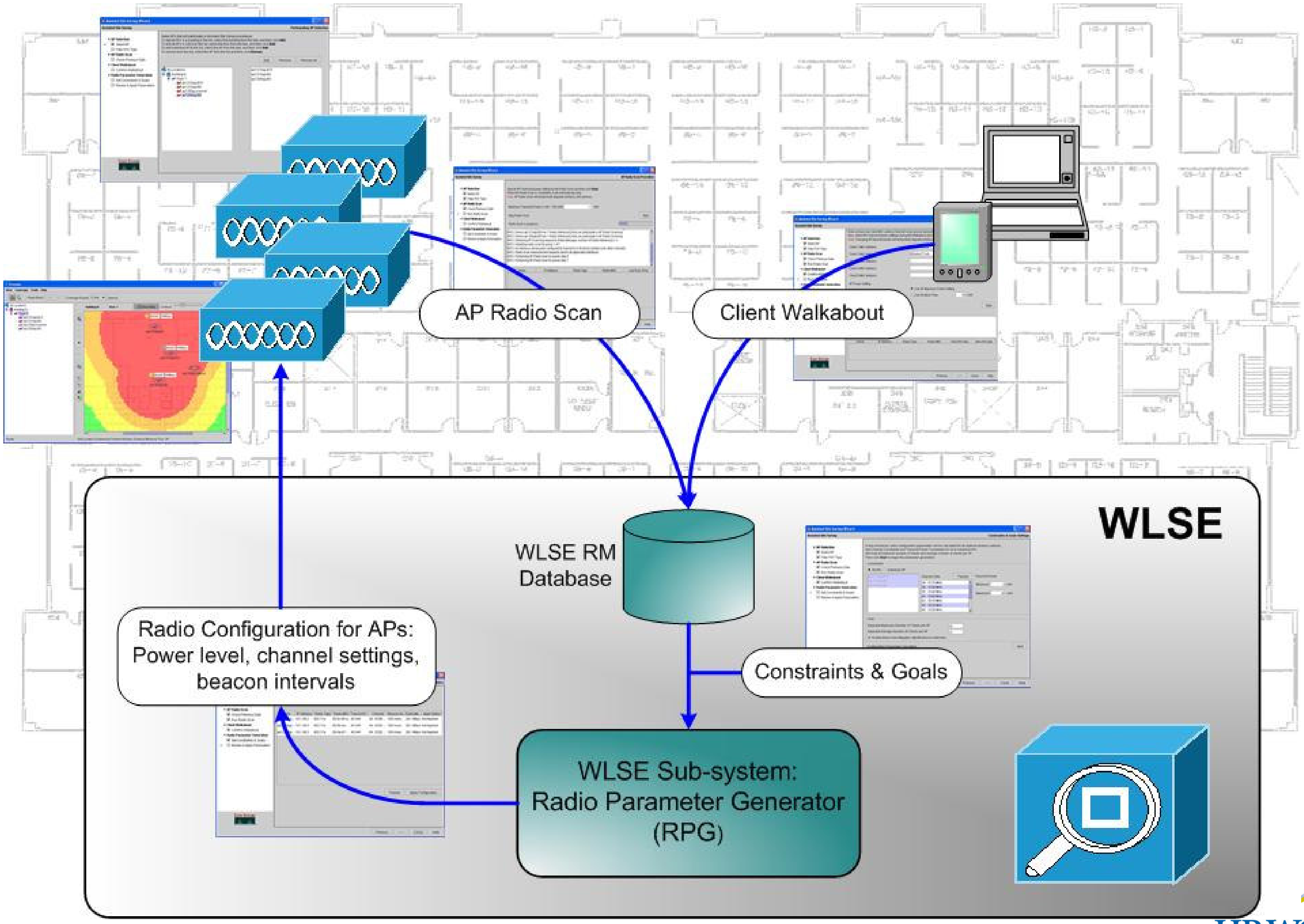
- Deployment and operational wizard tool for optimizing RF configuration
- Uses two innovative methods to characterize the RF environment
  - AP Radio Scan
  - Client Walkabout
- Radio Parameter Generation process RF data for optimal configuration
- Does a good job configuring WLANs in many environments, but is not a replacement for a real site survey
- Complex RF environments present some challenges to the Assisted Site Survey tool



Select APs that will participate in this procedure.
To add all APs in a building to the list, select the building from the tree, and then click **Add**.
To add all APs in a floor to the list, select the floor from the tree, and then click **Add**.
To add individual AP to the list, select the AP from the tree, and then click **Add**.
To remove from the list, select the AP from the list and then click **Remove**.

10.1.12.22
10.1.12.23
10.1.12.18
10.1.12.19

Assisted Site Survey: Explained



AP Radio Scan

Client Walkabout

WLSE

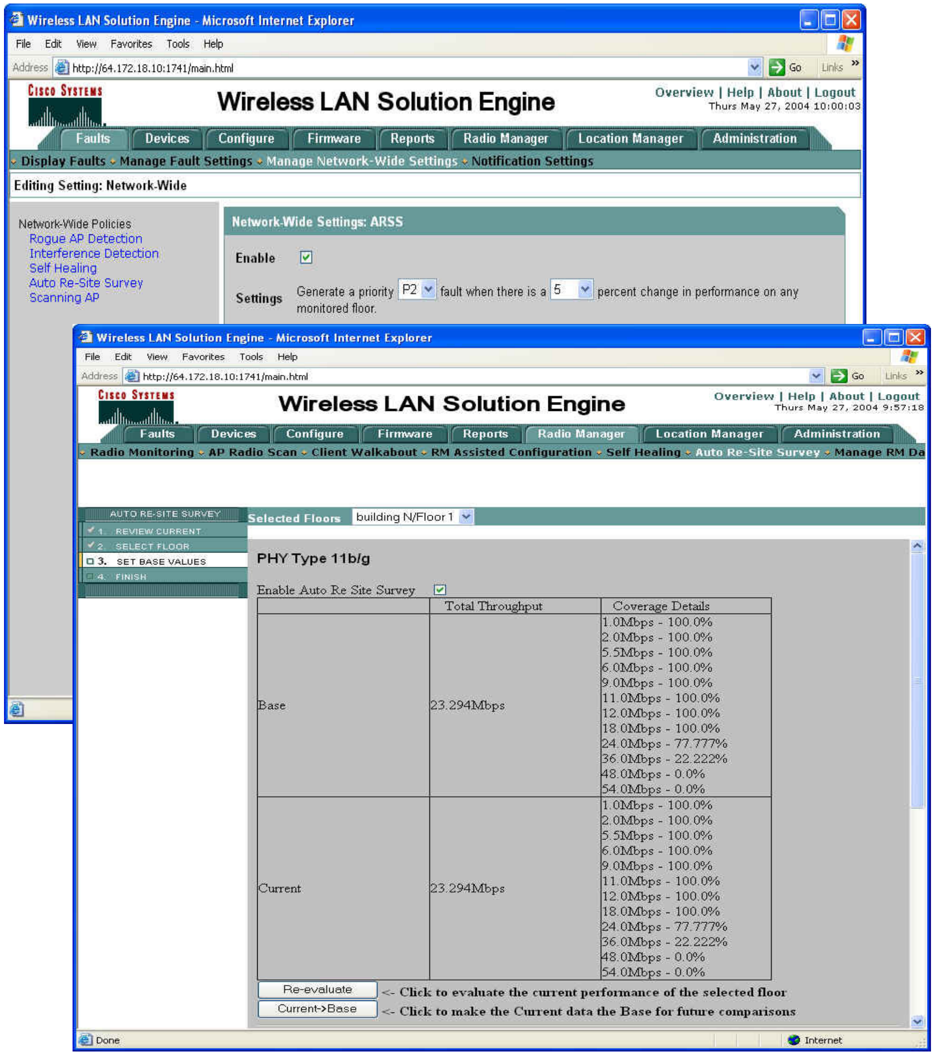
WLSE RM Database

Radio Configuration for APs: Power level, channel settings, beacon intervals

Constraints & Goals

WLSE Sub-system: Radio Parameter Generator (RPG)

Auto Re-Site Survey


Wireless LAN Solution Engine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://64.172.18.10:1741/main.html
Go Links
Cisco Systems
Overview | Help | About | Logout
Thurs May 27, 2004 10:00:03
Faults Devices Configure Firmware Reports Radio Manager Location Manager Administration
Display Faults Manage Fault Settings Manage Network-Wide Settings Notification Settings
Network-Wide Policies
Rogue AP Detection
Interference Detection
Self Healing
Auto Re-Site Survey
Scanning AP

Wireless LAN Solution Engine

Editing Setting: Network-Wide

Network-Wide Settings: ARSS

Enable ☑

Settings: Generate a priority P2 fault when there is a 5 percent change in performance on any monitored floor.

Wireless LAN Solution Engine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://64.172.18.10:1741/main.html
Go Links
Cisco Systems
Overview | Help | About | Logout
Thurs May 27, 2004 9:57:18
Faults Devices Configure Firmware Reports Radio Manager Location Manager Administration
Radio Monitoring AP Radio Scan Client Walkabout RM Assisted Configuration Self Healing Auto Re-Site Survey Manage RM Da
AUTO RE-SITE SURVEY
✓ 1. REVIEW CURRENT
✓ 2. SELECT FLOOR
□ 3. SET BASE VALUES
□ 4. FINISH
Done
Internet

Wireless LAN Solution Engine

Selected Floors: building N/Floor 1

PHY Type 11b/g

Enable Auto Re Site Survey ☑

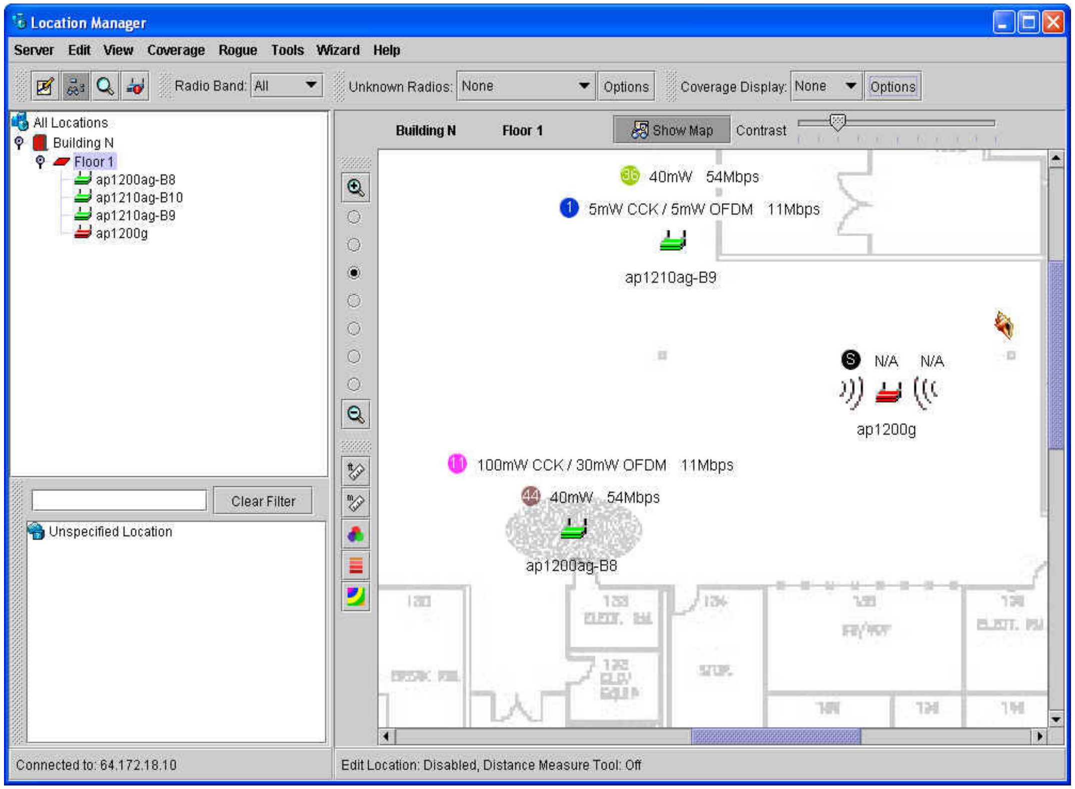
	Total Throughput	Coverage Details
Base	23.294Mbps	1.0Mbps - 100.0% 2.0Mbps - 100.0% 5.5Mbps - 100.0% 6.0Mbps - 100.0% 9.0Mbps - 100.0% 11.0Mbps - 100.0% 12.0Mbps - 100.0% 18.0Mbps - 100.0% 24.0Mbps - 77.777% 36.0Mbps - 22.222% 48.0Mbps - 0.0% 54.0Mbps - 0.0%
Current	23.294Mbps	1.0Mbps - 100.0% 2.0Mbps - 100.0% 5.5Mbps - 100.0% 6.0Mbps - 100.0% 9.0Mbps - 100.0% 11.0Mbps - 100.0% 12.0Mbps - 100.0% 18.0Mbps - 100.0% 24.0Mbps - 77.777% 36.0Mbps - 22.222% 48.0Mbps - 0.0% 54.0Mbps - 0.0%

Re-evaluate <- Click to evaluate the current performance of the selected floor

Current->Base <- Click to make the Current data the Base for future comparisons

- Administrator establishes performance baselines for network and performance degradation thresholds
- AP Radio Scan, Client Walkabout, Radio Monitoring provide continuous RF characterization updates
- Performance degradations that cross the defined threshold generates a fault and the RPG subsystem can be used to generate new power, channel, and beacon interval settings to re-optimize WLAN performance

Location Manager



Radio Band: All

Unknown Radios: None

Coverage Display: None

- All Locations
  - Building N
    - Floor 1
      - ap1200ag-B8
      - ap1210ag-B10
      - ap1210ag-B9
      - ap1200g

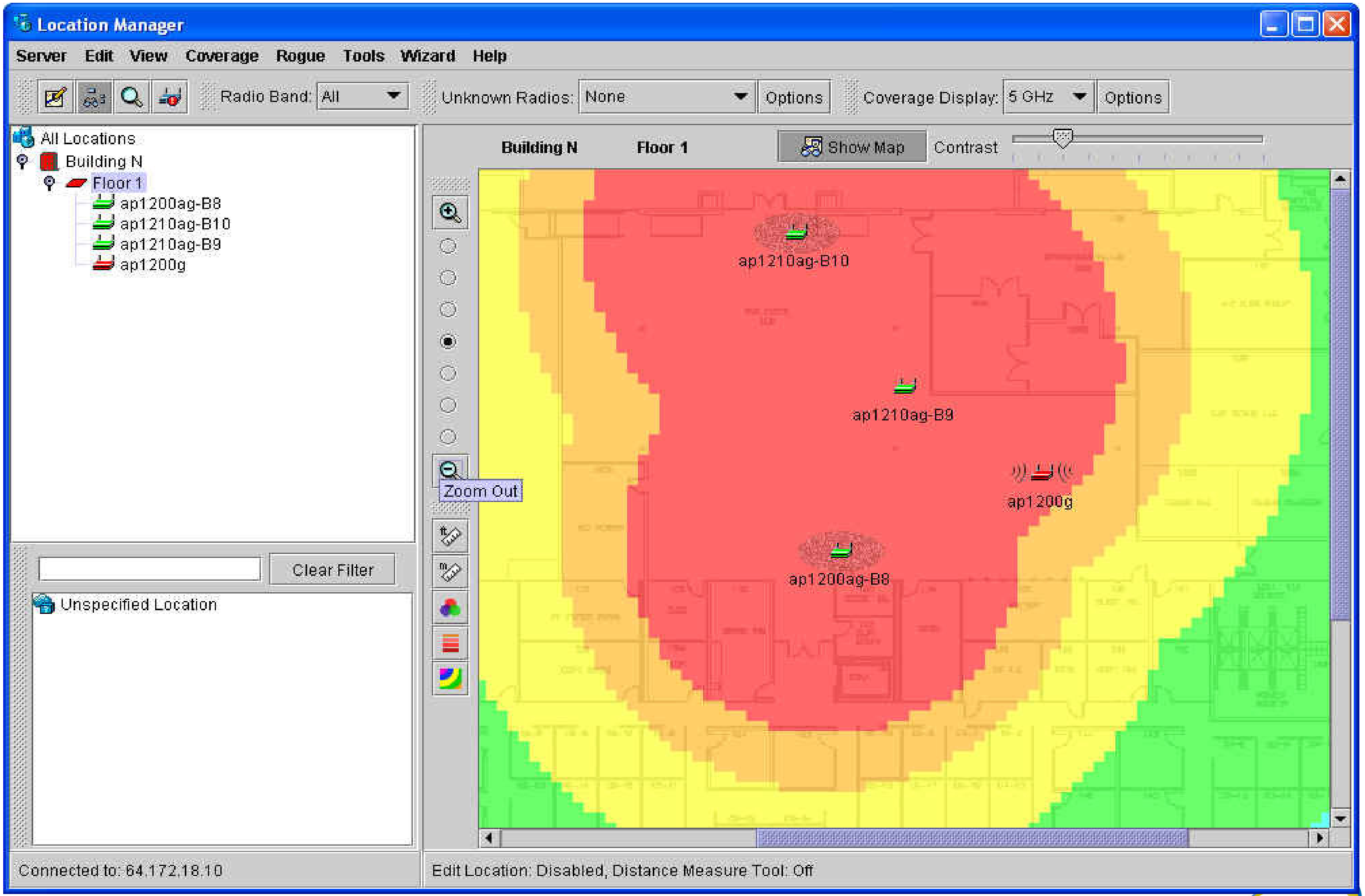
Unspecified Location

Connected to: 64.172.18.10

Edit Location: Disabled, Distance Measure Tool: Off

- **Per Floor Visualization**
  - –AP Location
  - –AP RF Settings Display—Channel, Frequency, Data Rate
  - –Coverage display by data rate, signal strength
- **Launch point for other RF Tools**

Location Manager: Coverage Display



Radio Band: All

Unknown Radios: None

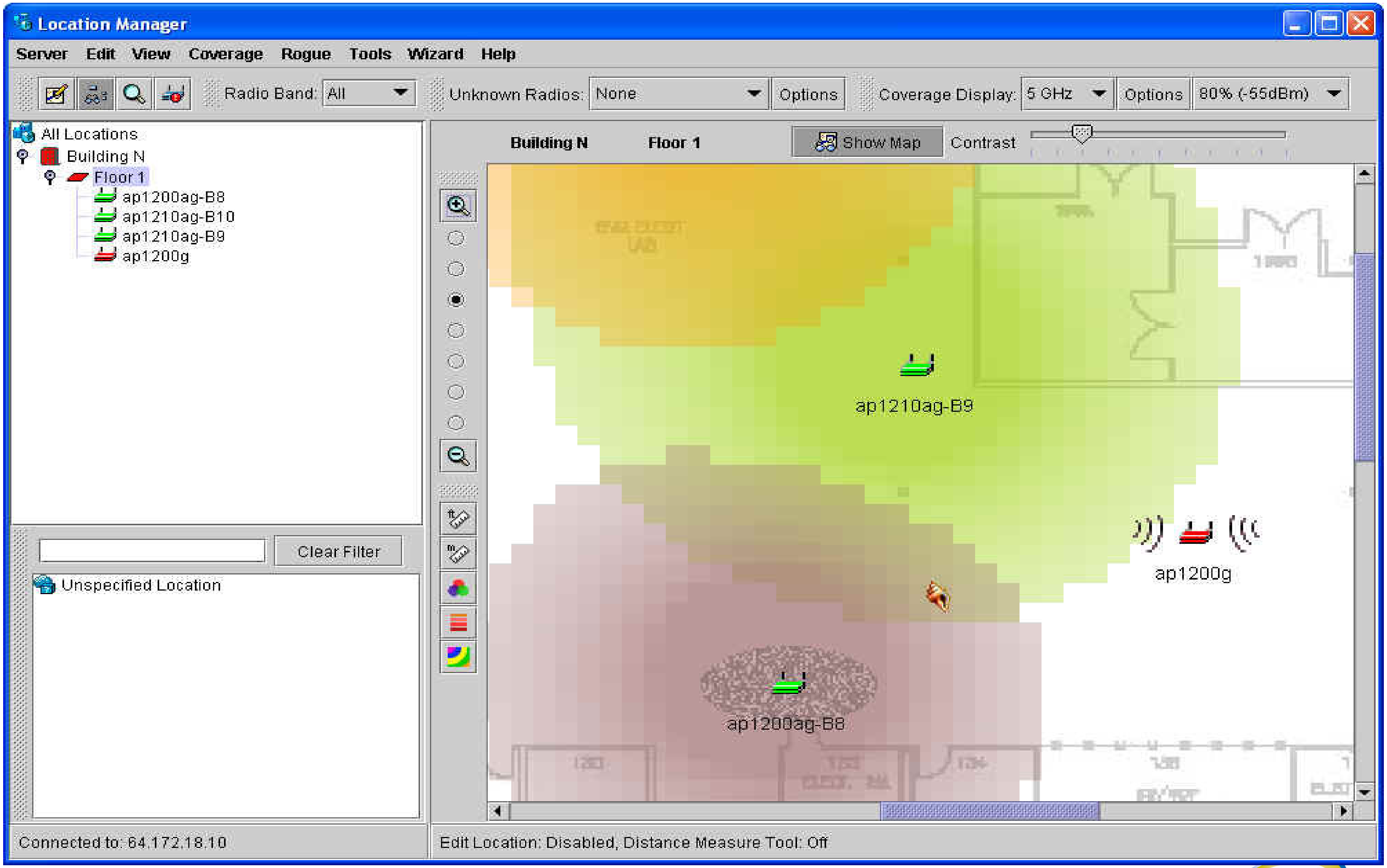
Coverage Display: 5 GHz

Connected to: 64.172.18.10

Edit Location: Disabled, Distance Measure Tool: Off

Note: Coverage display is shown by data rates

Location Manager: Coverage Display

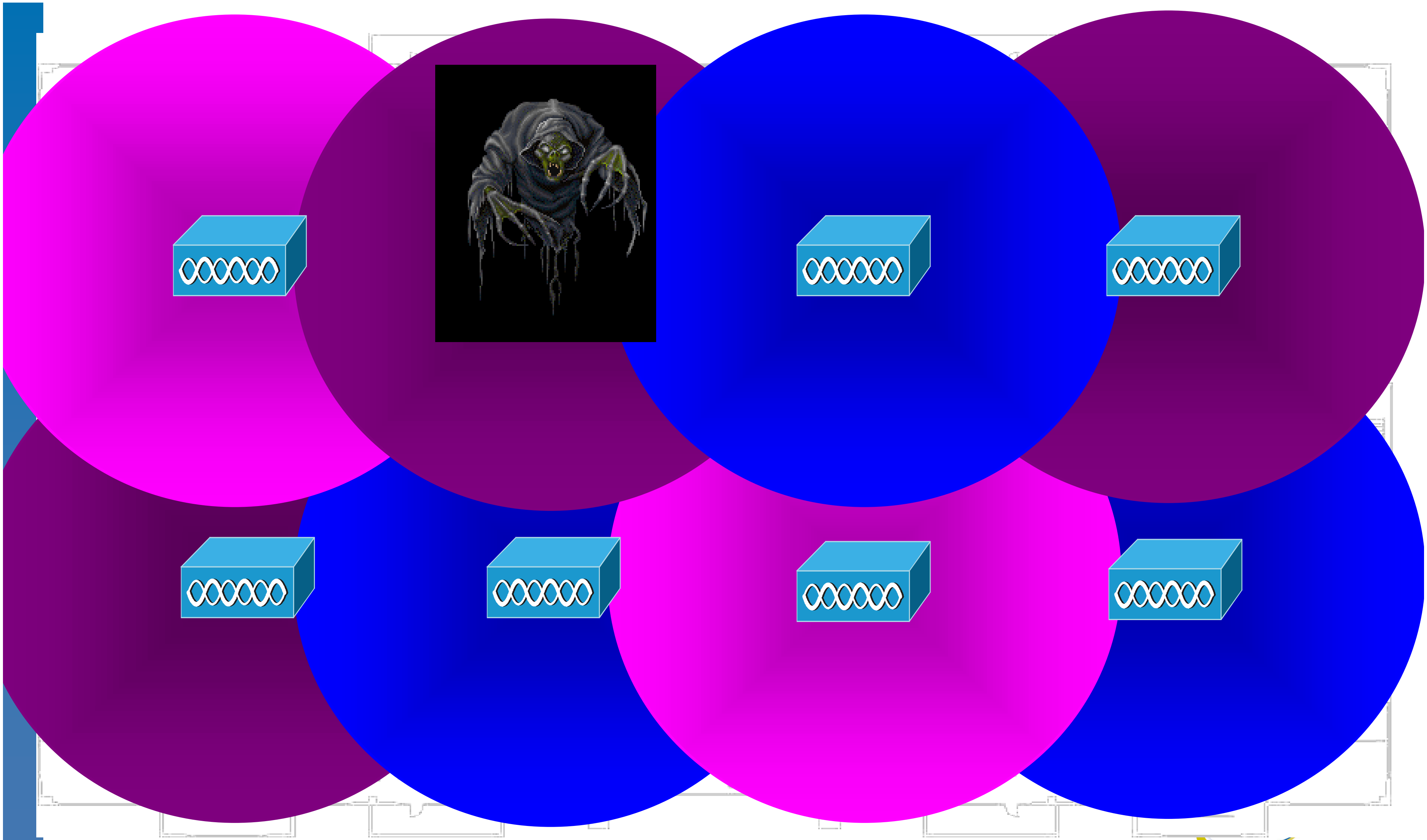


Connected to: 64.172.18.10

Edit Location: Disabled, Distance Measure Tool: Off

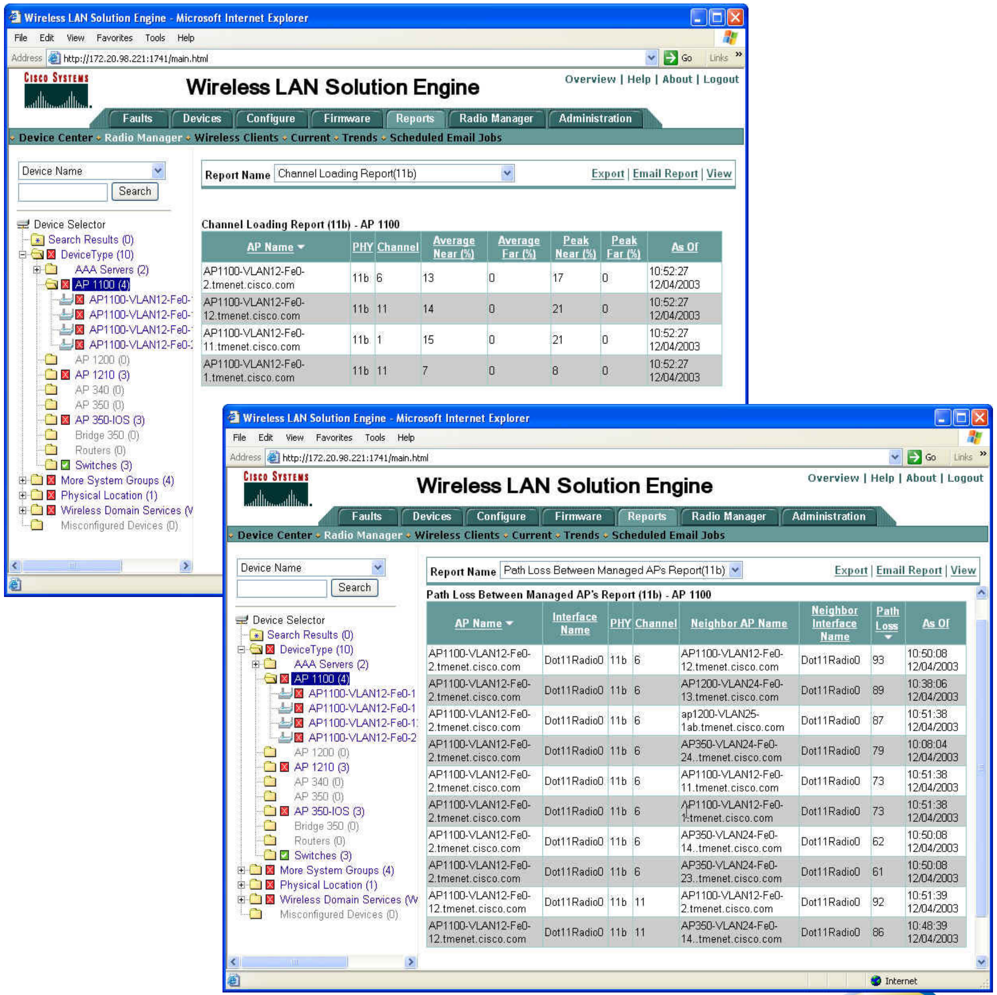
Note: Coverage display is shown by signal strength

Self-Healing



Radio Network Reports

- Radio configuration—inventory style reports
- Key reports that help understand the RF environment characteristics:
  - Path loss between APs
  - Channel Loading



Wireless LAN Solution Engine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://172.20.98.221:1741/main.html
Wireless LAN Solution Engine
Overview | Help | About | Logout
Faults Devices Configure Firmware Reports Radio Manager Administration
Device Center • Radio Manager • Wireless Clients • Current • Trends • Scheduled Email Jobs
Device Name
Search
Device Selector
Search Results (0)
DeviceType (10)
AAA Servers (2)
AP 1100 (4)
AP 1200 (0)
AP 1210 (3)
AP 340 (0)
AP 350 (0)
AP 350-IOS (3)
Bridge 350 (0)
Routers (0)
Switches (3)
More System Groups (4)
Physical Location (1)
Wireless Domain Services
Misconfigured Devices (0)
Export | Email Report | View
Internet

Report Name: Channel Loading Report(11b)

Channel Loading Report (11b) - AP 1100

AP Name	PHY	Channel	Average Near (%)	Average Far (%)	Peak Near (%)	Peak Far (%)	As Of
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	11b	6	13	0	17	0	10:52:27 12/04/2003
AP1100-VLAN12-Fe0-12.tmenet.cisco.com	11b	11	14	0	21	0	10:52:27 12/04/2003
AP1100-VLAN12-Fe0-11.tmenet.cisco.com	11b	1	15	0	21	0	10:52:27 12/04/2003
AP1100-VLAN12-Fe0-1.tmenet.cisco.com	11b	11	7	0	8	0	10:52:27 12/04/2003

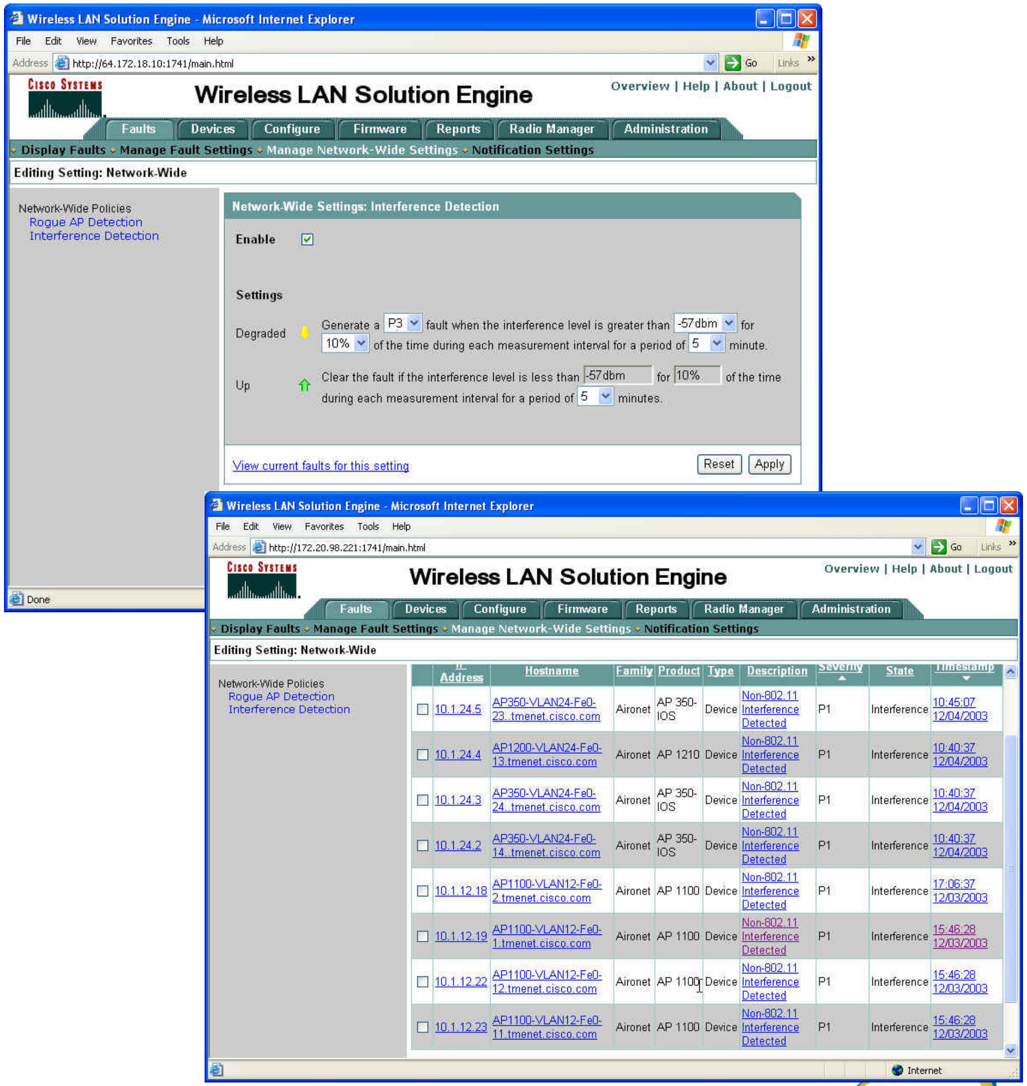
Report Name: Path Loss Between Managed APs Report(11b)

Path Loss Between Managed AP's Report (11b) - AP 1100

AP Name	Interface Name	PHY	Channel	Neighbor AP Name	Neighbor Interface Name	Path Loss	As Of
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP1100-VLAN12-Fe0-12.tmenet.cisco.com	Dot11Radio0	93	10:50:08 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP1200-VLAN24-Fe0-13.tmenet.cisco.com	Dot11Radio0	89	10:38:06 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	ap1200-VLAN25-1ab.tmenet.cisco.com	Dot11Radio0	87	10:51:38 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP350-VLAN24-Fe0-24..tmenet.cisco.com	Dot11Radio0	79	10:08:04 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP1100-VLAN12-Fe0-11.tmenet.cisco.com	Dot11Radio0	73	10:51:38 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP1100-VLAN12-Fe0-1.tmenet.cisco.com	Dot11Radio0	73	10:51:38 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP350-VLAN24-Fe0-14..tmenet.cisco.com	Dot11Radio0	62	10:50:08 12/04/2003
AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	11b	6	AP350-VLAN24-Fe0-23..tmenet.cisco.com	Dot11Radio0	61	10:50:08 12/04/2003
AP1100-VLAN12-Fe0-12.tmenet.cisco.com	Dot11Radio0	11b	11	AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Dot11Radio0	92	10:51:39 12/04/2003
AP1100-VLAN12-Fe0-12.tmenet.cisco.com	Dot11Radio0	11b	11	AP350-VLAN24-Fe0-14..tmenet.cisco.com	Dot11Radio0	86	10:48:39 12/04/2003

Non-802.11 Interference Detection

- Customizable noise floor threshold
- Fault generated when non-802.11 interference detected
- Critical to understanding interference that degrades WLAN performance


Wireless LAN Solution Engine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://64.172.18.10:1741/main.html
Go Links
Cisco Systems
Wireless LAN Solution Engine
Overview | Help | About | Logout
Faults Devices Configure Firmware Reports Radio Manager Administration
Display Faults · Manage Fault Settings · Manage Network-Wide Settings · Notification Settings
Network-Wide Policies
Rogue AP Detection
Interference Detection
Done

Editing Setting: Network-Wide

Network-Wide Settings: Interference Detection

Enable ☑

Settings

Degraded: Generate a P3 fault when the interference level is greater than -57dbm for 10% of the time during each measurement interval for a period of 5 minute.

Up: Clear the fault if the interference level is less than -57dbm for 10% of the time during each measurement interval for a period of 5 minutes.

View current faults for this setting

Reset Apply

Wireless LAN Solution Engine - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://172.20.98.221:1741/main.html
Go Links
Cisco Systems
Wireless LAN Solution Engine
Overview | Help | About | Logout
Faults Devices Configure Firmware Reports Radio Manager Administration
Display Faults · Manage Fault Settings · Manage Network-Wide Settings · Notification Settings
Network-Wide Policies
Rogue AP Detection
Interference Detection
Internet

Editing Setting: Network-Wide

	IP Address	Hostname	Family	Product	Type	Description	Severity	State	Timestamp
□	10.1.24.5	AP350-VLAN24-Fe0-23..tmenet.cisco.com	Aironet	AP 350-IOS	Device	Non-802.11 Interference Detected	P1	Interference	10:45:07 12/04/2003
□	10.1.24.4	AP1200-VLAN24-Fe0-13.tmenet.cisco.com	Aironet	AP 1210	Device	Non-802.11 Interference Detected	P1	Interference	10:40:37 12/04/2003
□	10.1.24.3	AP350-VLAN24-Fe0-24..tmenet.cisco.com	Aironet	AP 350-IOS	Device	Non-802.11 Interference Detected	P1	Interference	10:40:37 12/04/2003
□	10.1.24.2	AP350-VLAN24-Fe0-14..tmenet.cisco.com	Aironet	AP 350-IOS	Device	Non-802.11 Interference Detected	P1	Interference	10:40:37 12/04/2003
□	10.1.12.18	AP1100-VLAN12-Fe0-2.tmenet.cisco.com	Aironet	AP 1100	Device	Non-802.11 Interference Detected	P1	Interference	17:06:37 12/03/2003
□	10.1.12.19	AP1100-VLAN12-Fe0-1.tmenet.cisco.com	Aironet	AP 1100	Device	Non-802.11 Interference Detected	P1	Interference	15:46:28 12/03/2003
□	10.1.12.22	AP1100-VLAN12-Fe0-12.tmenet.cisco.com	Aironet	AP 1100	Device	Non-802.11 Interference Detected	P1	Interference	15:46:28 12/03/2003
□	10.1.12.23	AP1100-VLAN12-Fe0-11.tmenet.cisco.com	Aironet	AP 1100	Device	Non-802.11 Interference Detected	P1	Interference	15:46:28 12/03/2003

Key Radio Management Points

- WLANs present new management challenges due to physics of radio
- Cisco Systems offers an innovative, cost-effective solution—the Cisco Structured Wireless Aware Network, featuring CiscoWorks Wireless LAN Solution Engine (WLSE)—to address these management challenges
- WLSE Radio Management Features
  - Location Manager—WLAN network visualization and centralized control
  - Assisted Site Survey—Lower deployment and operational costs, optimal WLAN configuration for maximum performance and end-user productivity
  - Rogue AP Detection—Comprehensive WLAN security and intrusion detection
  - Radio Network Reports—Characterization of RF environment for maximum network performance
  - Non-802.11 Interference Detection—Find and mitigate against sources of network performance degradation

Agenda

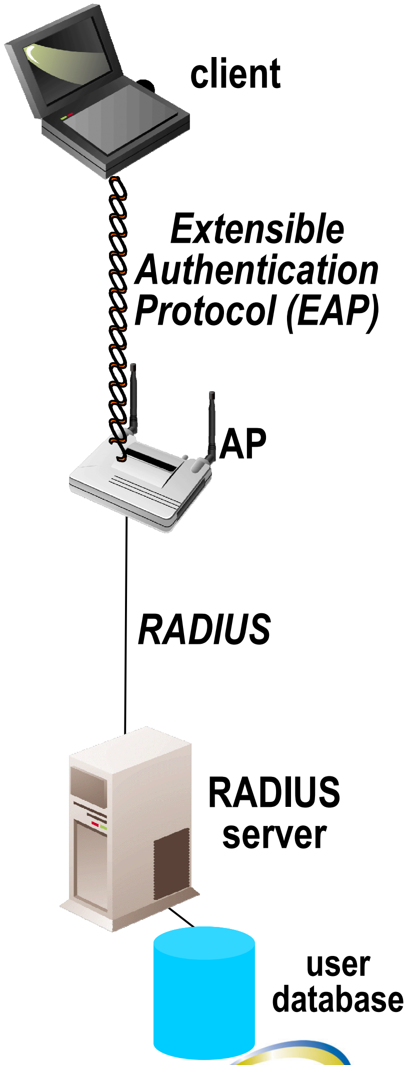
- Deployment Criteria
- Cisco's SWAN Solution
- 802.11a/b/g Technologies
- Centralized Network and RF (i.e. "Air") Management
- **802.11 Security**
- Wired/Wireless Integration
- Summary

Basic Requirements to Secure Wireless LANs

- Encryption algorithm
  - Mechanism to provide data privacy
- Message integrity
  - Ensures data frames are tamper free and truly from the source address
- Authentication framework
  - Framework to facilitate authentication messages between clients, access point, and AAA server
- Authentication algorithm
  - Mechanism to validate client credentials

802.1X Authentication Overview

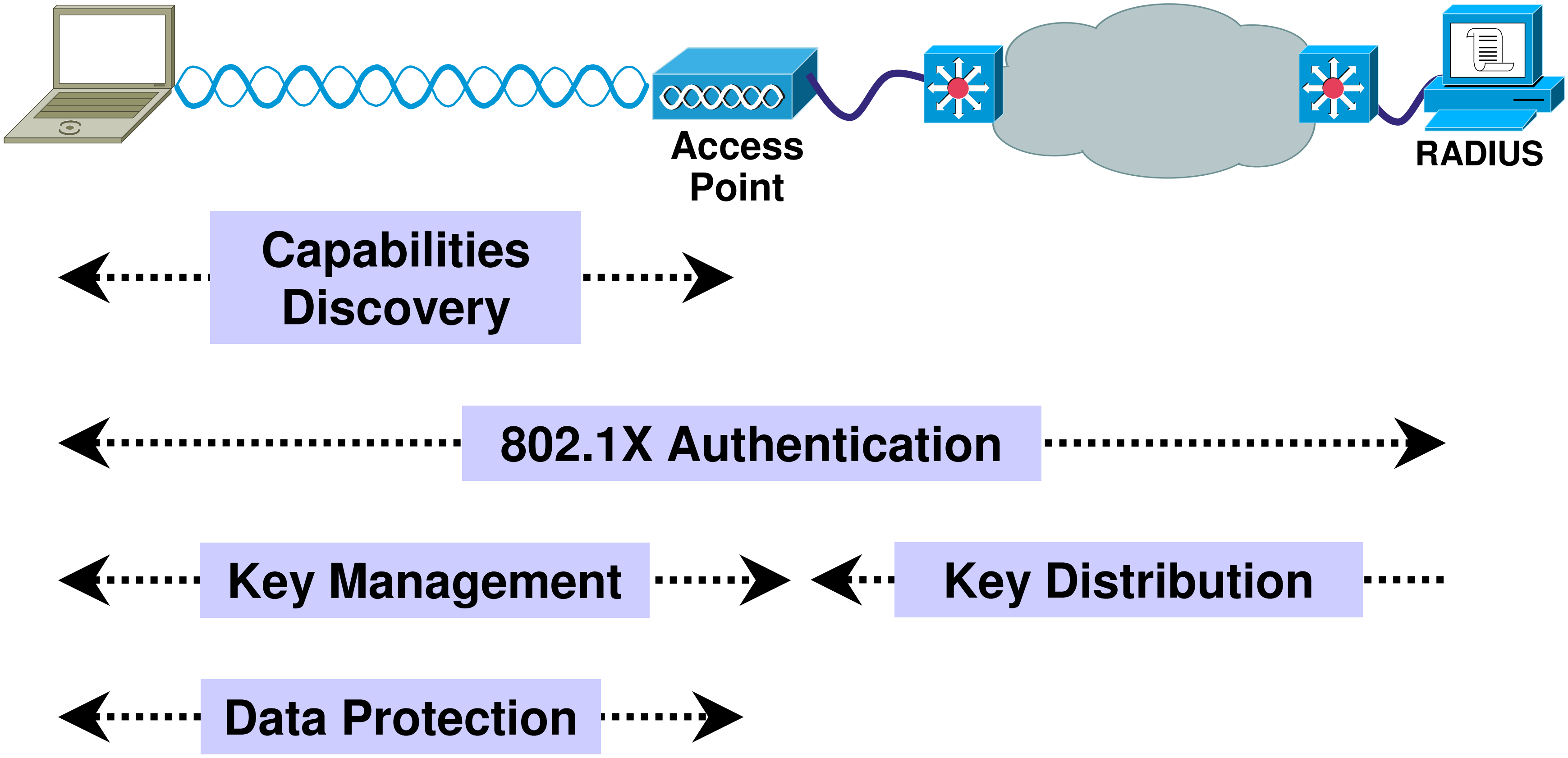
- IEEE 802.11 Task Group i recommendation for WLAN authentication
- Supported by Cisco since December 2000
- Extensible and Interoperable—Supports:
  - –Different EAP authentication methods or types
  - –New encryption algorithms, including AES as a replacement for RC4
- Key benefits
  - –Mutual authentication between client and authentication (RADIUS) server
  - –Encryption keys derived after authentication
  - –Centralized policy control to restrict user access based on user-groups



IEEE 802.11i (WLAN Security) Improvements

- 802.11i is an IEEE 802.11 subcommittee responsible for WLAN Security Improvements
- Key Components of IEEE 802.11i standard are:
  - EAP/802.1x framework based User Authentication
  - TKIP: Mitigate RC4 key scheduling vulnerability and active attack vulnerabilities
  - IV Expansion: 48-bit IVs
  - Key Management: Isolate Encryption key management from user authentication
  - AES: Long term replacement protocol for RC4 (WEP)
- WPA is the Wi-Fi Alliance (WFA) inclusion of 802.11i Security Recommendations

802.11i/WPA Authentication and Key Management Overview

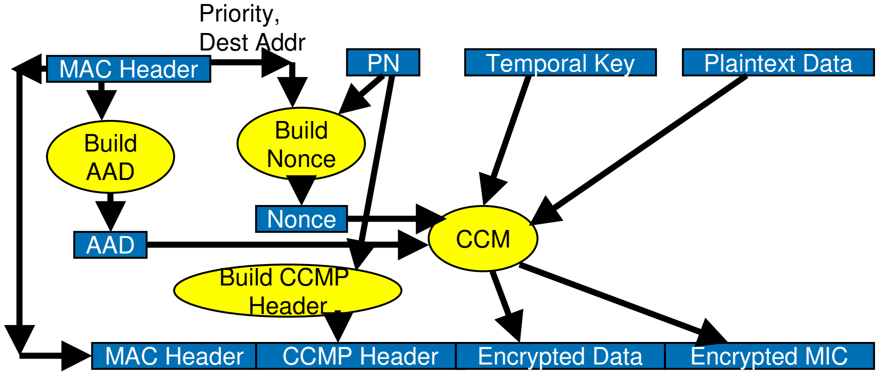


Wi-Fi Protected Access (WPA)

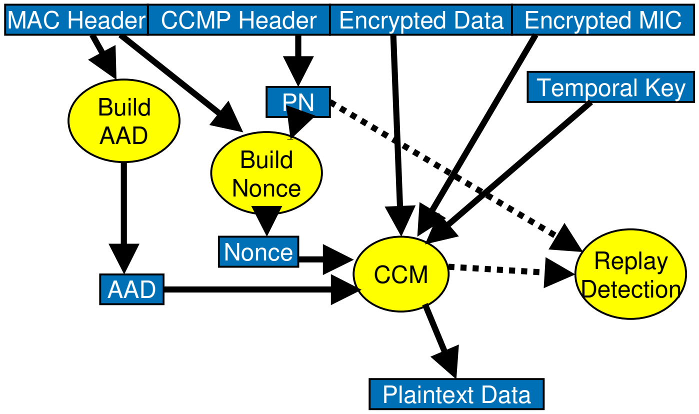
- Components of WPA:
  - Authenticated key management using 802.1X:
    - EAP authentication and Pre-Shared Key (PSK) authentication
  - TKIP: Per-Packet Keying and Message Integrity Check (MIC)
  - Unicast and broadcast key management
  - IV expansion: 48-bit IVs
- Cisco's support for WPA:
  - AP1200 and AP350 (IOS only) and AP1100
  - Cisco 350, CB20A, CB21AG/PI21AG, CCXv2 Clients
- Client support for WPA requires Host-level supplicant
  - Note: Host-level supplicant is required for key management function whereas TKIP functionality is implemented at the NIC driver/firmware level

WPAv2 Description

- A Key component of WPAv2 is Advanced Encryption Standard (AES) support
  - 128-bit AES-CCM (CCM is Counter Mode for confidentiality and CBC-MAC mode for integrity) to be supported in WPA2
- Optimized 4-way handshake to establish PTK and distribute GTK



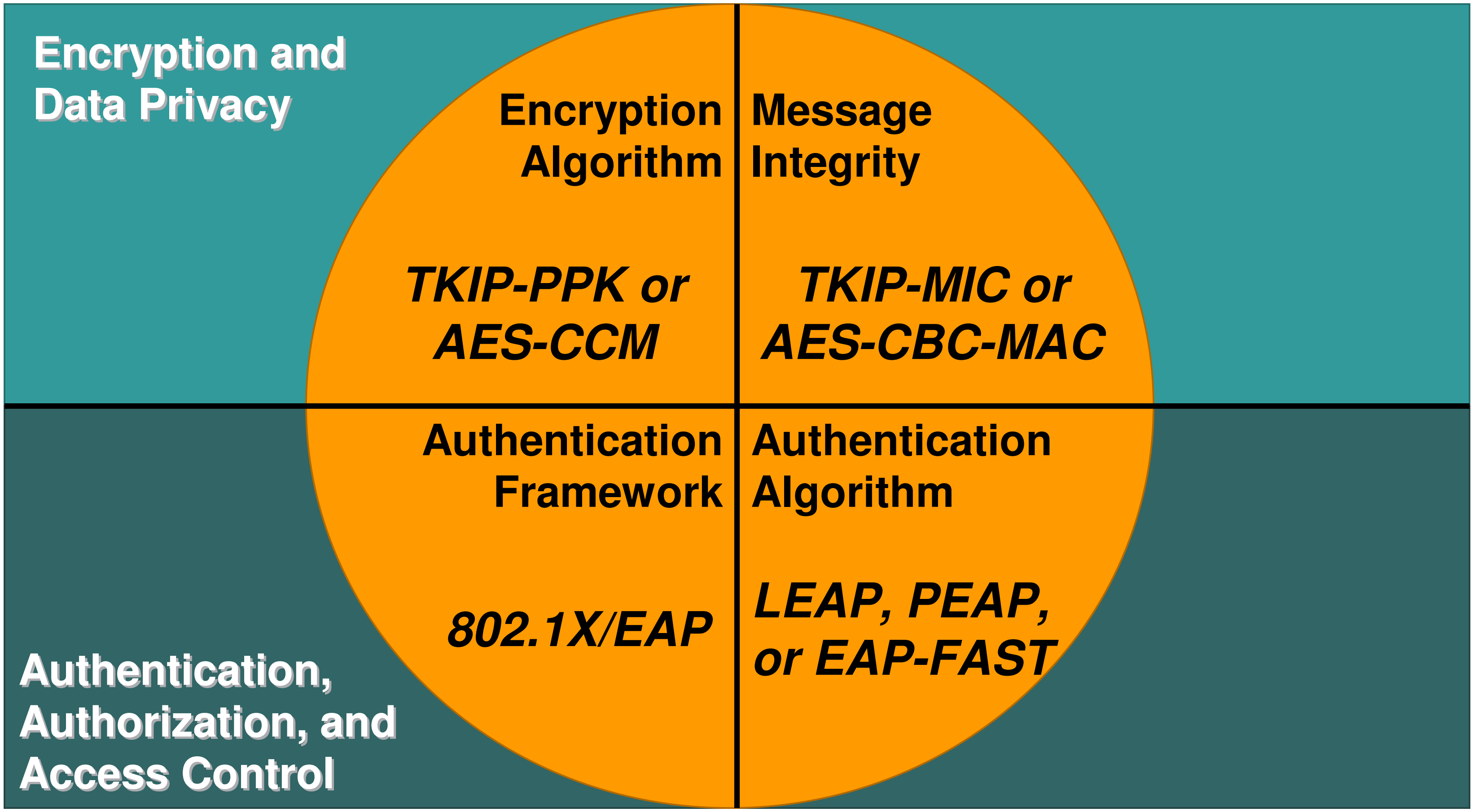
CCMP Encapsulation



CCMP Decapsulation

HP WORLD 2004
Solutions and Technology Conference & Expo

Basic Requirements to Secure Wireless LANs



Encryption and Data Privacy

Encryption Algorithm

TKIP-PPK or AES-CCM

Message Integrity

TKIP-MIC or AES-CBC-MAC

Authentication Framework

802.1X/EAP

Authentication Algorithm

LEAP, PEAP, or EAP-FAST

Authentication, Authorization, and Access Control

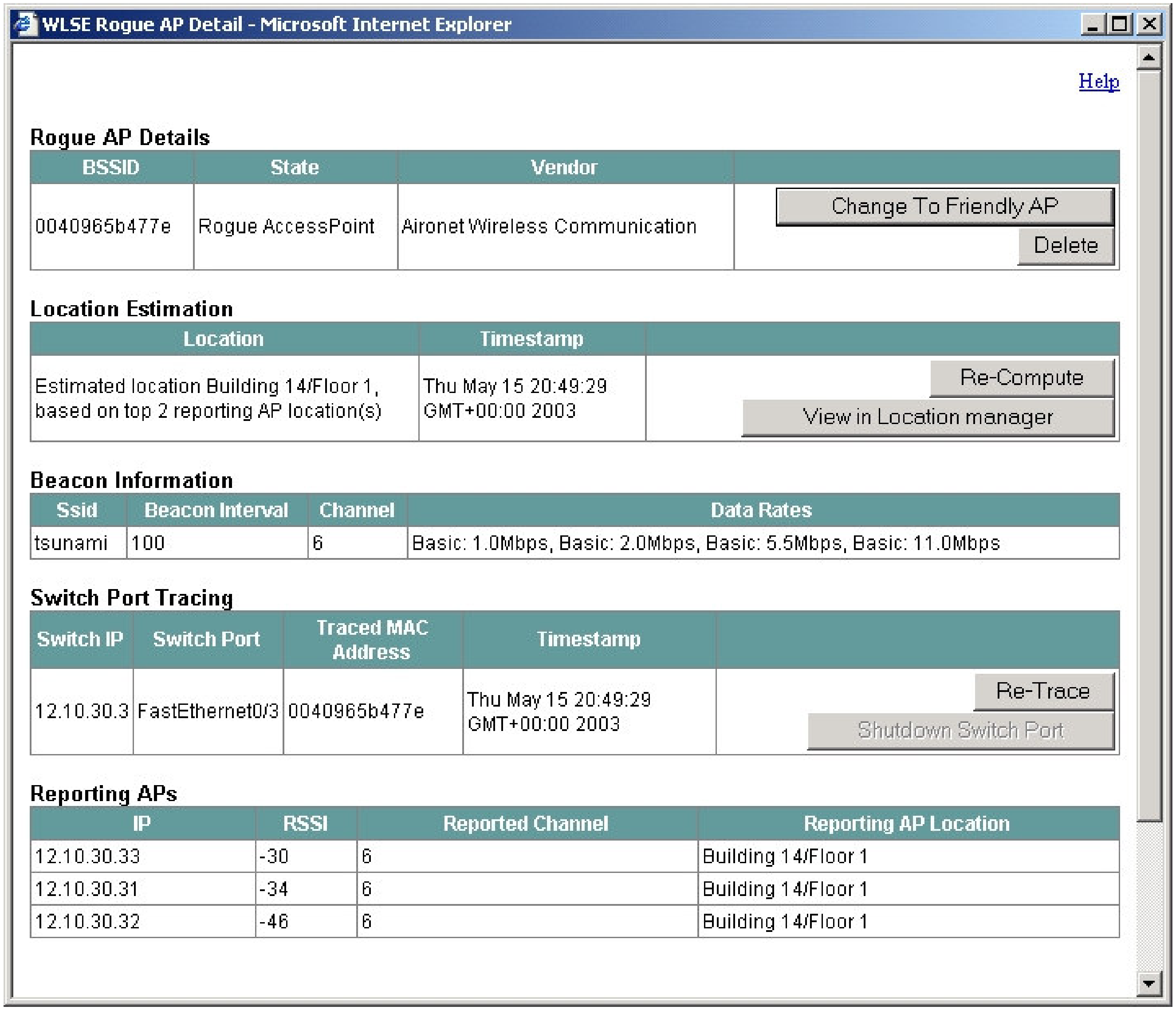
Advanced Requirements to Secure Wireless LANs

- Secure management policies
  - Secure Telnet, SSH, SNMP, FTP, TFTP, RADIUS, and WLCCP traffic to the APs and Bridges
- Wireless IDS
  - Provide capability to detect and suppress unauthorized APs, detect active attacks, and enhance Layer-2 Security
- Wired/Wireless Integration best practices
  - Mapping wireless security policies to the wired network
  - Use of multiple user/device groups (via SSIDs/VLANs/mGRE tunnels)
  - Use of wired security features for wireless lan deployment

Rogue AP Detection and Suppression

- Rogue AP detection methodology
  - APs and clients collect and report BSSID information via beacons and probe responses
  - WLSE compares collected BSSID information versus authorized (i.e. managed APs) BSSID information
  - Unauthorized APs are flagged and reported via faults monitoring functionality
- Rogue AP suppression techniques
  - Administrator is notified location of the rogue AP via location manager; locate the rogue AP and physically remove it!
  - Trace the rogue AP over the wired network and shut-down the switch port!

Cisco Works WLSE:
Rogue AP Details Screen



Rogue AP Details

BSSID	State	Vendor	
0040965b477e	Rogue AccessPoint	Aironet Wireless Communication	Change To Friendly AP Delete

Location Estimation

Location	Timestamp	
Estimated location Building 14/Floor 1, based on top 2 reporting AP location(s)	Thu May 15 20:49:29 GMT+00:00 2003	Re-Compute View in Location manager

Beacon Information

Ssid	Beacon Interval	Channel	Data Rates
tsunami	100	6	Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps

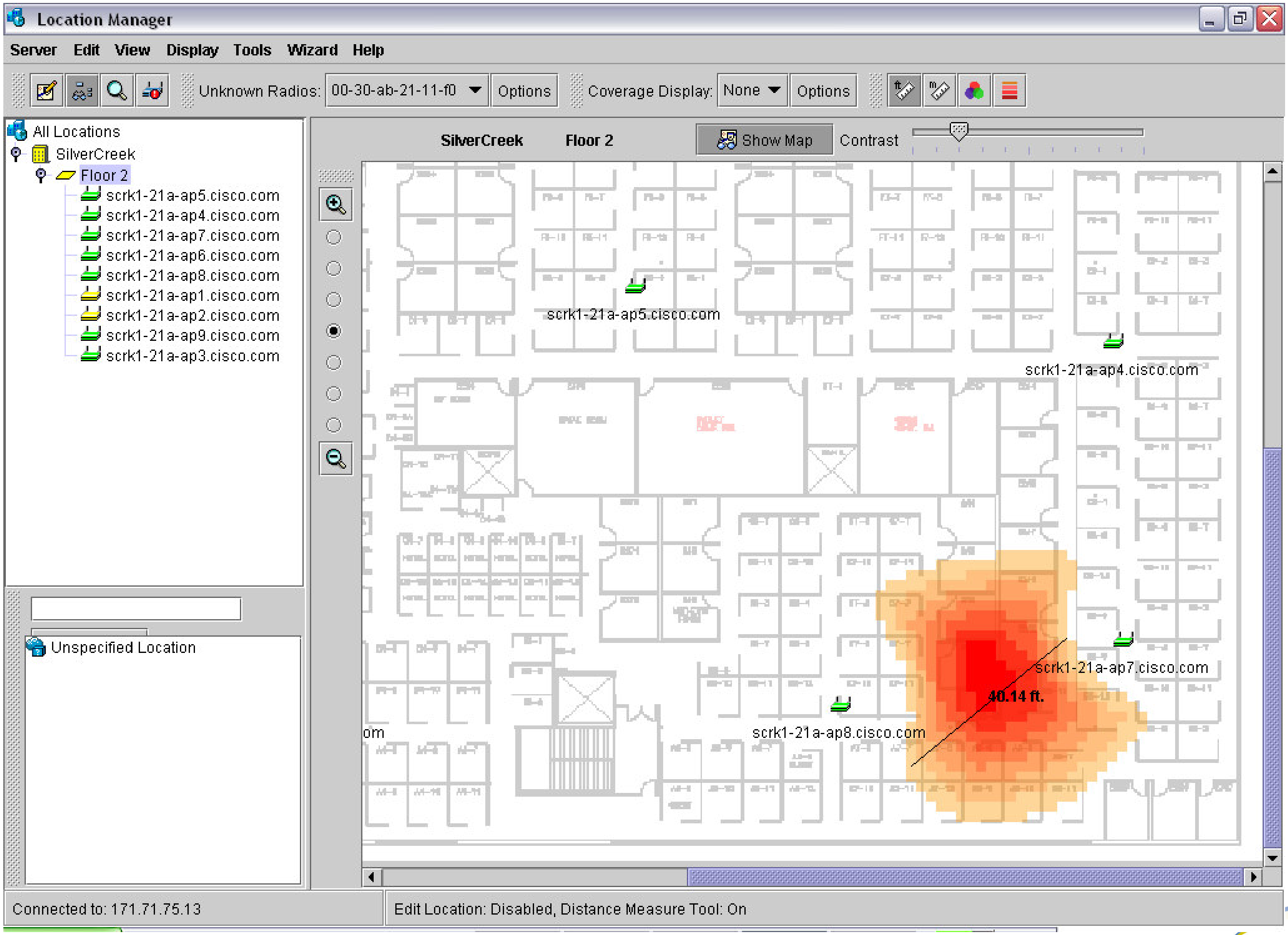
Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
12.10.30.3	FastEthernet0/3	0040965b477e	Thu May 15 20:49:29 GMT+00:00 2003	Re-Trace Shutdown Switch Port

Reporting APs

IP	RSSI	Reported Channel	Reporting AP Location
12.10.30.33	-30	6	Building 14/Floor 1
12.10.30.31	-34	6	Building 14/Floor 1
12.10.30.32	-46	6	Building 14/Floor 1

CiscoWorks WLSE: Location Manager



Connected to: 171.71.75.13

Edit Location: Disabled, Distance Measure Tool: On

Agenda

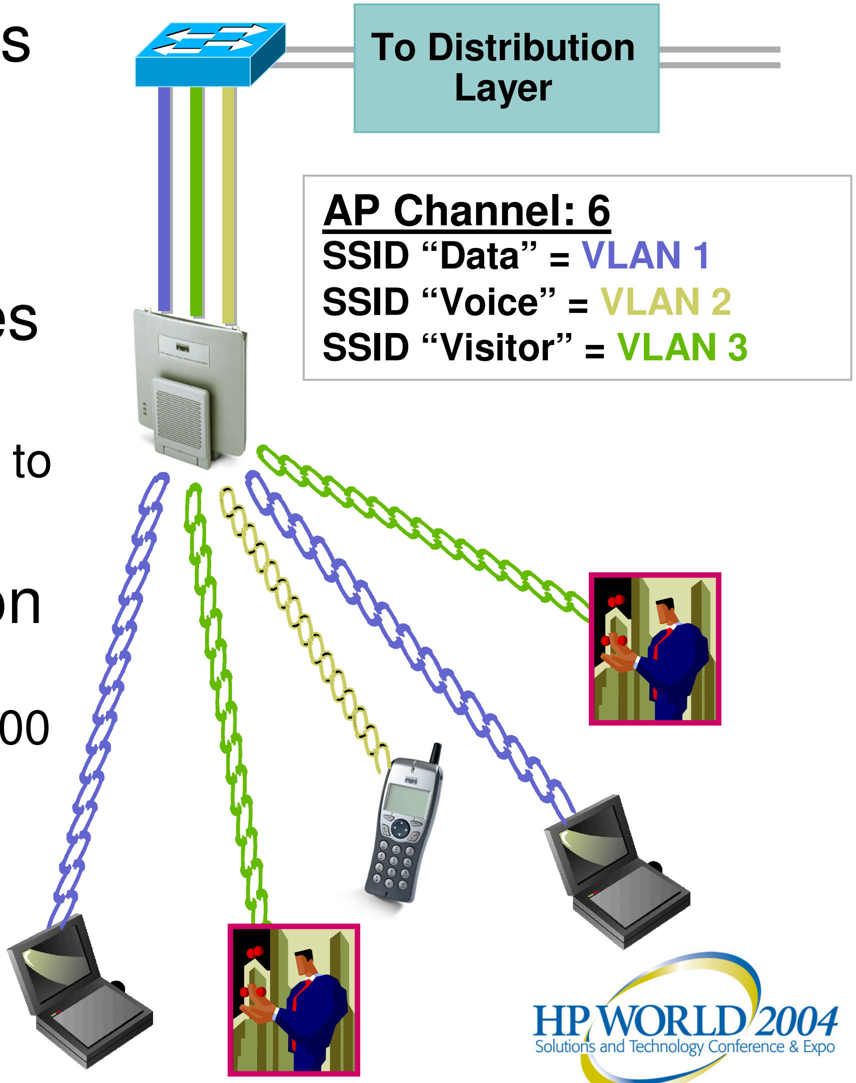
- Deployment Criteria
- Cisco's SWAN Solution
- 802.11a/b/g Technologies
- Centralized Network and RF (i.e. "Air") Management
- 802.11 Security
- **Wired/Wireless Integration**
- Summary

Wired/Wireless Integration Best Practices

- Mapping wireless security policies to the wired network
  - Use of multiple user/device groups (via SSIDs/VLANs/mGRE tunnels)
- Use of wired security features for wireless LAN deployment
- Layer-2/Layer-3 Fast secure roaming
- Catalyst 6500 switch integration
  - Central point of ingress for control and data traffic
  - End-to-end integrated security
  - Fast secure Layer-2/Layer-3 roaming

Mapping Wireless Security Policies to the Wired Network

- Multiple WLAN Security Policies
  - Data vs. voice vs. legacy devices vs. guest access
  - VLAN to SSID mapping
- Mapping WLAN security policies to wired security policies
  - Use L2 to L4 ACLs on the wired side to reinforce WLAN security policies
- Catalyst 6500 WLSM Integration
  - Use 6500 security features on the mGRE interface terminating on the 6500



To Distribution Layer

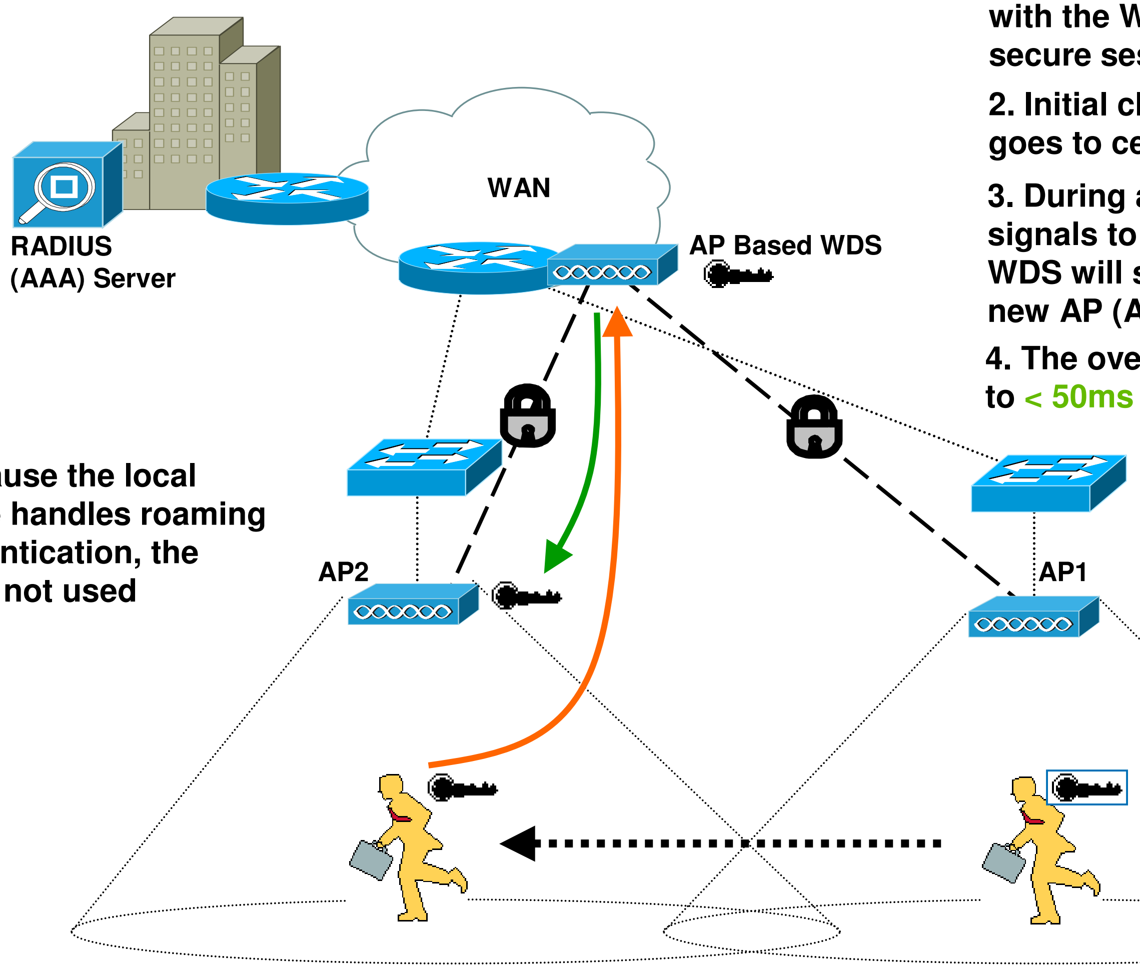
AP Channel: 6

SSID "Data" = VLAN 1

SSID "Voice" = VLAN 2

SSID "Visitor" = VLAN 3

Cisco SWAN: Fast Secure Roaming



1. AP must now 802.1X authenticate with the WDS AP (AP1) to establish a secure session

2. Initial client 802.1X authentication goes to central AAA server (~500ms)

3. During a client roam, the client signals to the WDS it has roamed and WDS will send the clients key to the new AP (AP2)

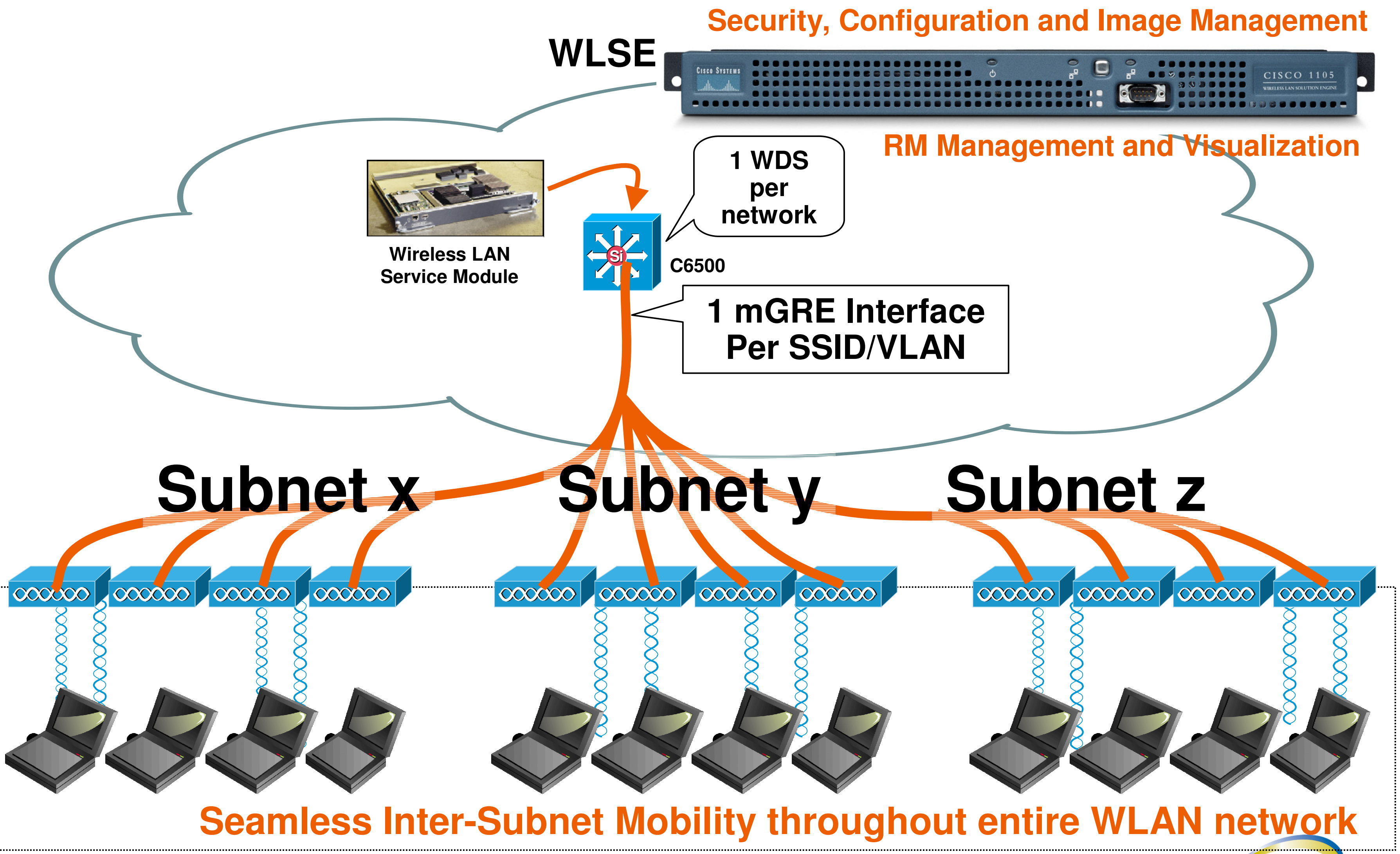
4. The overall handoff time is reduced to < 50ms

NOTE: Because the local WDS device handles roaming and reauthentication, the WAN link is not used

Catalyst 6500 Switch Integration

- Wired/wireless integration enabled with Wireless LAN Service Module (WLSM)
  - One pair of Catalyst 6500 (equipped with WLSMs and Supervisor 720 modules) to enable wireless traffic aggregation
  - NOTE: WLAN traffic aggregation can be enabled at distribution or data-center layer levels
  - Increased WDS scalability for roaming and RF management services
  - Layer-3 Roaming supported
- Central point of ingress for control and data traffic
  - Data traffic is aggregated at the 6500 switch using mGRE tunnels from the APs
    to the Switch
  - mGRE tunnels terminate on the 6500 supervisor (hardware based GRE encapsulation is supported using the Supervisor 720)
  - Control traffic (WLCCP traffic) terminates on the WLSM
- End-to-end integrated security
  - Ability to leverage existing 6500 security features for WLAN user traffic aggregation

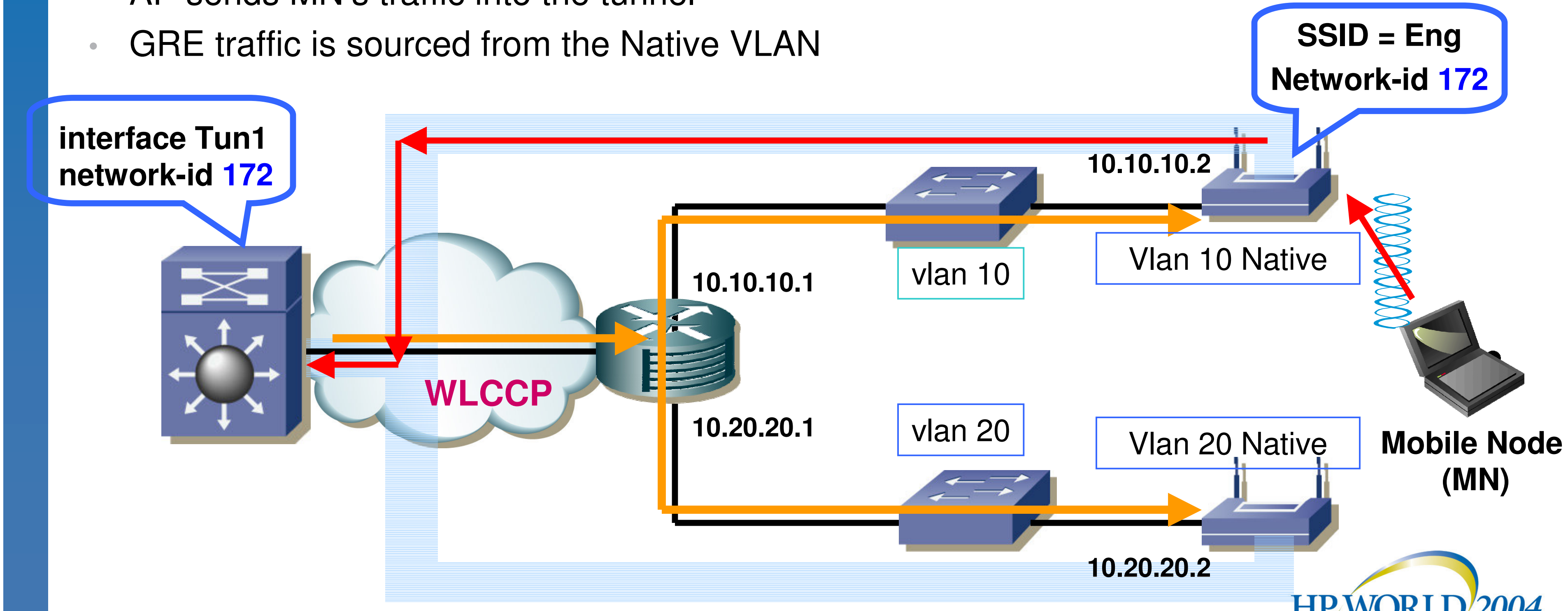
Cisco SWAN Solution: Switch-Based WDS


Security, Configuration and Image Management
WLSE
RM Management and Visualization
1 WDS per network
Wireless LAN Service Module
C6500
1 mGRE Interface Per SSID/VLAN
Subnet x
Subnet y
Subnet z
Seamless Inter-Subnet Mobility throughout entire WLAN network

HP WORLD 2004 Solutions and Technology Conference & Expo

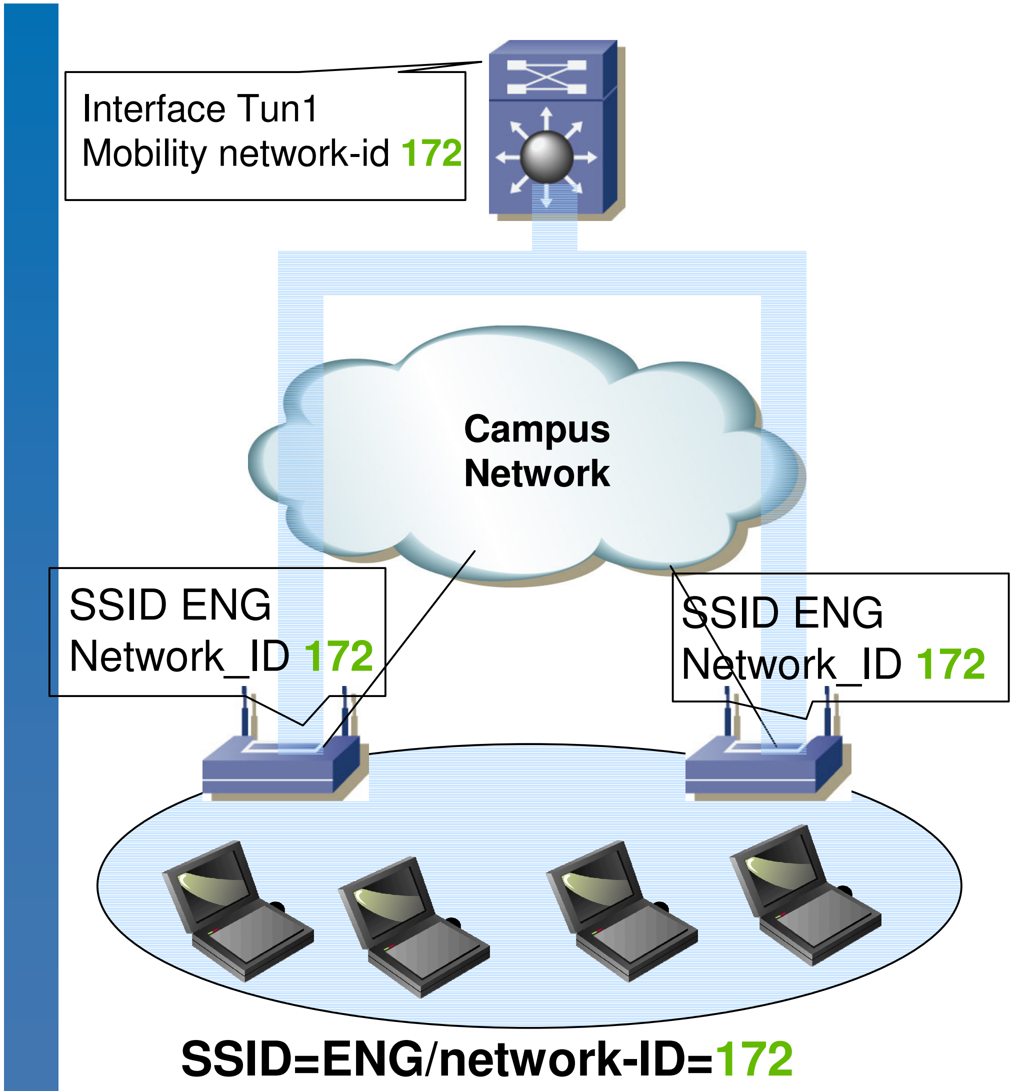
Catalyst 6500 WLSM Overview
How Does It Work?

- Define a Native VLAN on the AP's and Access Switches
- Assign IP address to Access Points
- Define Mobility Group on sup720 and Access Points
- AP's learn the mGRE endpoint through WLCCP
- mGRE tunnel is built
- AP sends MN's traffic into the tunnel
- GRE traffic is sourced from the Native VLAN



Catalyst 6500 WLSM Overview

Mobility Group



MOBILITY GROUP:

- Seamless L3 Mobility is enabled within one Mobility Group
- Identified by SSID/network-ID on the AP. Can be specified also as SSID/VLAN-ID/network-ID if multiple VLANs are enabled locally on the AP
- NOTE: If multiple VLANs are enabled on the AP, no need to span VLANs across the campus network to enable L3 mobility!
- Identified by the Tunnel interface on the sup720
- The same SSID/Network-ID on all the AP's where L3 mobility is required
- One network-ID = one wireless subnet
- Limit of 16 SSID/Network-ID

Catalyst 6500 Security Features

Recommended Catalyst 6500 Security Feature Sets to Consider for Wireless/Wired Integration:

- Layer-2/3/4 ACLs (hardware accelerated support) along with various ACL options (standard, extended, reflexive, and time-based)
- Router ACLs (RACLs)
- TCP Intercept: To stop TCP SYN flooding attacks
- Unicast RPF (URPF) Checks: Mitigate problems caused by malformed or spoofed packets
- RP Rate Limiters: Used to prevent DoS attacks using “bogus” traffic (Example: ICMP ping requests from bogus IP addresses)
- IOS Firewall Feature Set: This is a software feature set that provides support for Authentication Proxy; Port to Application Mapping (PAM) and Content Based Access Control (CBAC)
- Service Module Integration (Firewall, IDS, VPN, and NAM service modules are supported with WLSM)

Agenda

- Deployment Criteria
- Cisco's SWAN Solution
- 802.11a/b/g Technologies
- Centralized Network and RF (i.e. "Air") Management
- 802.11 Security
- Wired/Wireless Integration
- **Summary**

Summary

- Consider BW requirements, client devices, and user applications (example: data Vs VoIP) to select the appropriate 802.11a/b/g technologies
- Scalable and centralized network and RF management matters!
  - Centralized configuration and software management for wireless AP devices
  - Centralized RF management to enable RF monitoring, assisted site-survey, and self-healing functionalities
- Choose standardized 802.11i security to enable user-based authentication and data confidentiality
- Consider Wired/Wireless integration to enable end-to-end security, mobility, and QoS

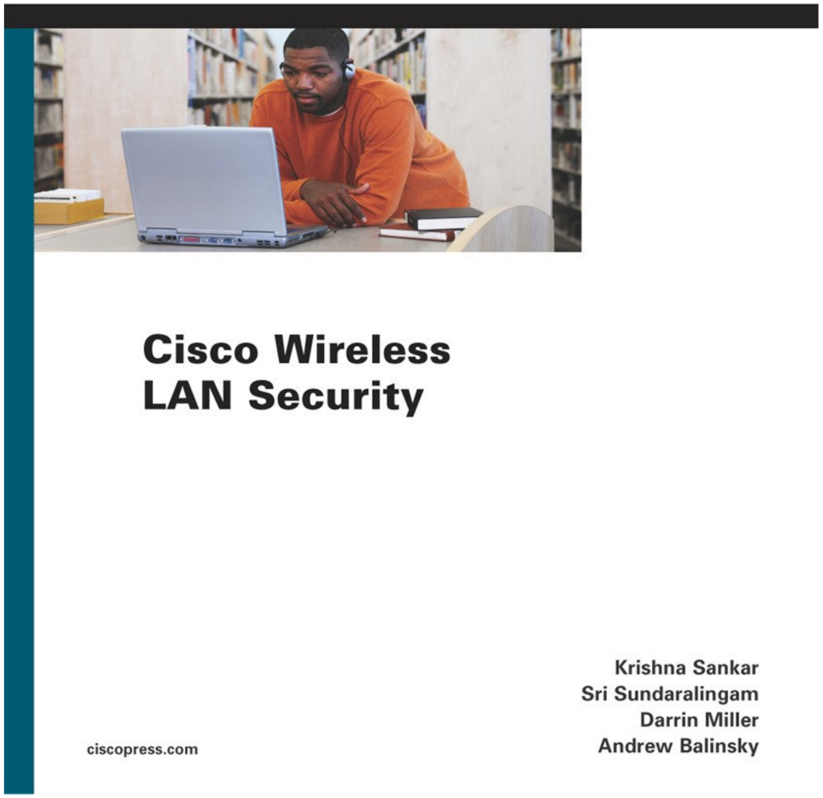
Reference URLs

- Cisco SWAN Web-Site
  - http://www.cisco.com/go/swan
- Cisco Aironet Security Web site
  - http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html
- Latest CCX (Cisco certified clients) Information
  - http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Coming Soon …

Cisco Systems

ISBN: 1587051540



Cisco Wireless LAN Security

Krishna Sankar
Sri Sundaralingam
Darrin Miller
Andrew Balinsky

ciscopress.com

http://ciscopress.com/title/1587051540

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP