An Architectural Approach to Secure Mobility

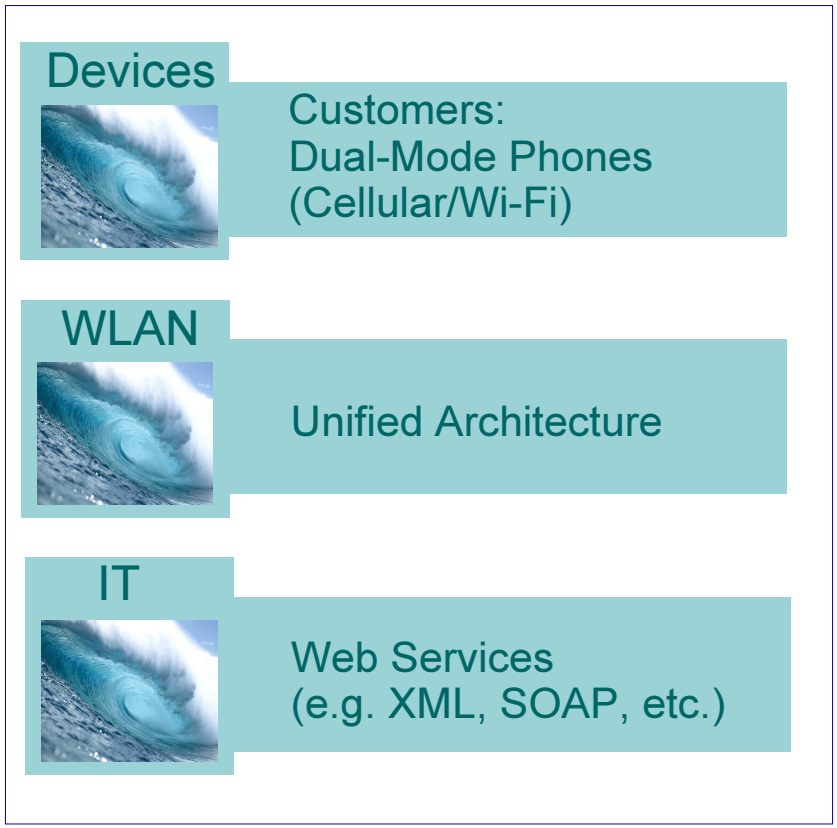
Cisco Technology Solutions 2008

Peter Thomas

Secure Mobility

- An Architectural Approach
- Case Studies
- Wireless Security - what are others doing? Where are we going?
- 802.11n – what is it, and how does it benefit you?

Mobility - Business Relevance



Wi-Fi:
A better B2C medium than TV, print, media, and online

- 1.2 billion Wi-Fi clients will ship by 2010 worldwide

IDC, Dec 2007

Greet Customers as They Walk by Store Premises

Customer away from Store

Mobile Personal Assistant Launcher

Customer Nearby Store

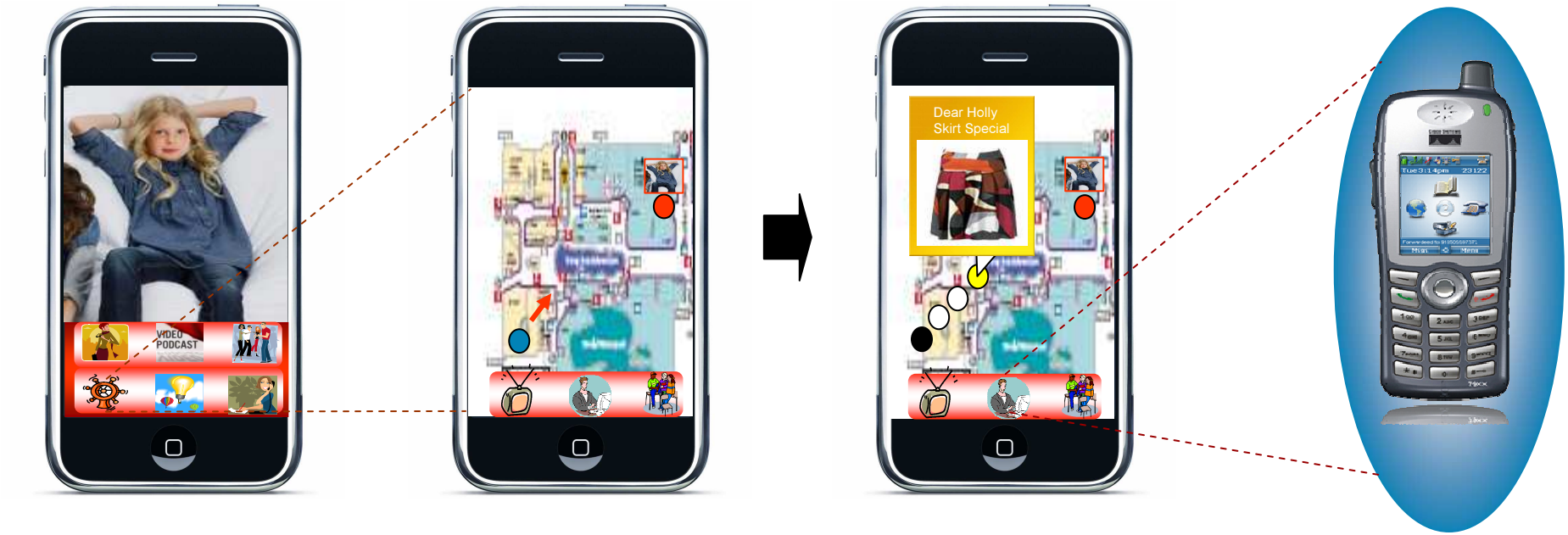
A Better Shopping Experience:

In-Store Concierge

Store Navigator

Smart Ads

Customer Service

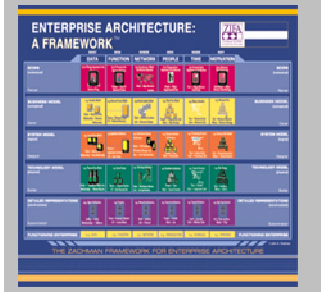


Help Customers Find Items More Easily

An Architectural Approach

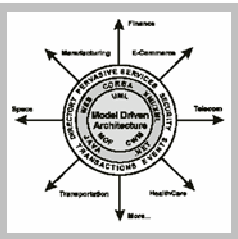
Enterprise Architectures And The Network

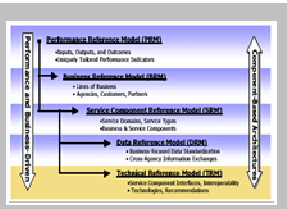
TOGAF



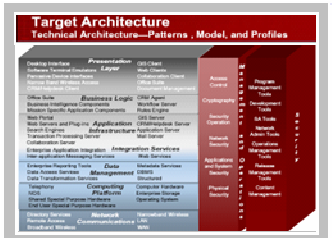
Zachman Framework

IAF - CapGemini



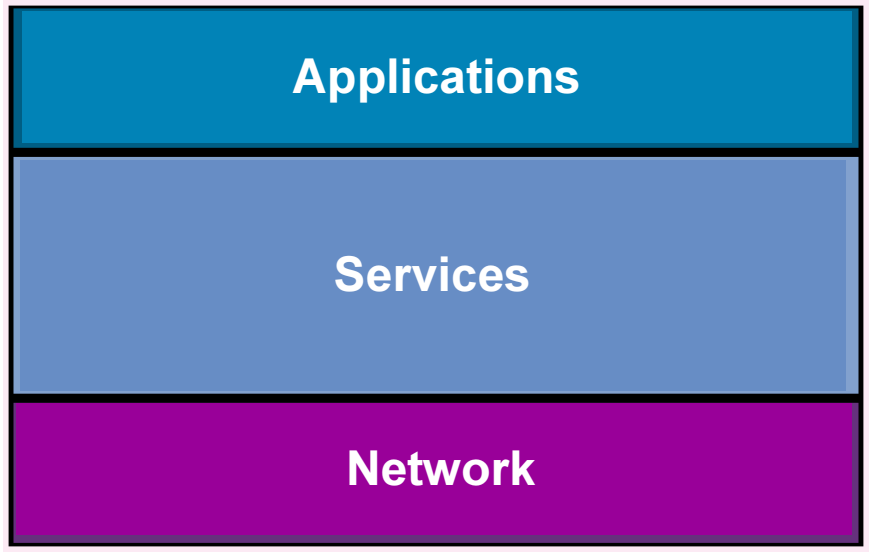


Federal Enterprise Architecture

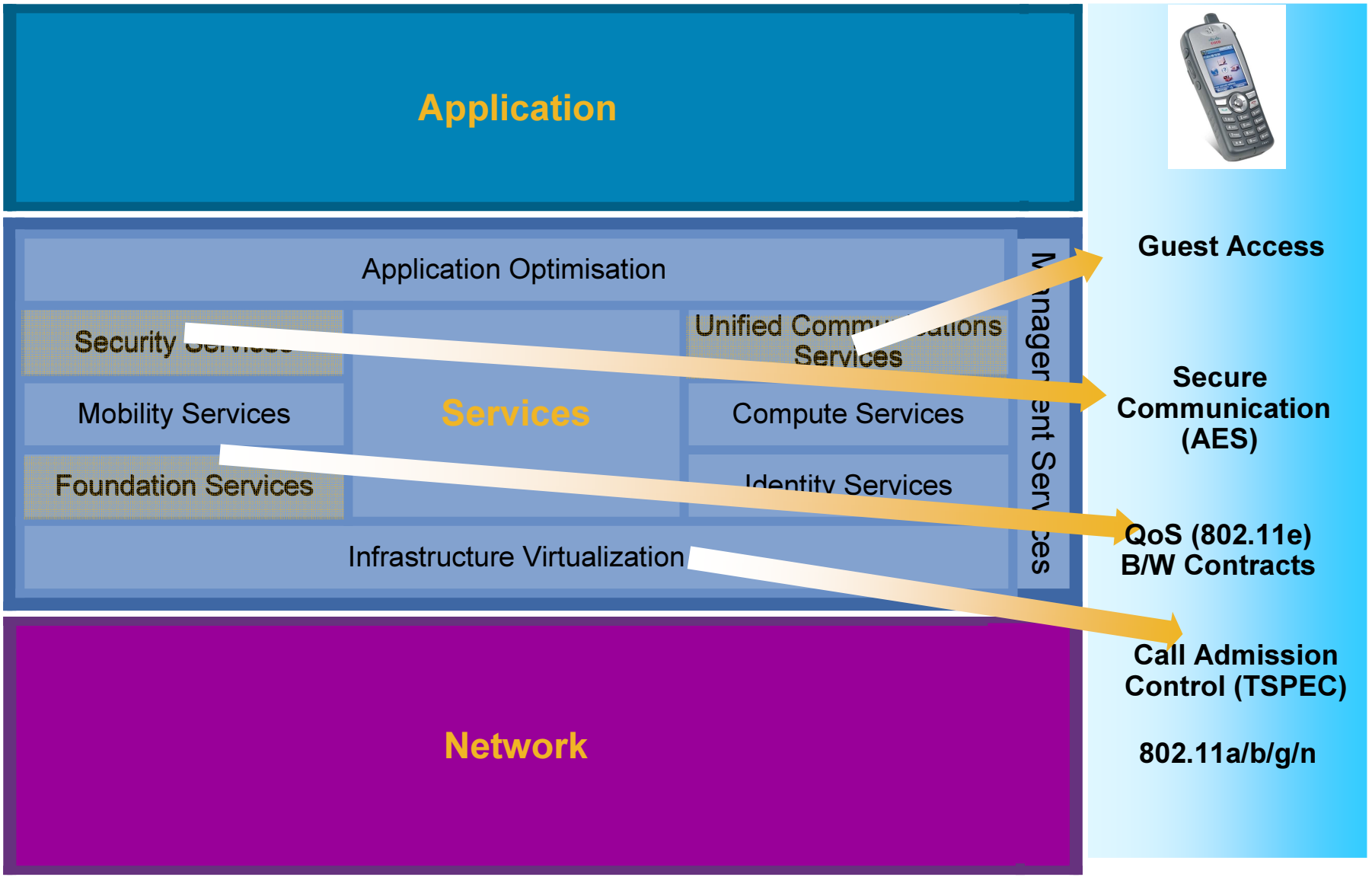


Homeland Security

More than Just Connectivity



The Network as The Platform for …

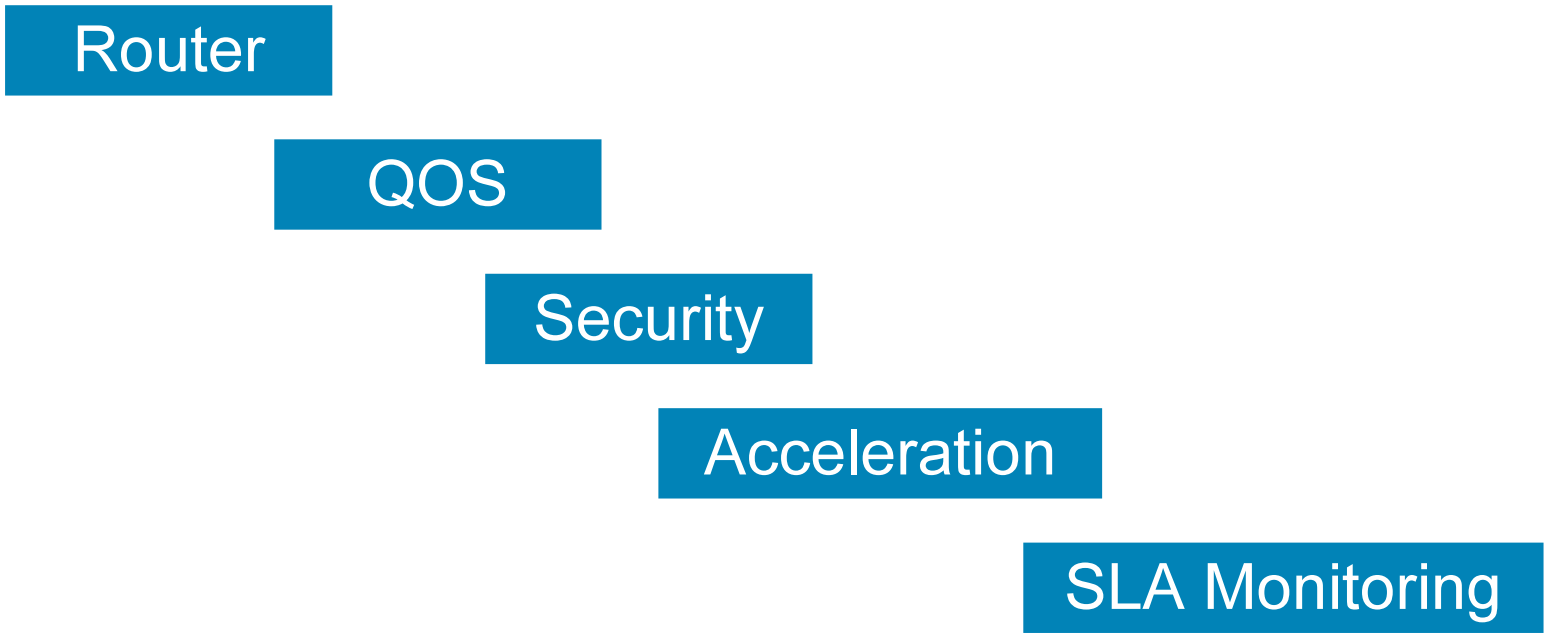


What happens without N/W Architecture

Or not understanding business requirements?

Router brought on price, isolated requirements

Got Connectivity….. But what about?



Who integrates and supports this? In short and long term

Architectural Considerations

- Looking a Role of wireless network, what business needs can be supported?
- Build a platform not a technology
- How do the platform interact with other IT components. A upper level application, a provider (location), and a user (authentication).
- Repeatable solutions/services (templates), leads to quality and simplifies designs. Branch, HQ, Warehouse.
- Ability to deal with changing demands – long term investment protection

Looking a Role of wireless network, what business needs can be supported?

- No longer application specific.

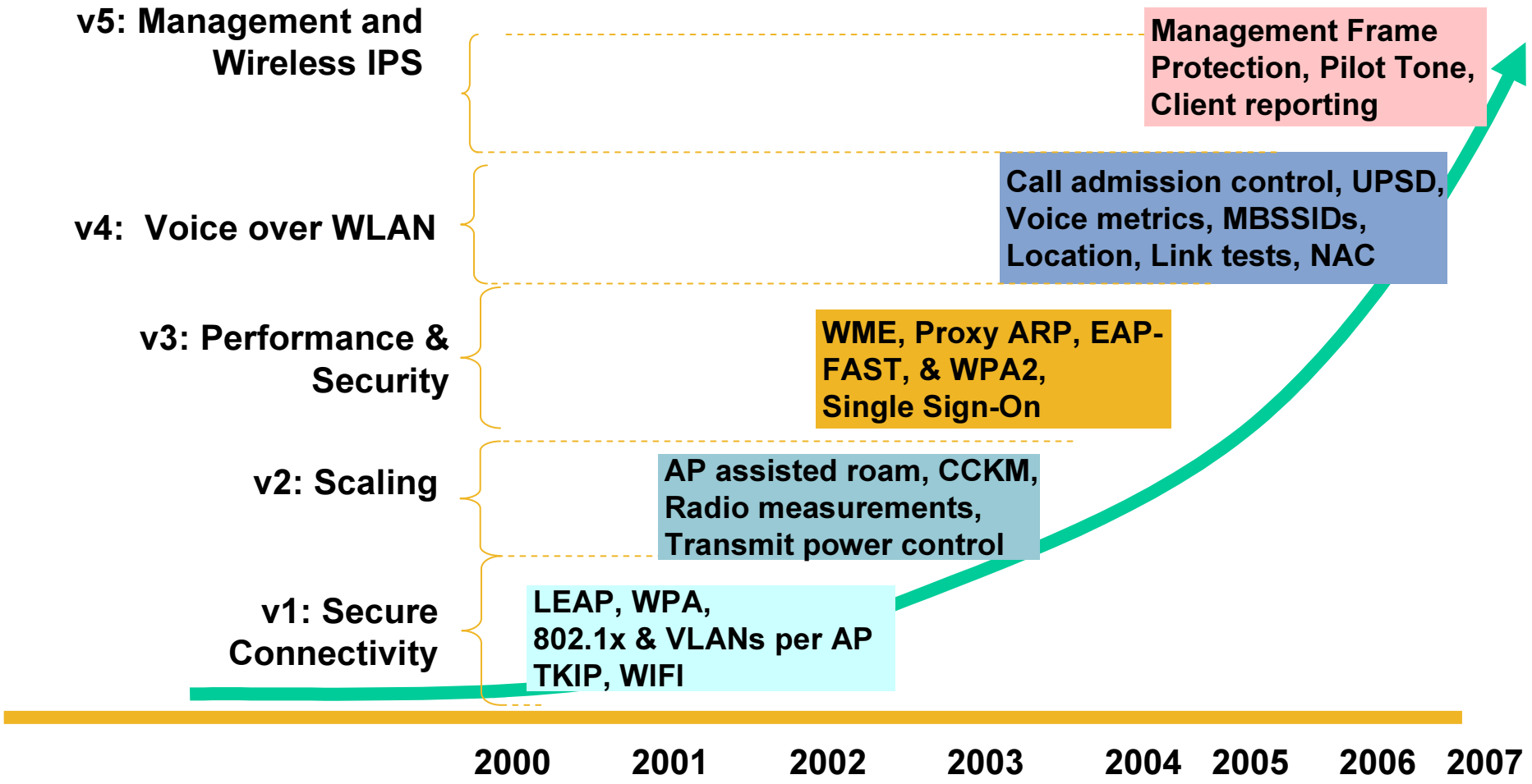
  Ideas can be left field, Wireless Digital Signs – WGB/indoor Mesh.

- Coverage areas – indoors and outdoors
- Be aware of what your clients are being sold.

  Decouple Client Devices from Infrastructure

  Set standards such as CCX compliance to reduce integration risks.

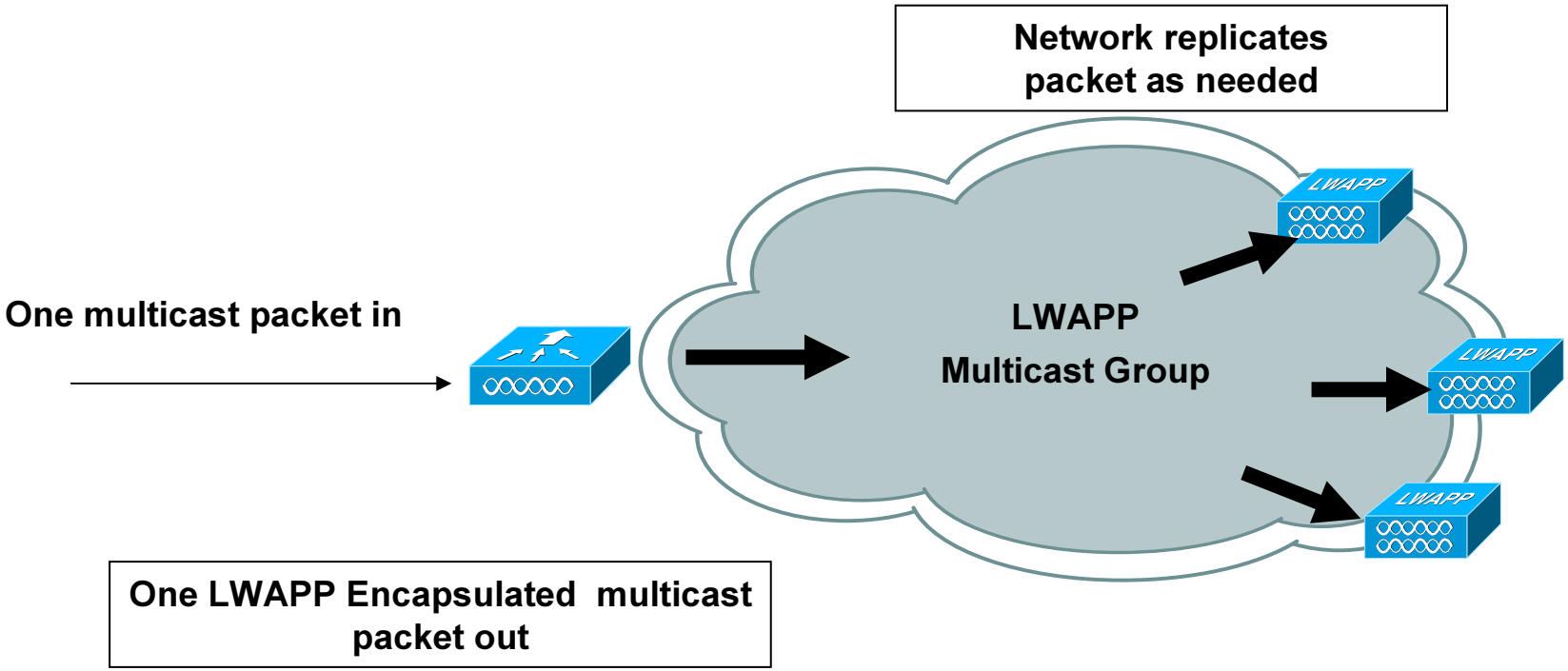
Cisco Client Extensions (CCX) releases 1-5



Looking a Role of wireless network, what business needs can be supported?

- Consider new demands such as security and environment monitoring. Bandwidth - 802.11n, high performance controllers in the 6500
- Virtualise/Segment. Hospital not only servicing Operating Theatres but also VMOs. Inherent in Cisco Unified Wireless, no external virtualisation required.
- Location services
- Live broadcasts to the Enterprise - Multicast support
- Security – do we secure everything?
- Service availability, configuration, monitoring, support – A capable management platform
- High Availability – Next Session

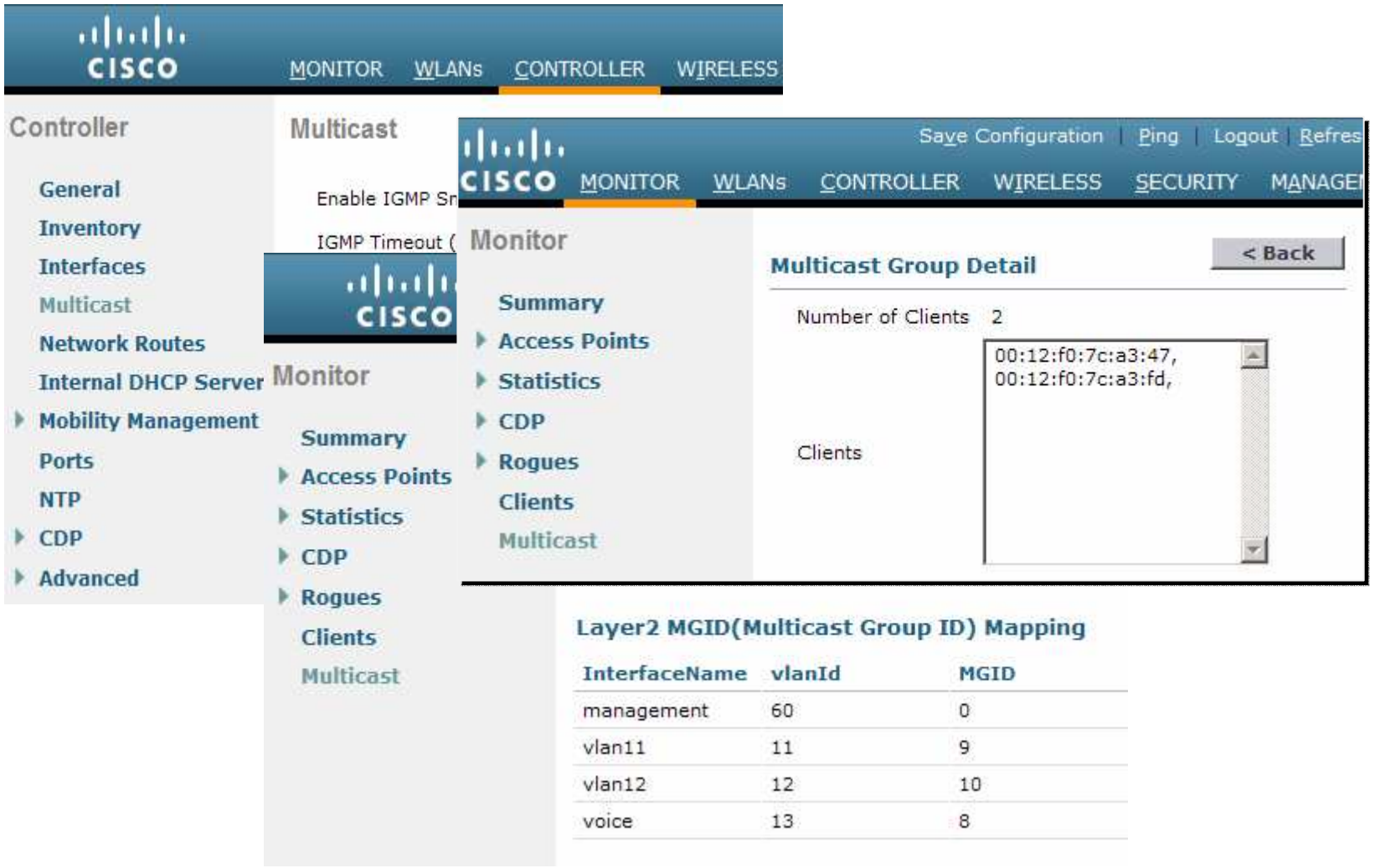
Proof Points - Multicast



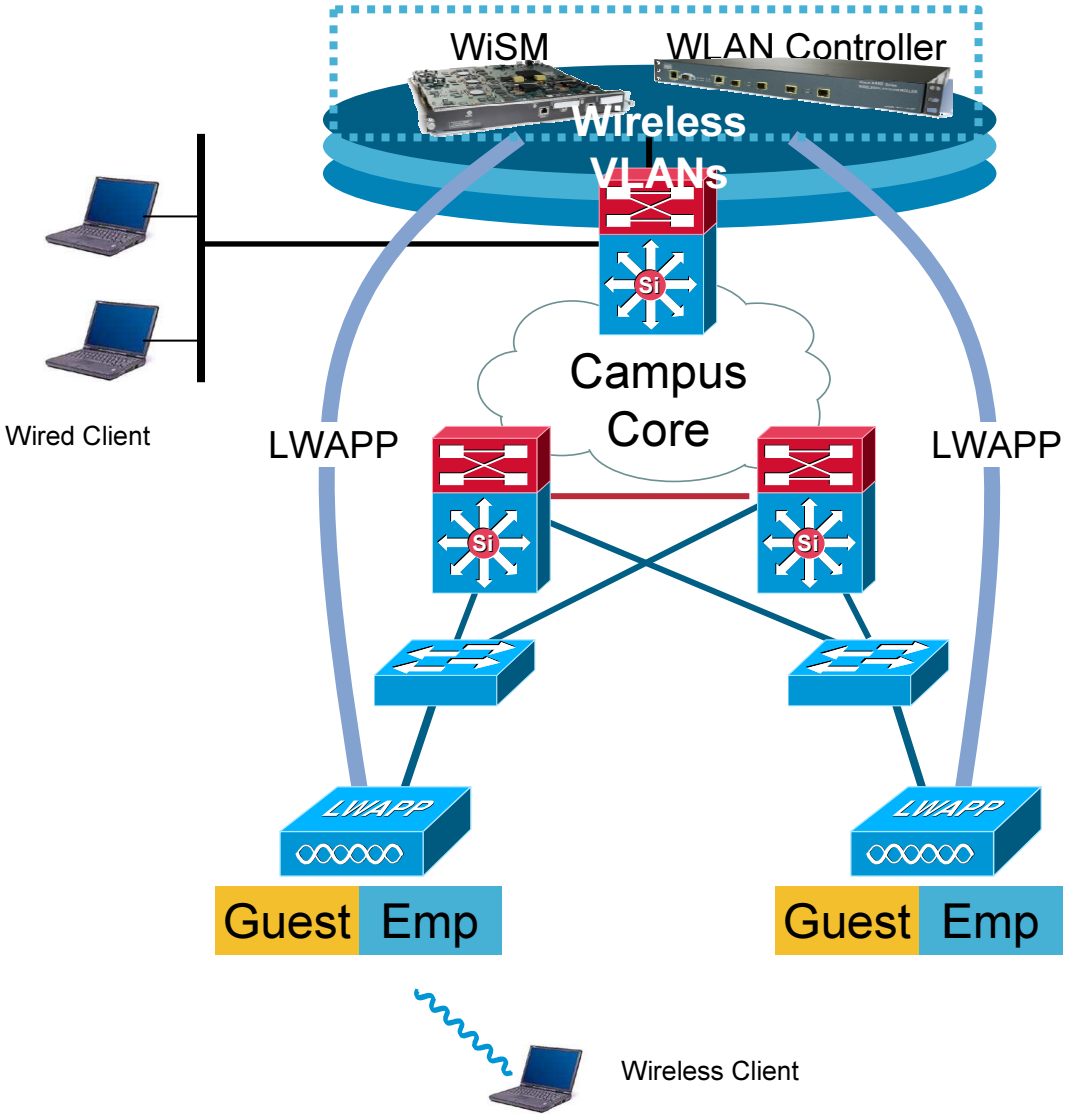
- Improved multicast performance over wireless networks
- Multicast packet replication occurs only at points in the network where it is required, saving wired network bandwidth

Multicast

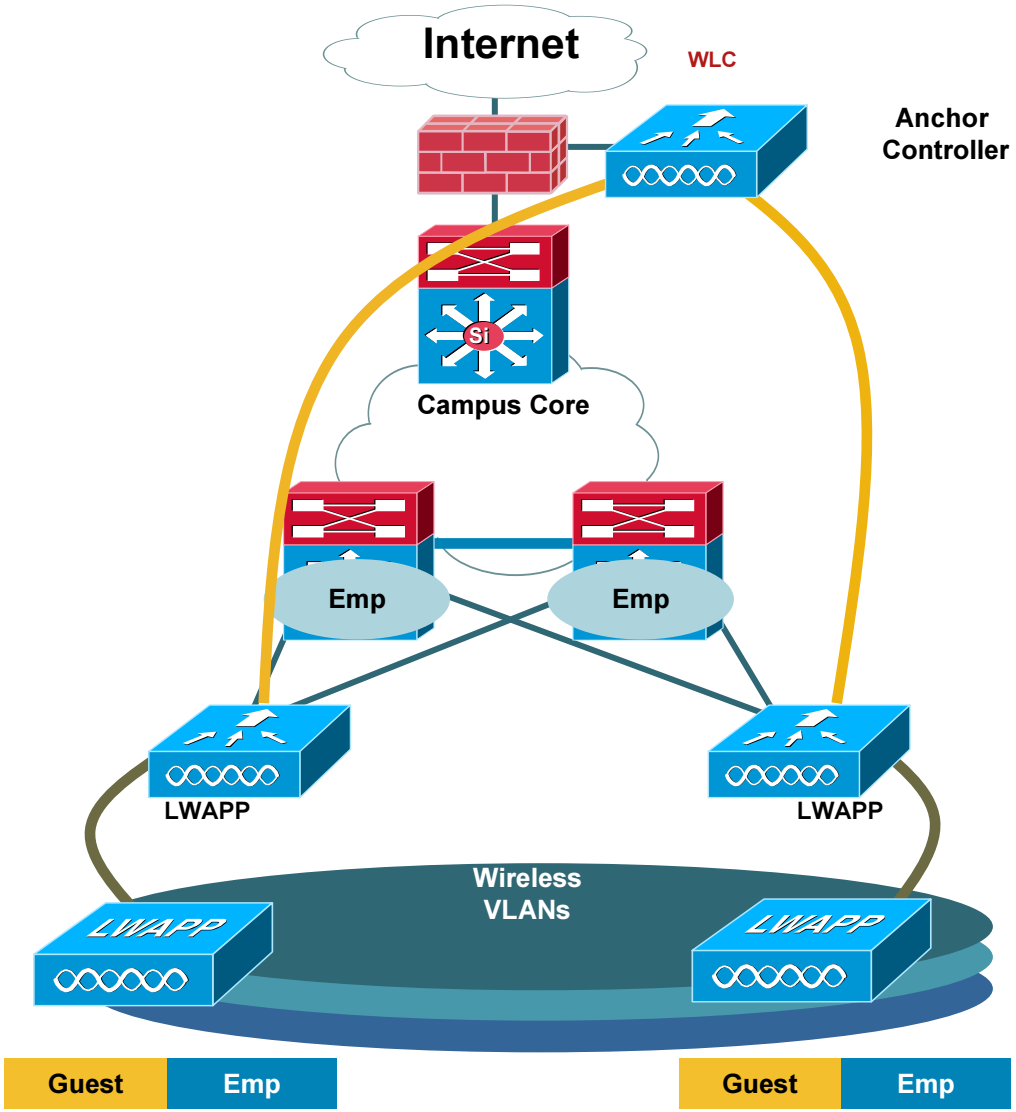
4.2



Unified Wired and Wireless Guest Access

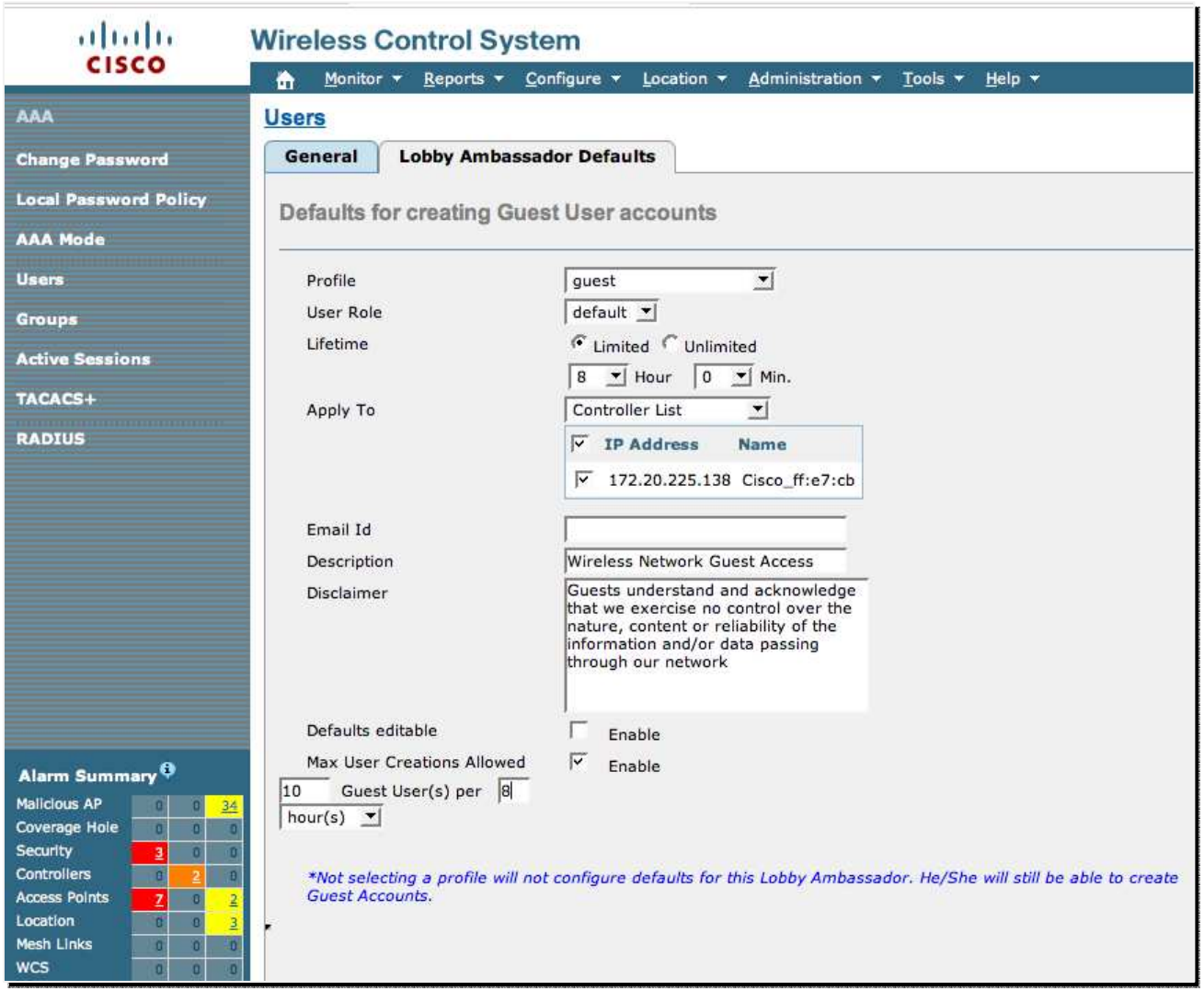


Unified Wired and Wireless Guest Access



Lobby Ambassador Controls

5.0



From the large to the small the 880 ISR

- New WAN/LAN Technologies:

  VDSL2, 3G Wireless, 802.11n WLAN

- Wireless LAN:

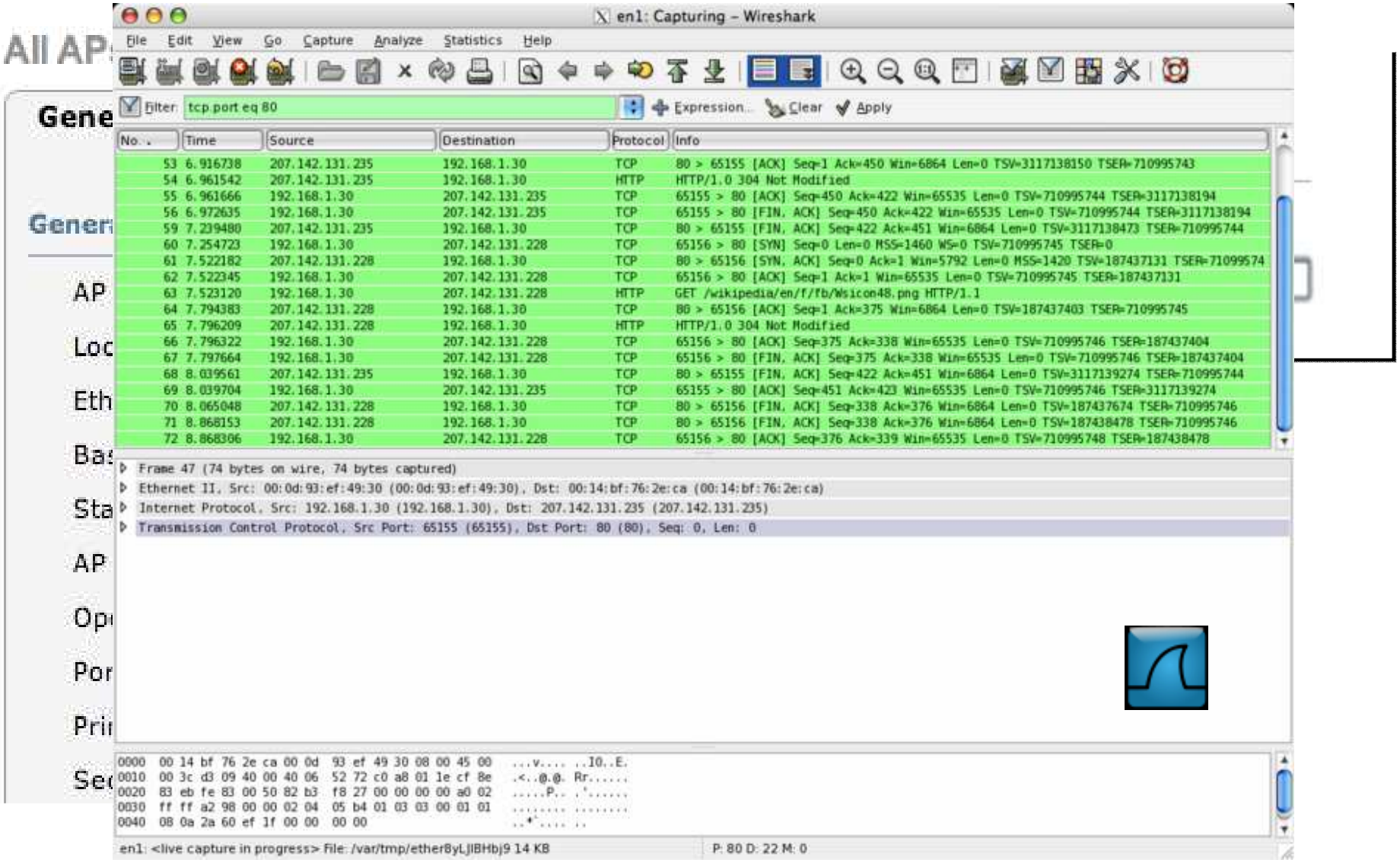
  Autonomous and LWAPP modes

  Independent AP SW upgrade

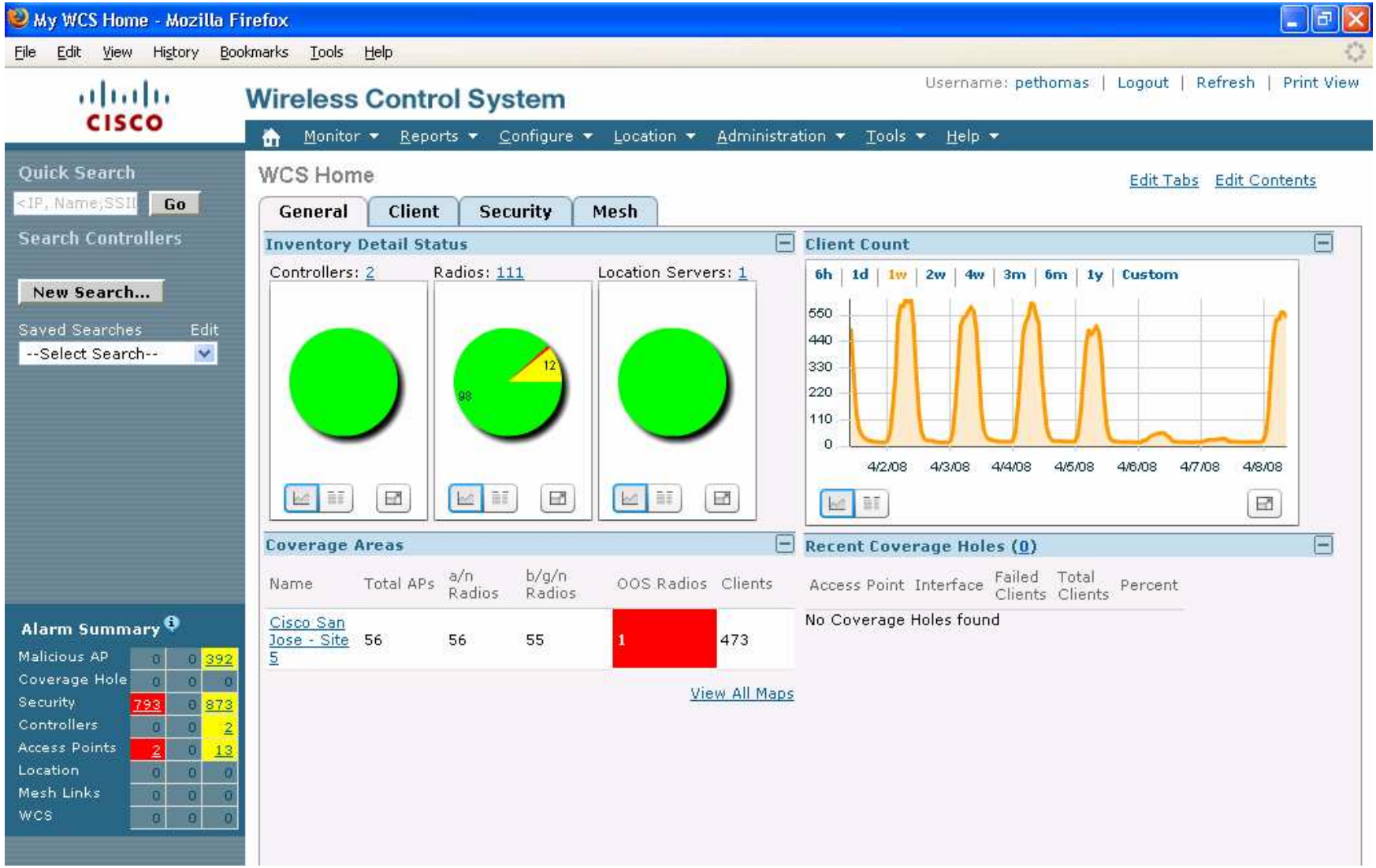
- Security:

  VPN, FW, IPS, URL Filtering

Integrated Sniffer Support



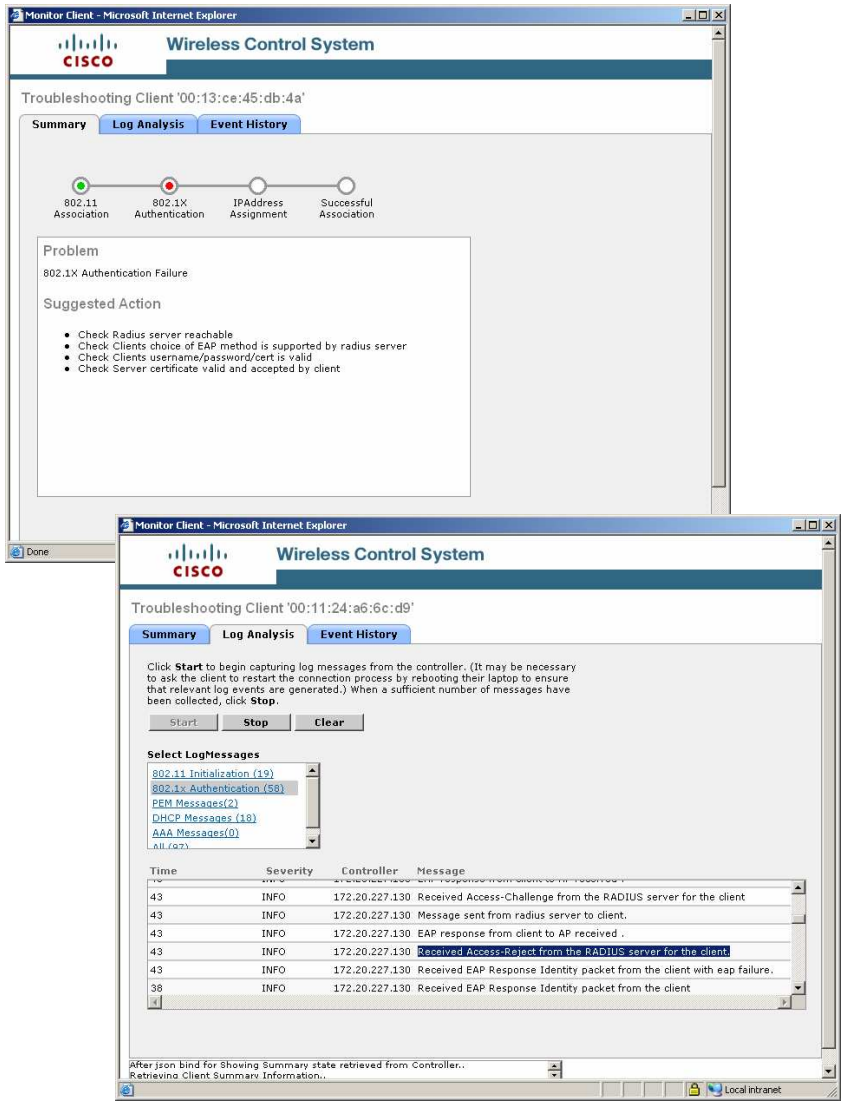
What's WCS?



Client Troubleshooting Tool

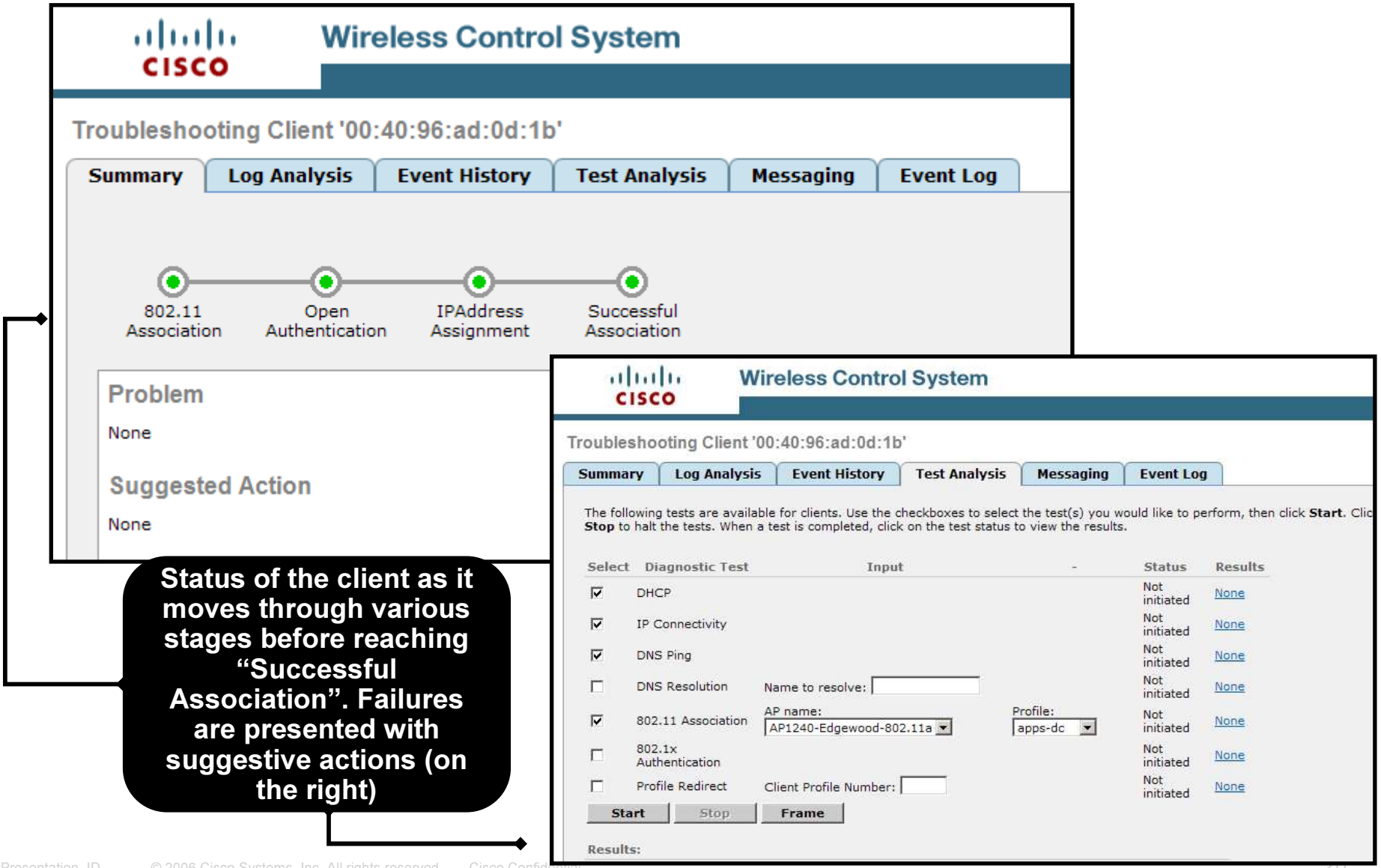
5.0

- CCX v5 clients can request diagnostic channel association
- Generate a consolidated summary of troubleshooting tests on diagnostic channel
- Assist network administrators to diagnose and suggest fixes to common client problems
- Debug layer 1 to layer 3 client problems using a step by step method
- Ability to dig into details and logs as needed



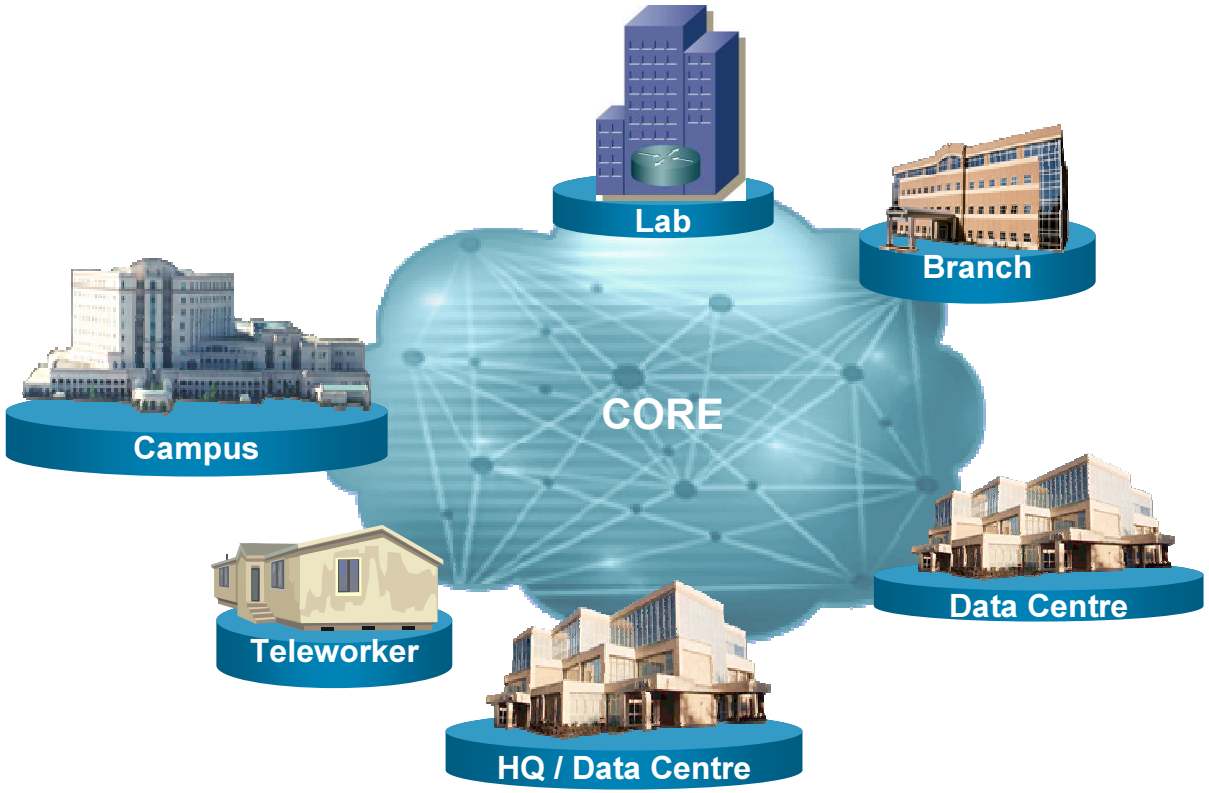
Client Troubleshooting

5.0



Status of the client as it moves through various stages before reaching "Successful Association". Failures are presented with suggestive actions (on the right)

Places In The Network – Reducing the Risk



Mobility Related SRND/CVDs

- Mobile Care Imatis Solution Design Guide
- PCI for Retail 2.0 Design Guide
- Voice over Wireless LAN 4.1 Design Guide
- Secure Wireless Design Guide 1.0
- Enterprise Mobility Design Guide 4.1

Case Studies and Applications

Manufacturing Plant

- Large gantry loading stock need network connectivity - wireless bridging.
- Wireless has to be reliable
- In a challenging RF environment
- And a challenging physical environment…


AUTEC


20 kN
61
60
50


RS
RITTAL
AUTEL
CE

33

Other Applications of a wireless infrastructure

- Power Station – Wanted Video anywhere on site.
- Power Station and Refinery - Solar Powered Bridges on Barges on Dams.
- Mining –Using solar powered Mesh APs on trailers.

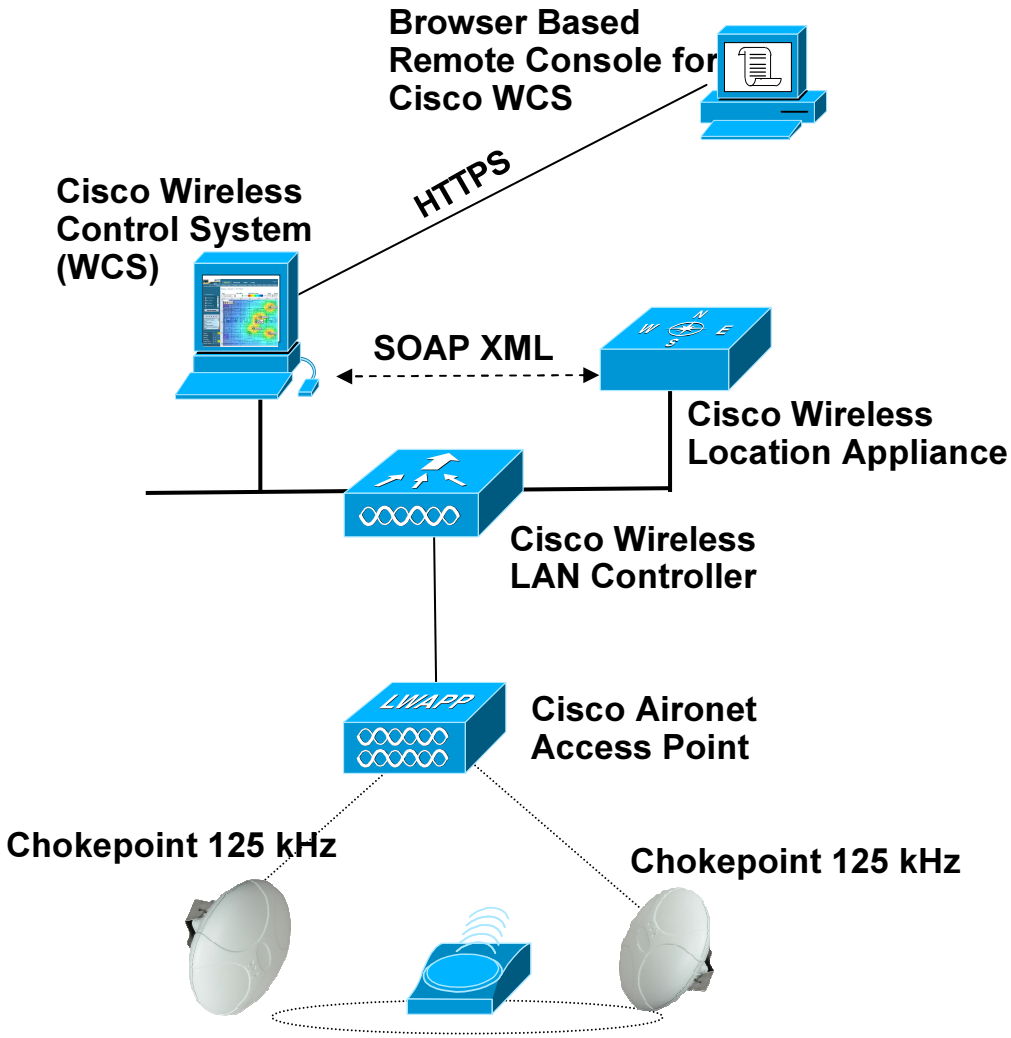
Other Applications

- Remember Minority Report?
- Interactive Signage
- What makes up that solution
- Applications – safety compliance

Wireless Location

- Pervasive tracking of people and object
- Real-time and historical tracking
- RF Chokepoint can give real-time and precise location updates
- CCX Tags – New family of CCX devices

Chokepoint Architecture



1. Device with a Wi-Fi tag moves into a zone with a chokepoint.
2. The chokepoint “triggers” the Wi-Fi tag using 125Khz radio.
3. Wi-Fi tag sends chokepoint information to the access point using its 802.11 Wi-Fi radio.
4. Access point sends information on to the controller which consolidates the information and asynchronously sends it on to location appliance.
5. Location appliance sends chokepoint’s location and any other information to Cisco WCS or a third party solution.


** STORM WARNING **
Please Secure all Buildings and Vehicles Contact Operations on Extension 555 for assistance if required.
IT Training Specialist

Safety - Is your certification current?

Geo Location– “Find the Expert”

Airport example:

- Access application via XML phone service on desktop IP phone
- Enter “target location” (or let network derive it)—e.g., “gate 70”
- Display map of “experts” (carrying 802.11 wireless phones)
- Allow user to select one from the map or click “Closest”
- Extend call to that expert’s wireless phone

Wireless and Security

Wireless Security

- Snapshot of what customers are using around Australia
- In addition to Cisco SRNDs and CVDs…
- NIST Special Publication 800-97. Establishing Wireless Robust Security Networks. A Guide to IEEE 802.11i. Useful checklists.

Cisco – EAP-FAST

- Initially deployed with LEAP, progressive migration to EAP-FAST. Supporting IP Handsets.
- Using Supplicant
- Supports Single Sign-On
- Supports both Windows and Macintosh operating systems
- Provides Authentication and Privacy

University – Open SSID

- Needed support students and staff
- Did not want to deal with OS Supplicant issues or costs
- Modified DNS to send a all requests to web server which hosted instructions and VPN Client (Cisco's IPSec client)
- Provides Authentication and Privacy
- Also supporting 802.1X through University roaming agreements (Eduroam)

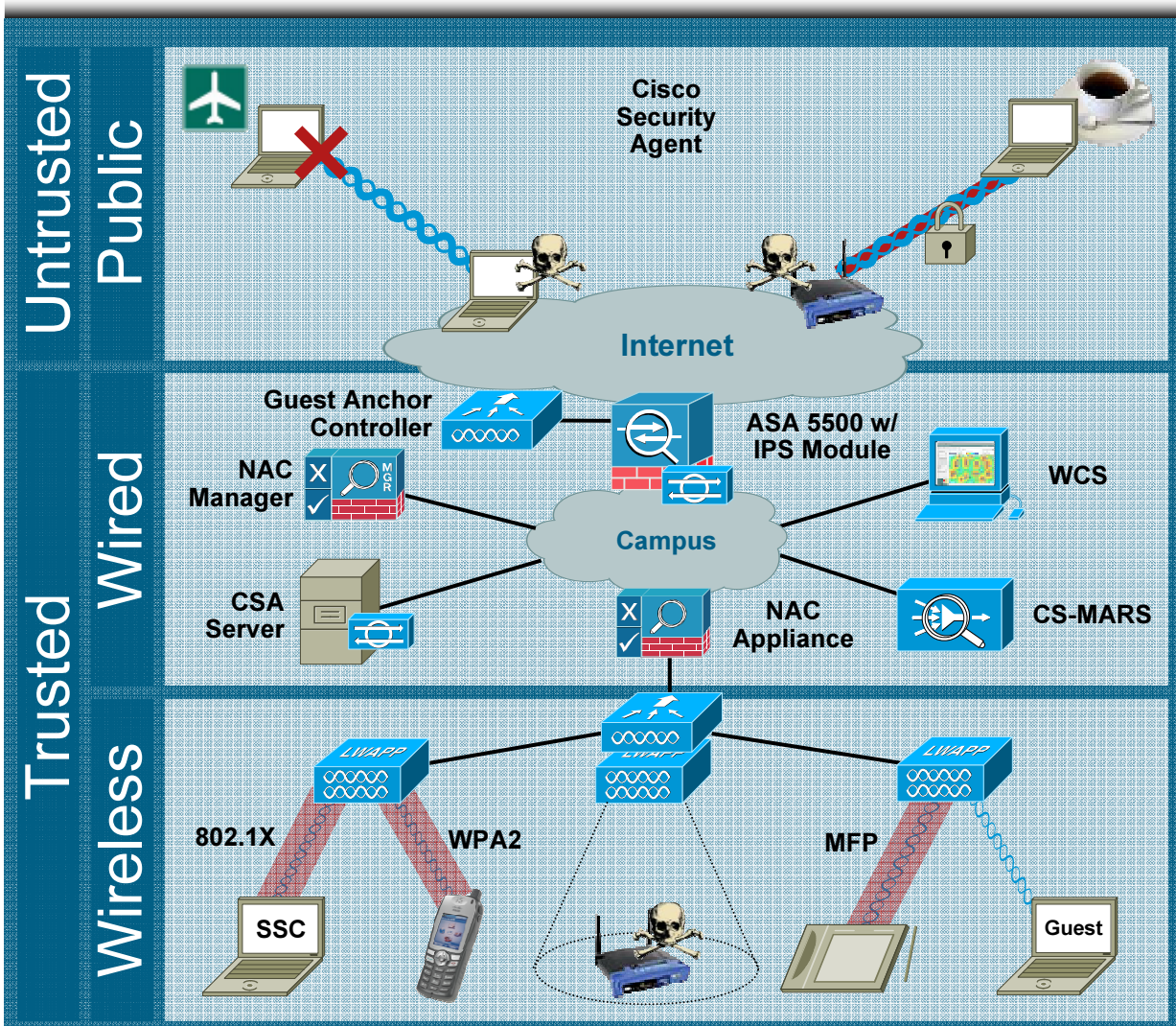
Large Enterprise - Guest

- Lightest touch on PCs – visitors may not have rights
- Compromise – provide Authentication but not confidentiality. Some enterprises using pre-shared keys to provide privacy.
- Using Lobby Ambassador capabilities – ability for designated team to created time-bombed accounts

Large Enterprise EAP-TLS

- Deployed as part of AD
- Was considering using two-factor auth but wanted better user experience
- Are authenticating Machine not user – therefore small risk of someone compromising accounts on PC
- Most Commonly Deployed from the straw pool

Pervasive Security and Mobility



Endpoint Protection

- Host intrusion prevention
- Endpoint malware mitigation

Traffic and Access Control

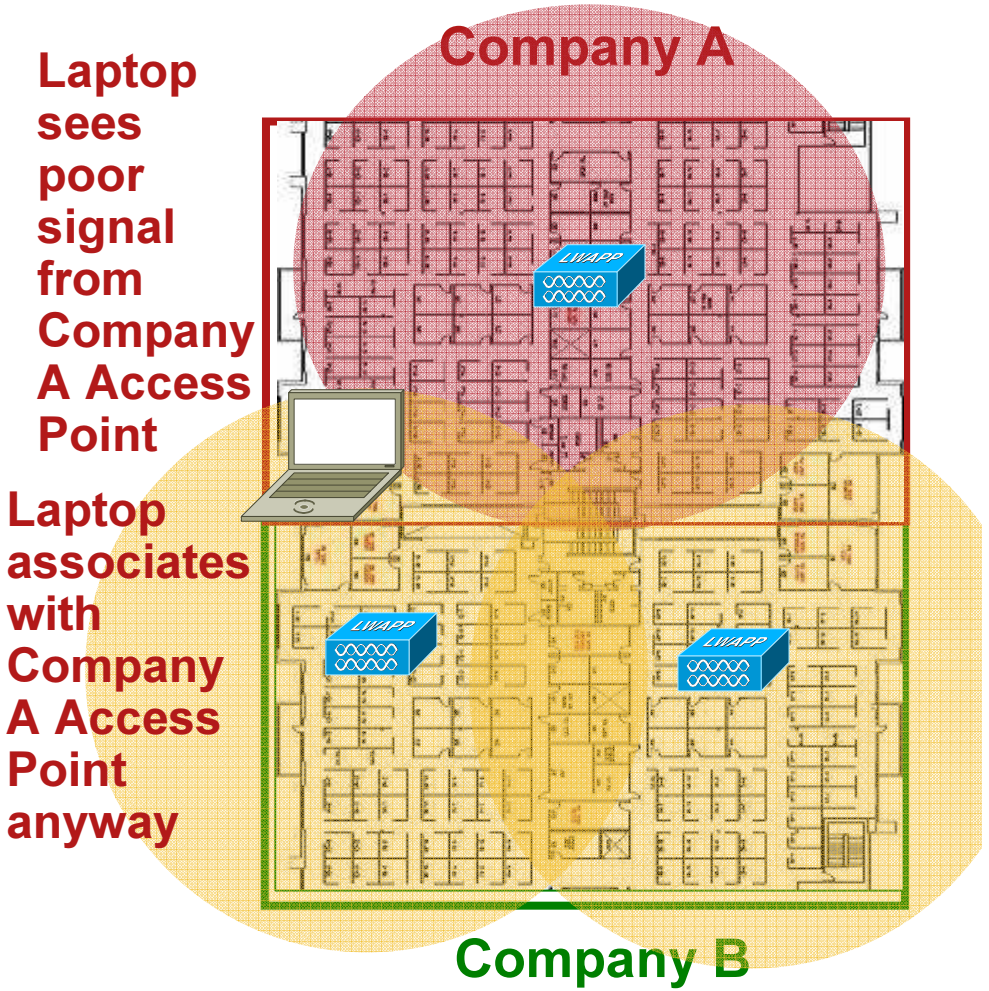
- Device posture assessment
- Dynamic, role-based network access and managed connectivity
- WLAN threat mitigation with IPS/IDS

WLAN Security Fundamentals

- Strong user authentication
- Strong transport encryption
- RF Monitoring
- Secure Guest Access

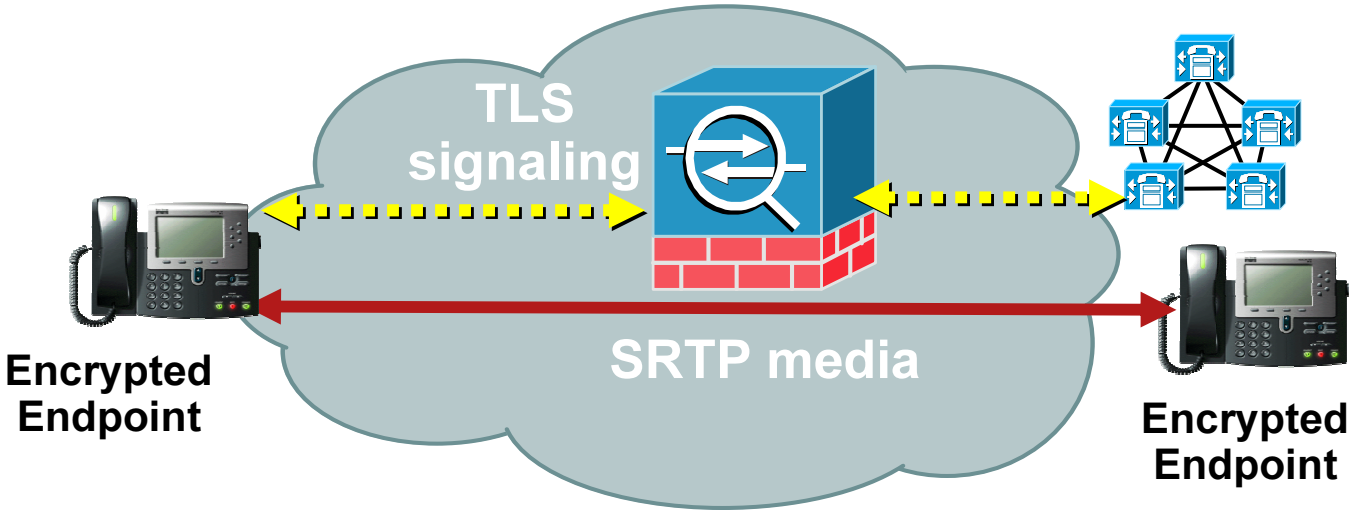
CSA Protects the Wireless Laptop

- CSA enforces SSID use
  - If laptop sees Company A SSIDs, it must associate with them
  - Laptop has to use corporate encryption mandates (EAP-Fast, etc)
- CSA blocks wireless – to – wired bridging
  - If ethernet is active, WLAN is disabled
- Location Aware Policies



ASA TLS Proxy - Encrypted Voice Firewall Solution

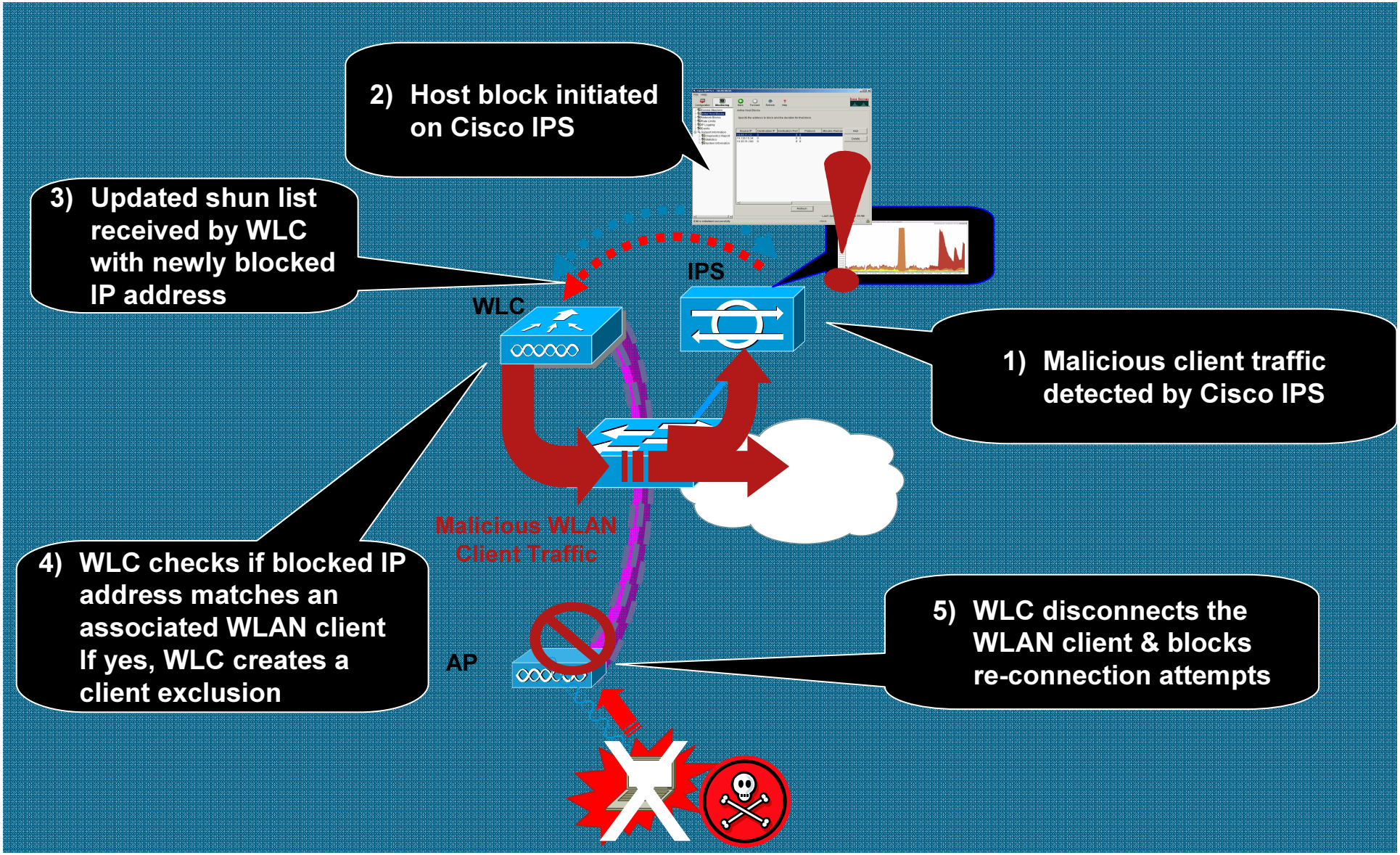
Solving the Firewall & Encryption Integration Problem



Any Cisco voice/video communications encrypted with SRTP/TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- **Maintains integrity and confidentiality of call while enforcing security policy through advanced SIP/SCCP firewall services**
- **TLS signaling is terminated and inspected, then re-encrypted for connection to destination (leveraging integrated hardware encryption services for scalable performance)**
- **Dynamic port is opened for SRTP encrypted media stream, and automatically closed when call ends**

WLC and IPS Integration



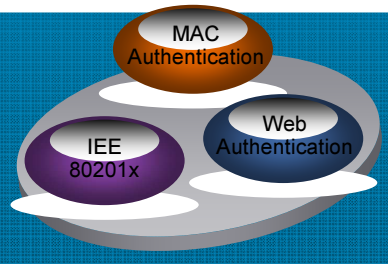
Cisco TrustSec (Trusted Security)

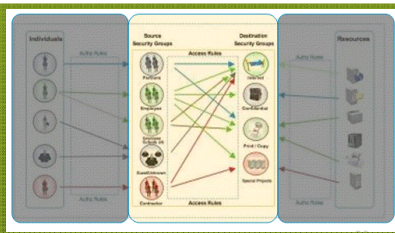
Seamless Authentication for Various Access Types

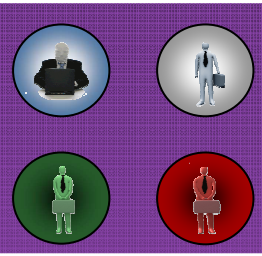
Secure Campus Access Control

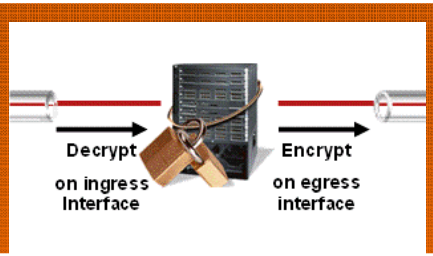
Converged Policy Framework

Converged Policy Definition for Different Access Types Policy Enforced Throughout the Network









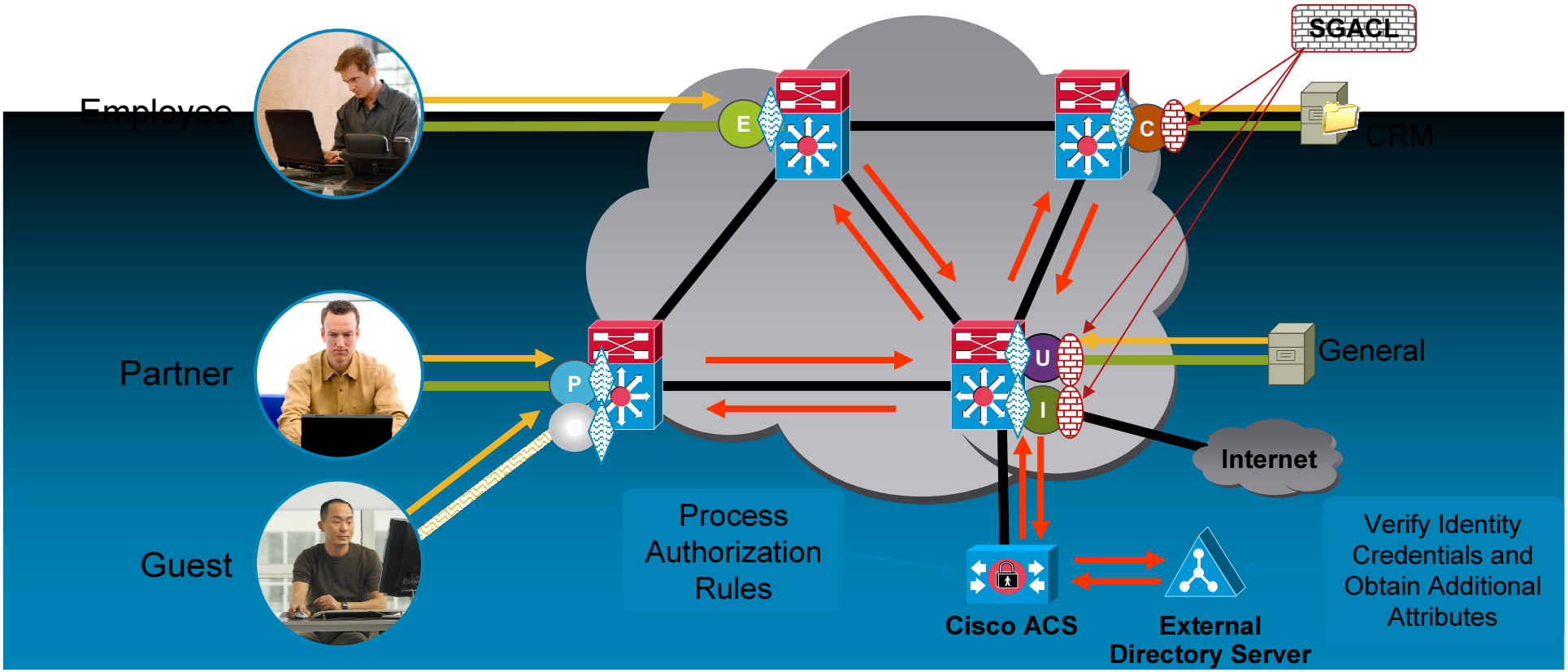
Transforming From Topology-aware to Role-aware Access Control

Role Aware Network

Integrity & Confidentiality

Prevent Data Sniffing and Tampering with Line-rate Hop-by-hop Encryption

Policy Enforcement Throughout the Network:
Role Based Access Control Set-up



Legend

Link/Port Status

- Unauthenticated
- Failed Authentication
- Authenticated
- Shutdown

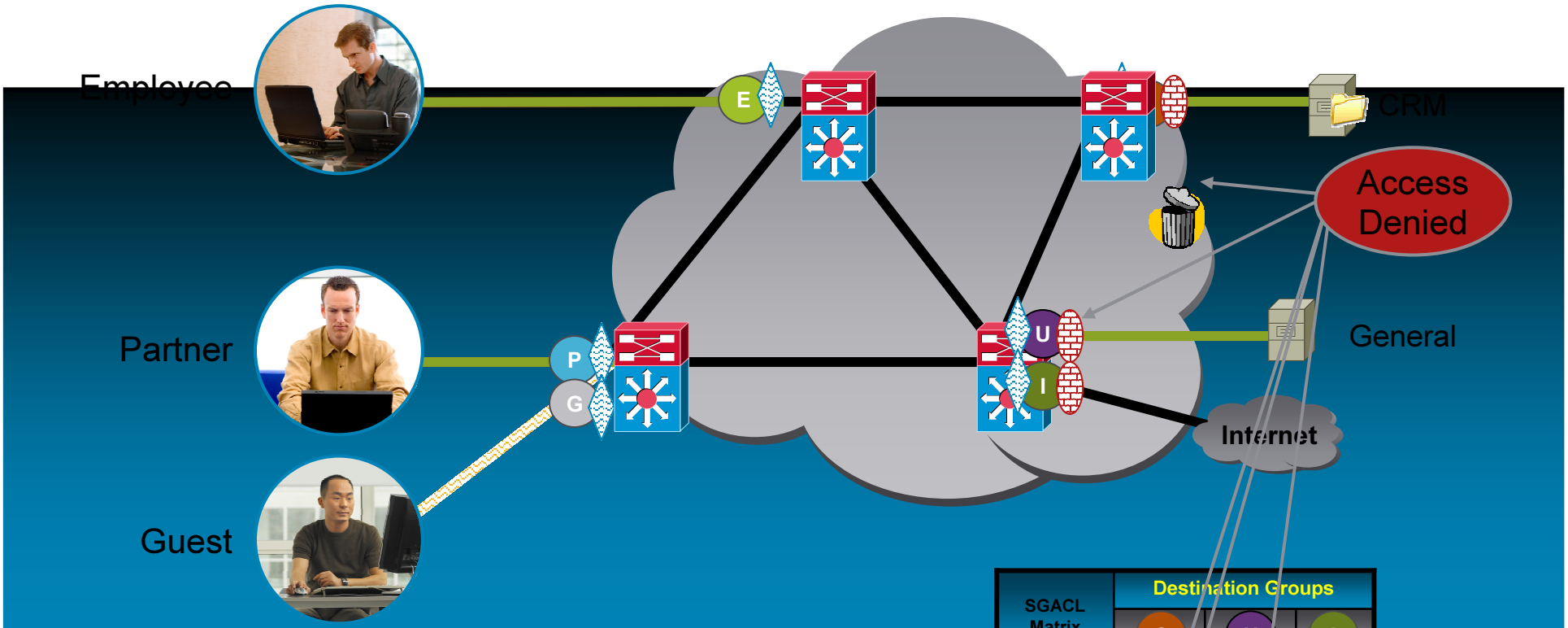
- Ingress Tagging
- Egress Filtering

Security Group Classifications

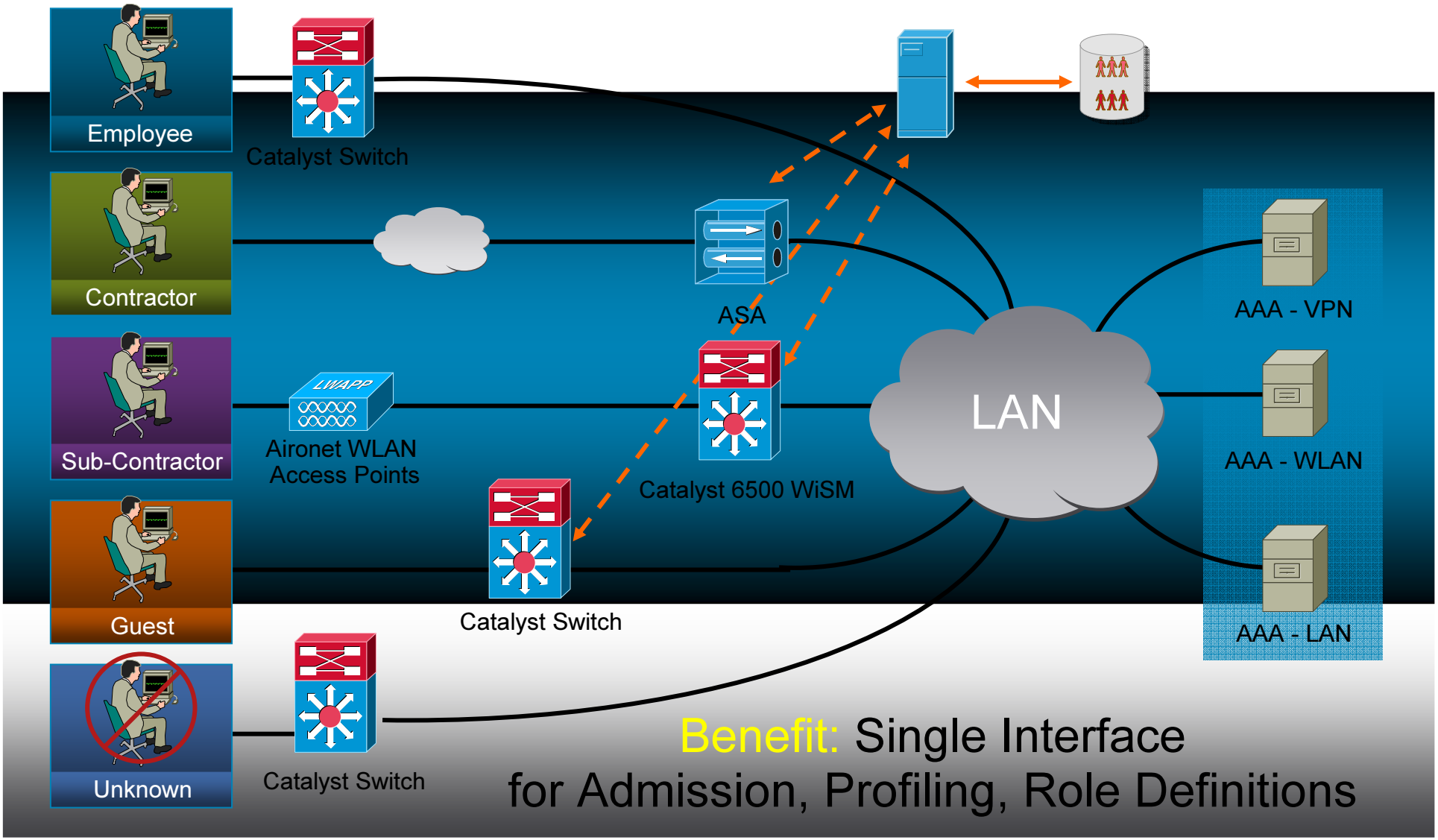
- E — Employee Group
- P — Partner Group
- Guest Group
- C — Confidential Group
- U — Unrestricted Group
- I — Internet Group

1. **Authentication Request**
2. **Radius and AD Authc/Authz**
4. **Group Membership Dynamically Assigned**
5. **SGACL Dynamically Applied**
6. **Links Up**

Policy Enforcement Throughout the Network:
Role Based Access Control Deployment

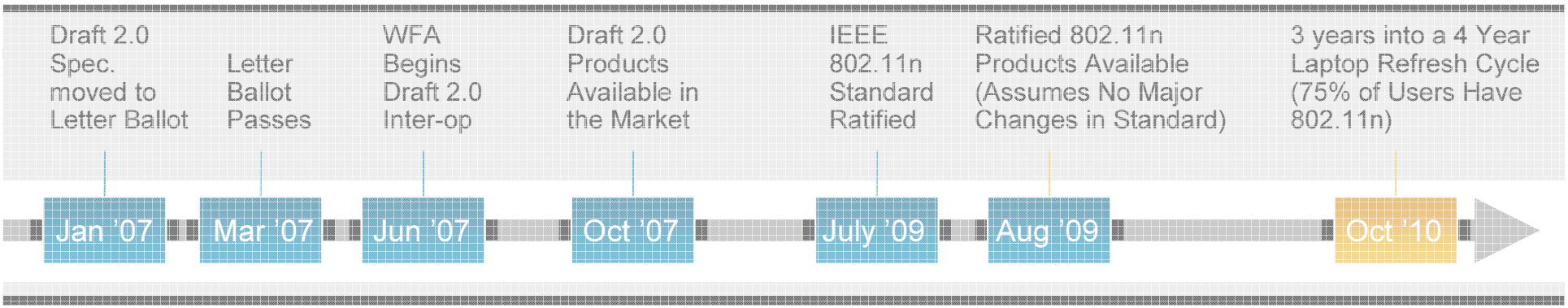


Converged Policy Framework:



802.11n
An Introduction

IEEE and the Wi-Fi Alliance



While changes to the standard are unlikely to require any hardware modifications to the existing Cisco AP, the platform **is modular** to ensure investment protection

802.11n Product Interoperability

- The first Wi-Fi certified 802.11n draft 2.0 Access Point
- Selected for the Wi-Fi interoperability testbed
  - All certified products tested against the AP1250
  - The only AP vendor selected for the test bed
  - The remainder are silicon manufacturers
- Cisco and Intel performing joint interoperability testing

Introducing the 1250 Access Point

- First Enterprise 802.11n AP
  - Modular
  - Upgradeable
- Hardware MIMO support
  - Spatial Multiplexing
    - Two spatial streams
  - MRC
  - TxBF
  - 2 Transmitters
  - 3 Receivers
- 10/100/1000 Ethernet
- Over 30,000 units shipped,

New Antennas for Aironet 1250 Series

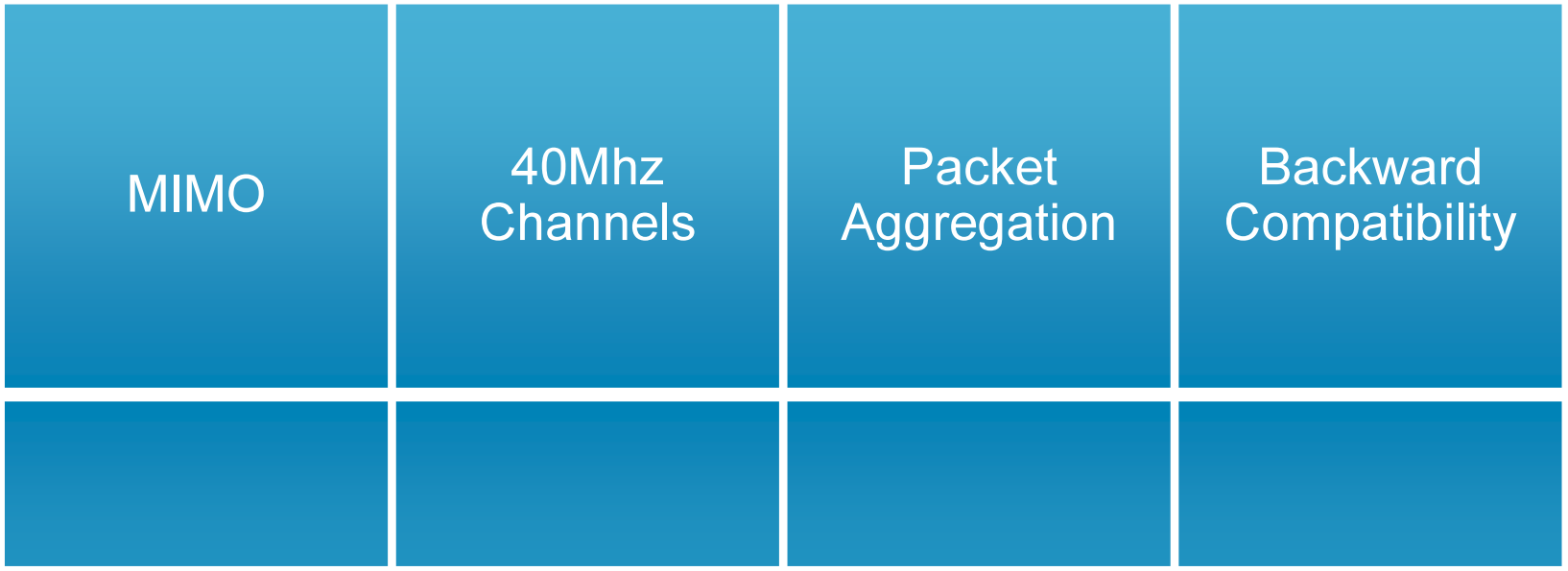
- Omnidirectional
  - Single enclosure with 3 antenna elements
    - 2.4 GHz 3dBi (AIR-ANT2430V-R)
    - 5 GHz 4 dBi (AIR-ANT5140V-R)

- Dipoles
  - New dipole without hinge (gray)
    - 2.4 GHz 2.2 dBi (AIR-ANT2422DG-R)
    - 5 GHz 3.5 dBi (AIR-ANT5135DG-R)
  - Also supports existing dipoles with hinge (black & white)

- Blue dot indicates 5 GHz

Technical Elements of 802.11n

MIMO	40Mhz Channels	Packet Aggregation	Backward Compatibility



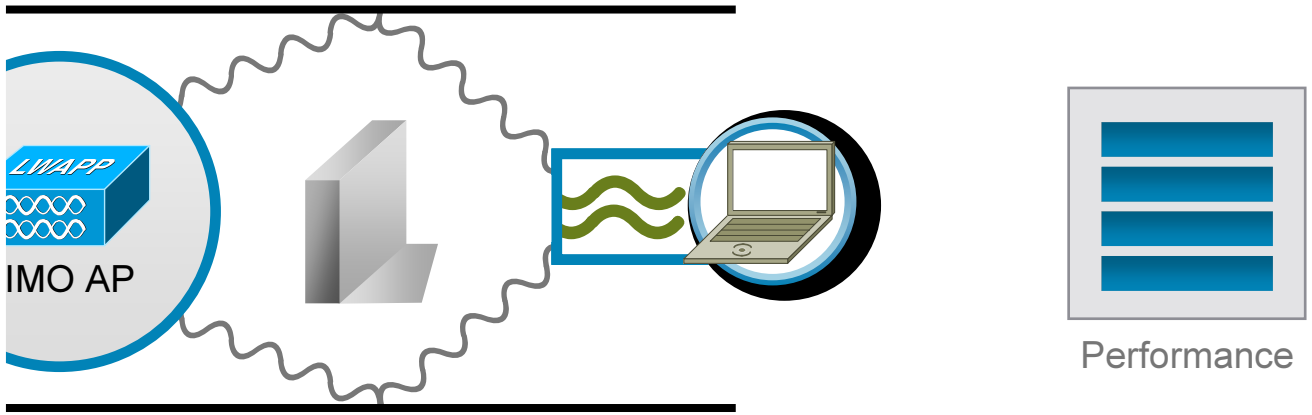
Aspects of 802.11n

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO (Multiple Input, Multiple Output)

With Beam Forming Transmissions Arrive in Phase, Increasing Signal Strength

Without Beam Forming Transmissions Arrive out of Phase



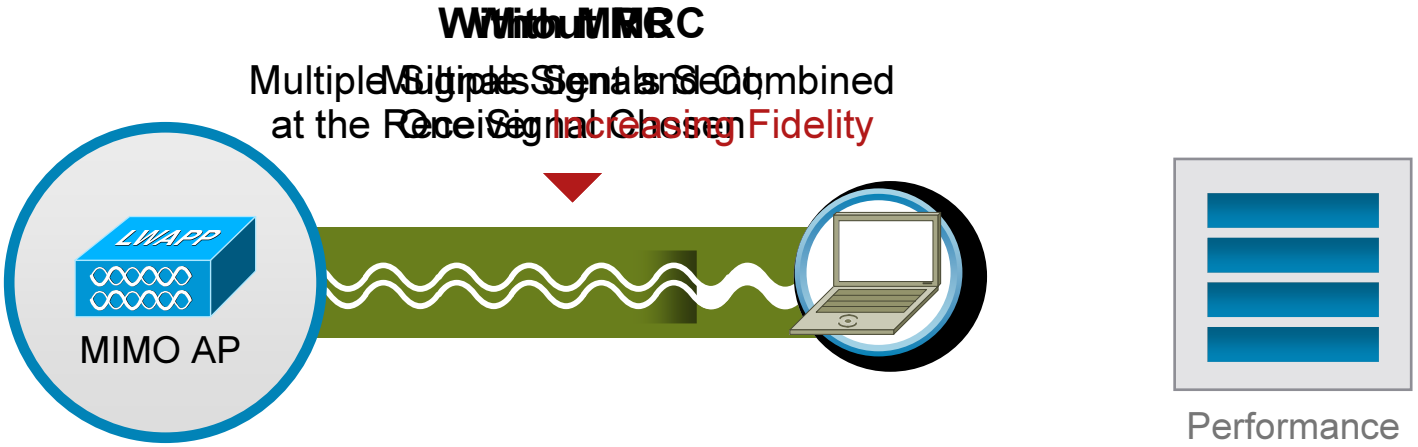
Performance

Performed by Transmitter (Talk Better)	Ensures Signal Received in Phase	Increases Receive Sensitivity
Beam Forming	Maximal Ratio Combining	Spatial Multiplexing

Aspects of 802.11n

40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO (Multiple Input, Multiple Output)



Performed by Receiver (Hear Better)	Combines Multiple Received Signals	Increases Receive Sensitivity	Works with non-MIMO and MIMO Clients

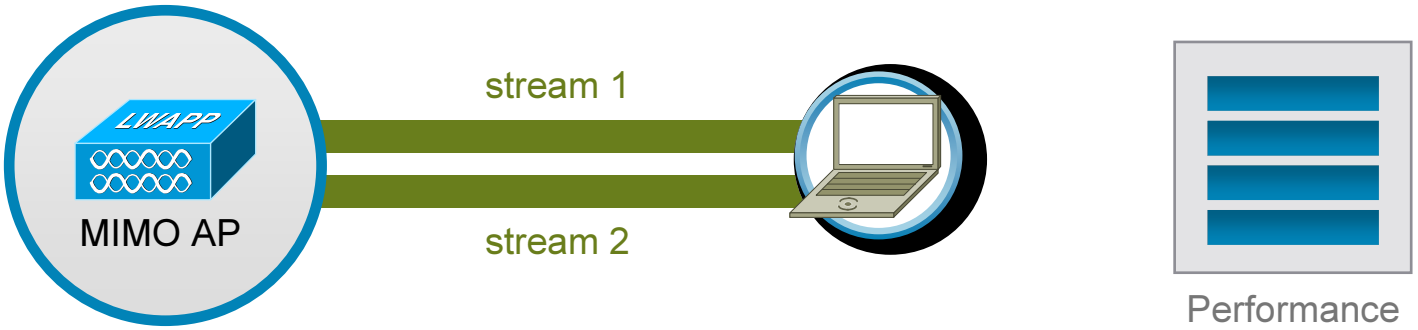
Beam Forming | Maximal Ratio Combining | Spatial Multiplexing

Aspects of 802.11n

40Mhz Channels | Packet Aggregation | Backward Compatibility

MIMO (Multiple Input, Multiple Output)

Information Is Split and Transmitted on Multiple Streams



Transmitter and Receiver Participate	Concurrent Transmission on Same Channel	Increases Bandwidth	Requires MIMO Client

Beam Forming | Maximal Ratio Combining | Spatial Multiplexing

Aspects of 802.11n

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

40Mhz Channels

Moving from 2 to 4 Lanes

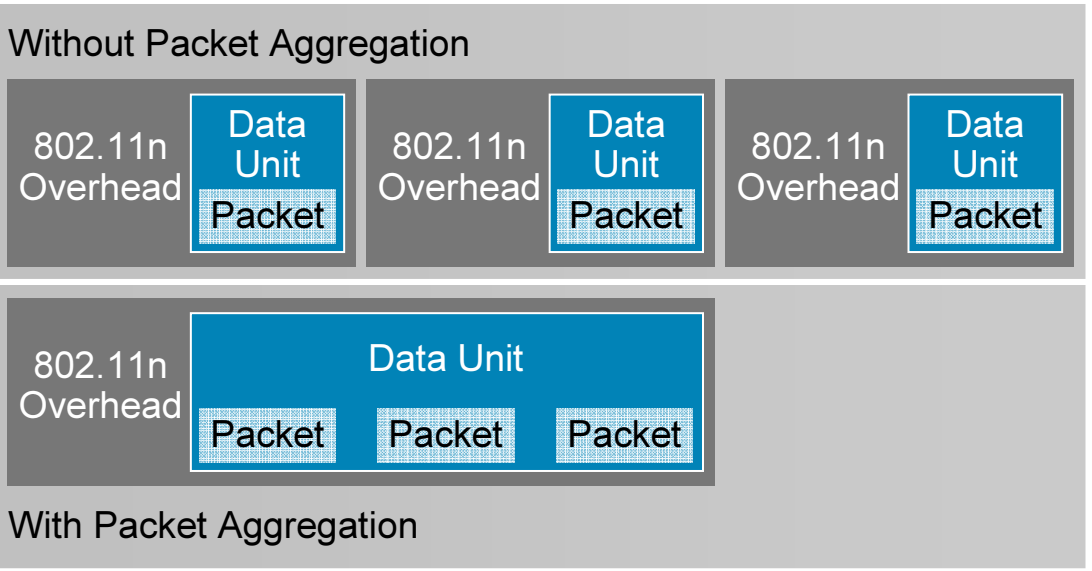
- 40-MHz = 2 aggregated 20-MHz channels—takes advantage of the reserved channel space through bonding to gain more than double the data rate of 2 20-MHz channels

Aspects of 802.11n

MIMO | 40Mhz Channels | Packet Aggregation | Backward Compatibility

Packet Aggregation

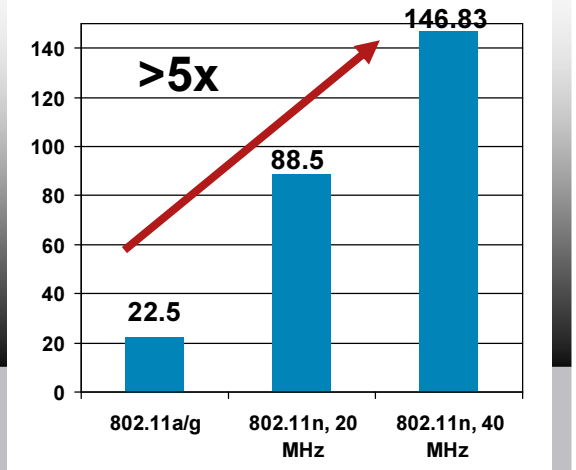
Carpooling Is More Efficient Than Driving Alone

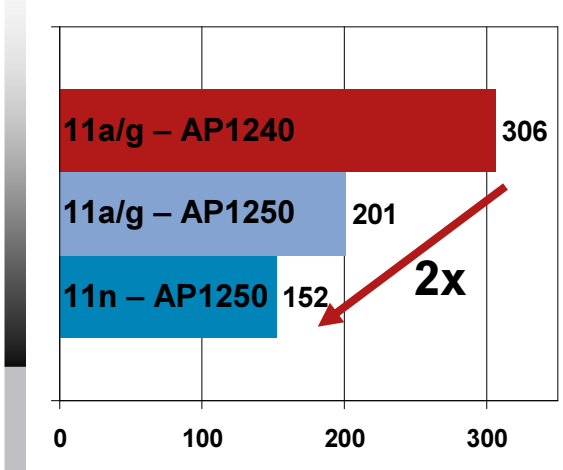


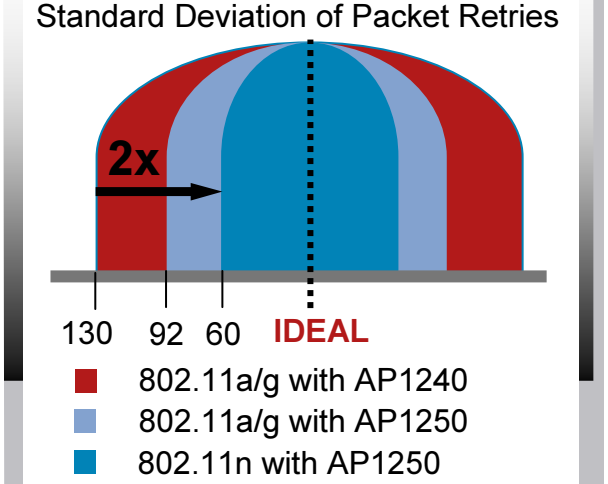
MSDU (h/w) v MPDU (s/w)

802.11n
It's About a Whole Lot More Than Speed

Throughput	Reliability	Predictability
5x more throughput	2x more reliable	2x more predictable
Enhanced file transfer and download speeds for large files	Lower latency for mobile unified communications	More consistent coverage and throughput for mobile applications



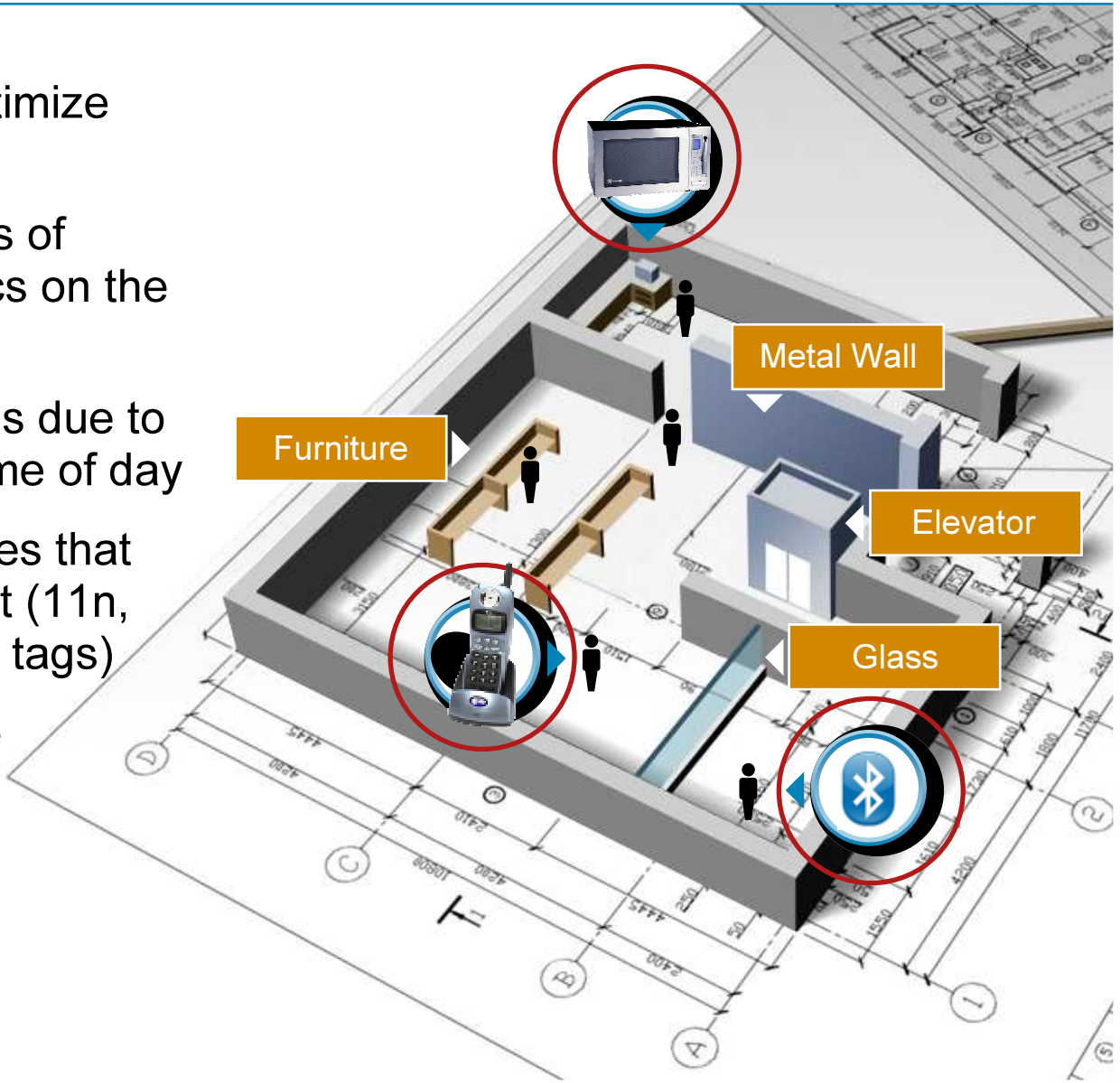




802.11n
Design and Deployment

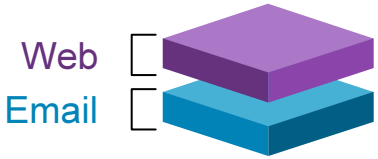
Site Survey Prepares for 802.11n

- Recommended to optimize 11n deployment
- Survey reveals effects of building characteristics on the wireless spectrum
- Measure RF variations due to human activity and time of day
- Survey with client types that you plan to implement (11n, 11abg, VoIP, location tags)
- Spectrum intelligence to detect interference

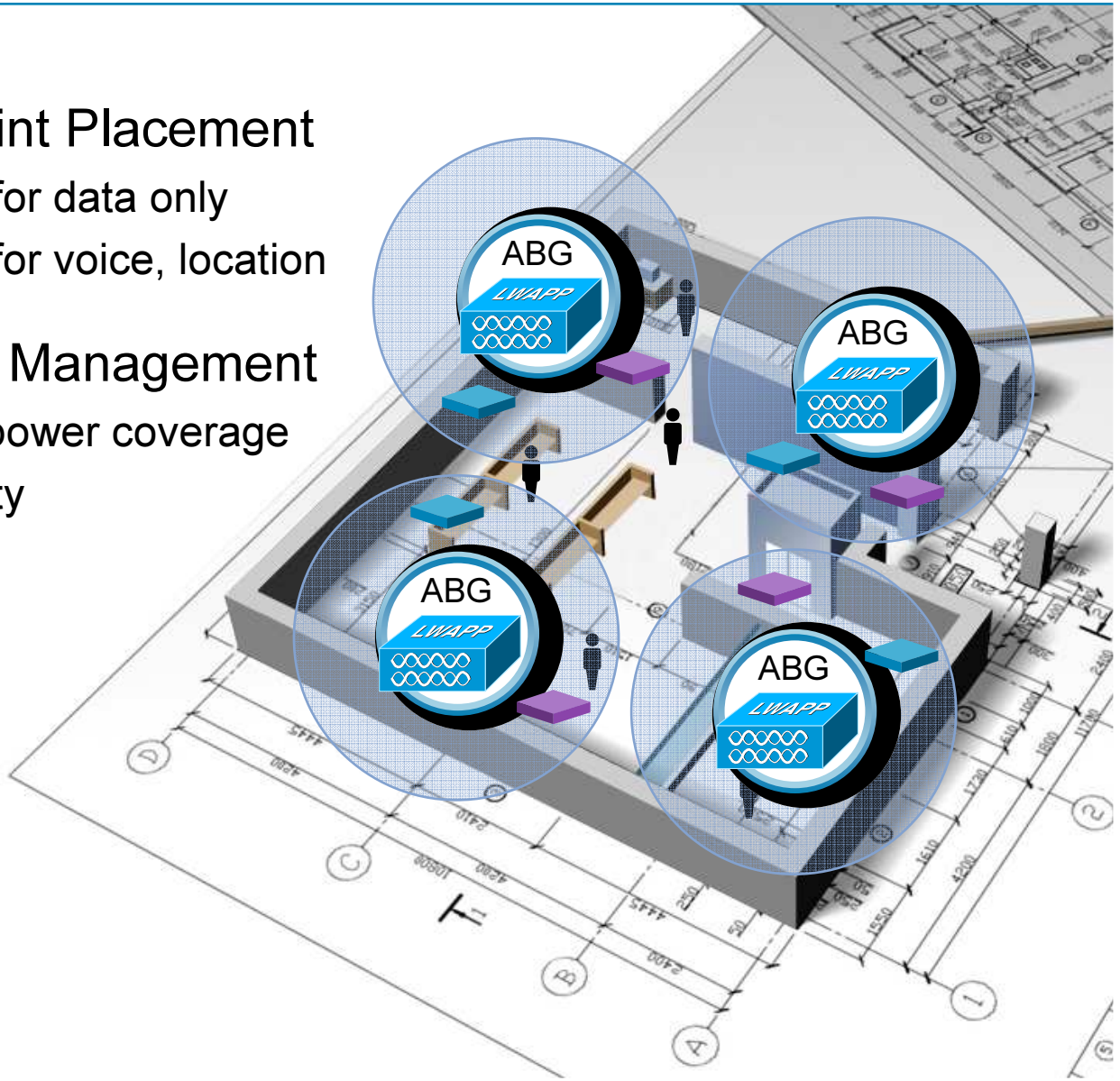


Access Point Placement

- ABG Access Point Placement
  - 1 per 5,000 sq feet for data only
  - 1 per 3,000 sq feet for voice, location
- Radio Resource Management
  - Adaptive channel / power coverage
  - Operational simplicity

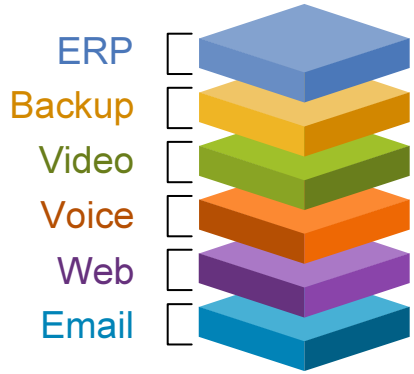


Several Supported Apps



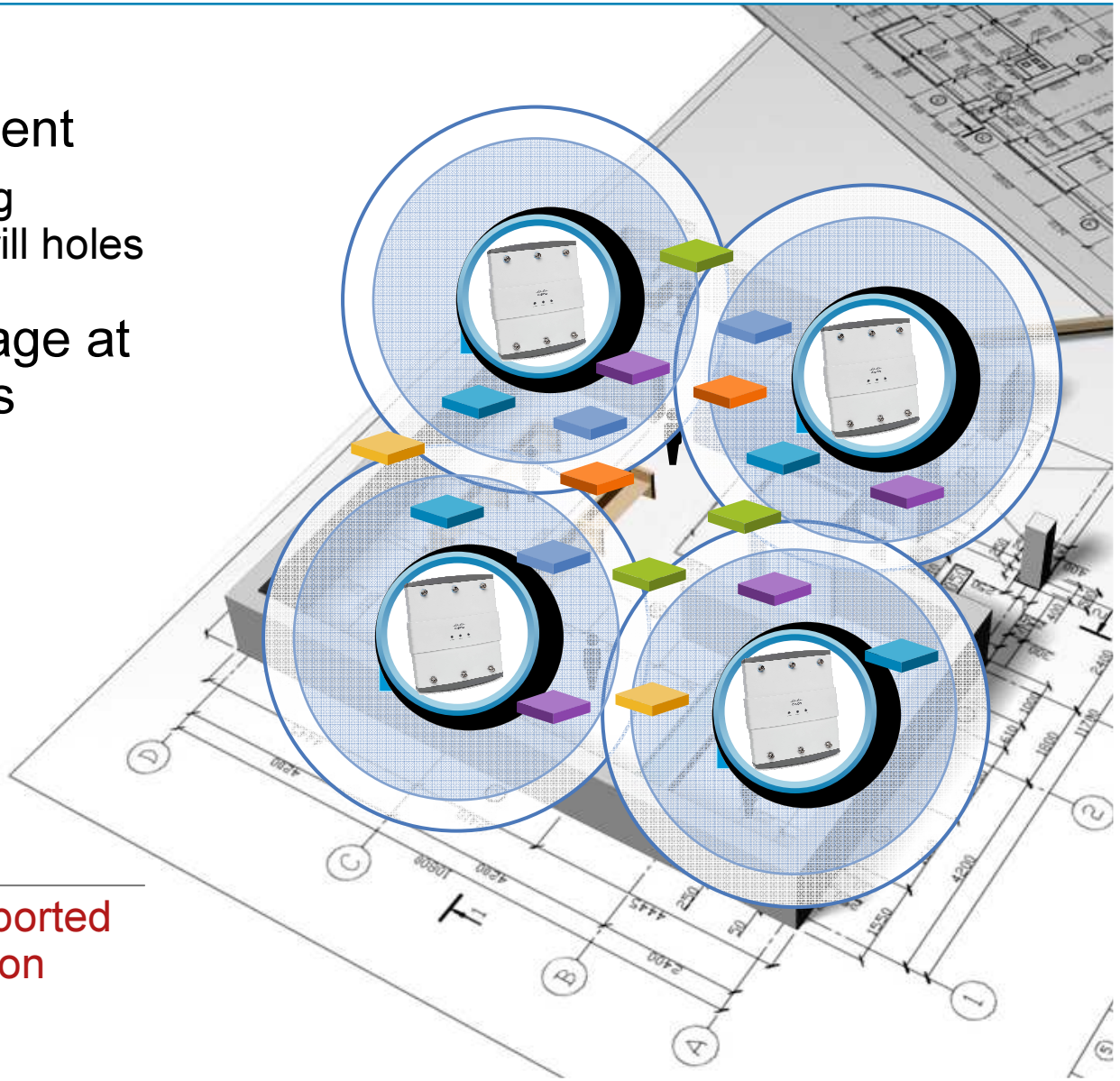
Access Point Placement

- 1 for 1 replacement
  - 1250 reuses existing Cisco AP bracket drill holes
- Improved coverage at higher data rates



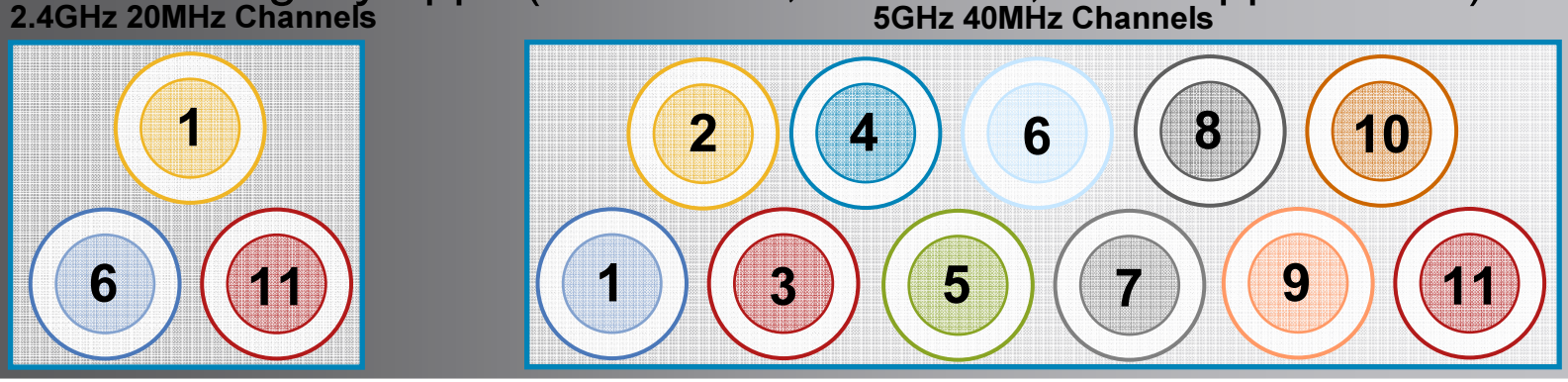
Supported Apps

More Applications Supported at Any Given Location



Effective Frequency Use—5GHz and 2.4GHz
Create a 5GHz Strategy

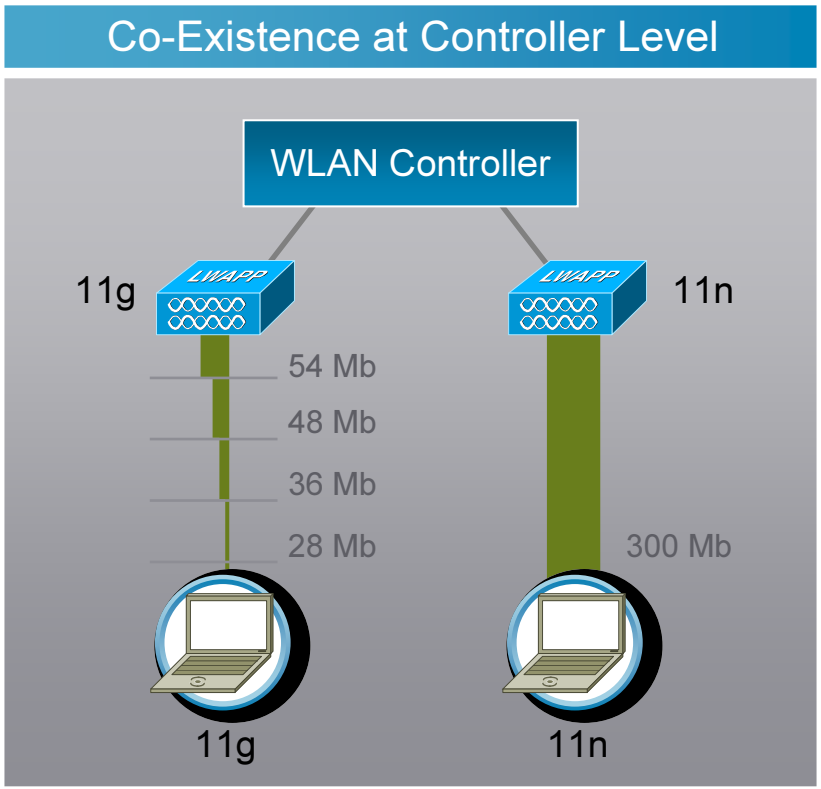
- 5GHz Recommended for 802.11n
  - More available spectrum—greater number of channels
  - Benefits from 40MHz channels, although 20MHz still works well
  - Many 11n devices only support 40MHz in 5GHz, although Cisco supports 40MHz in both 2.4GHz and 5GHz
- 2.4GHz still benefits from MIMO and packet aggregation
  - Ideal for legacy apps (handhelds, scanners, med. applications)

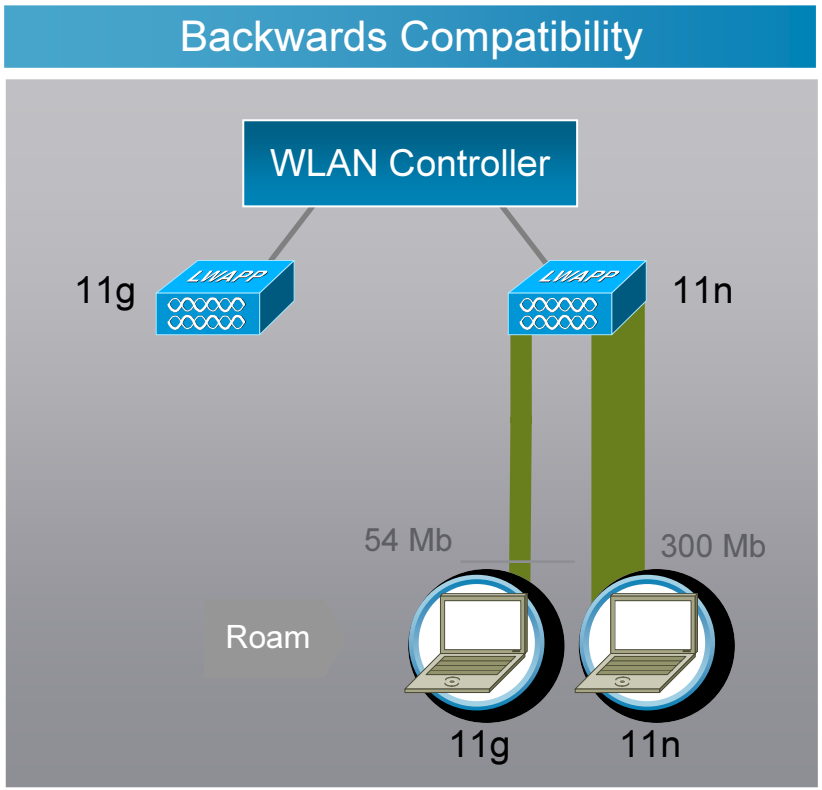


Backward Compatibility & Co-Existence

- Co-existence of ABG/N APs
- Benefits of 11n accrue to ABG clients

  MIMO benefits ABG clients on the AP receive side from MRC



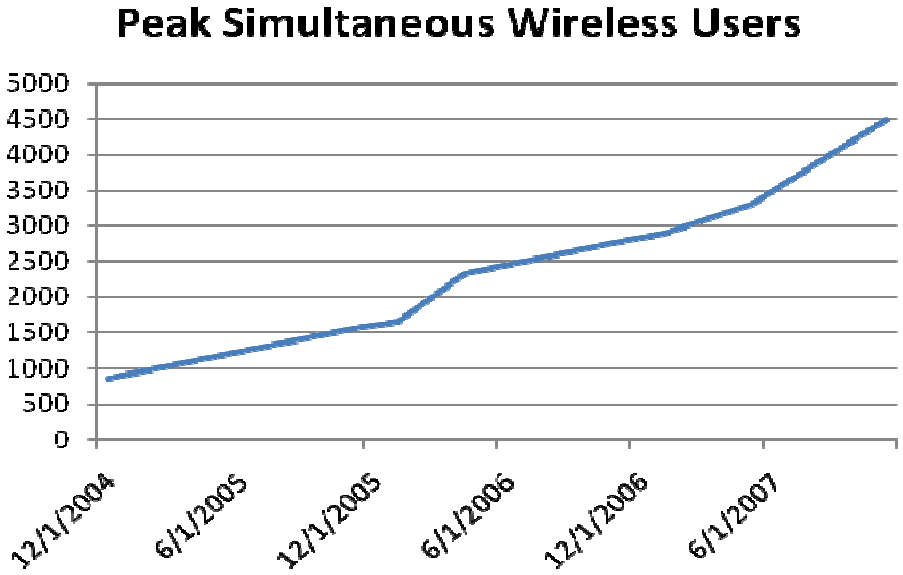


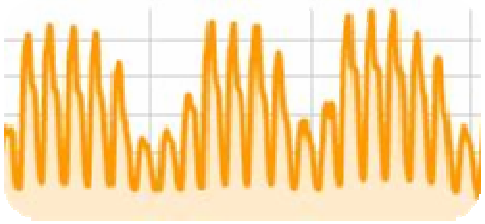
Duke University – 802.11n Experiences

- Increase in wireless connectivity
- Decrease in wired use

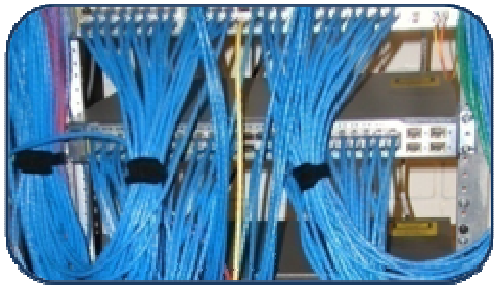
  Public wired ports (library) completely unused

- Increased need for mobility





Current infrastructure

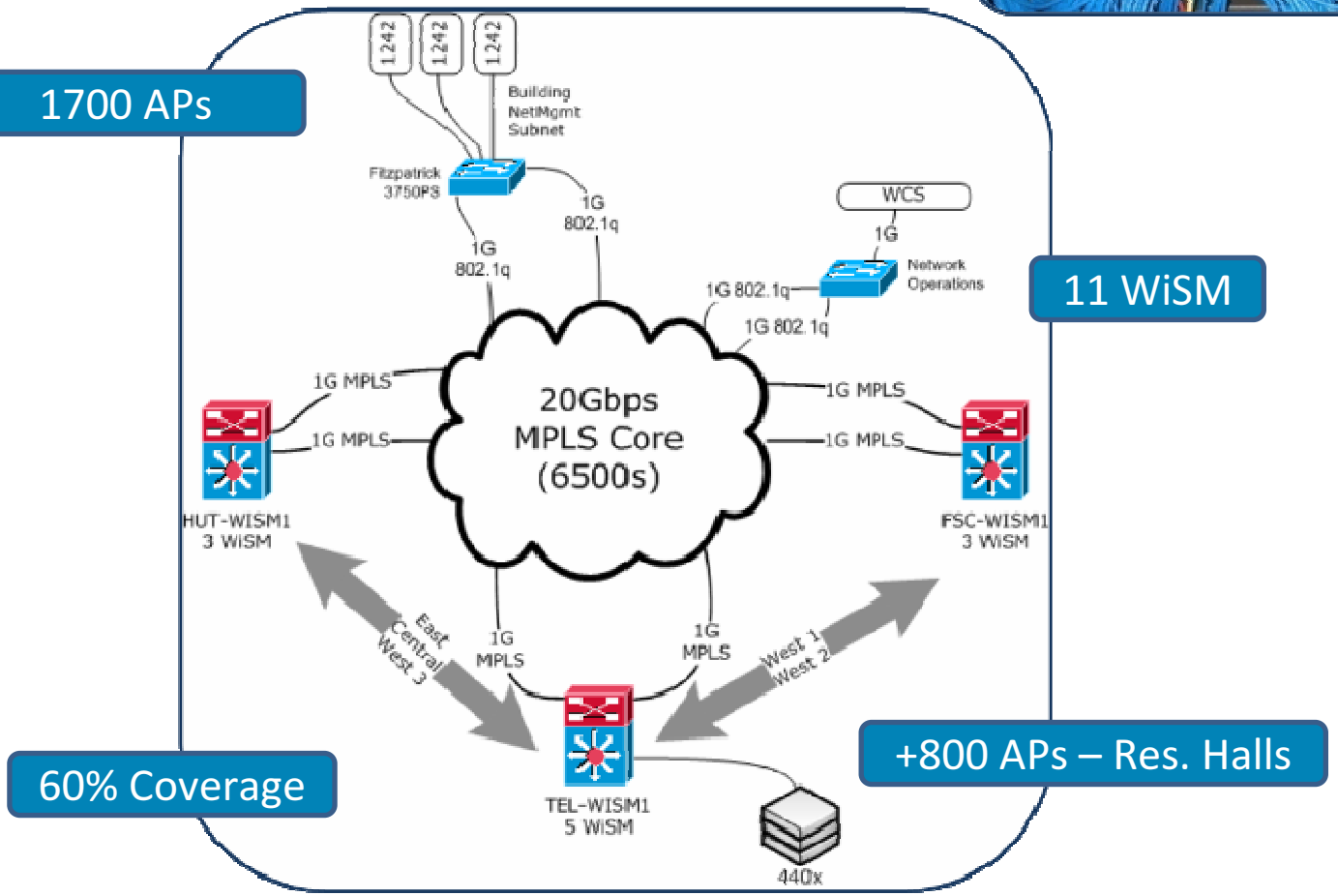


1700 APs

11 WiSM

60% Coverage

+800 APs – Res. Halls



802.11n Pilot Experiences

- 40%+ connecting with 802.11n
  - MacBook
  - Dell, Lenovo, others
- 129Mbps+ peak throughput (11n clients)
- 802.11g client: 2x faster on 11n AP compared to 11g AP
  - Especially pronounced at greater distances

802.11n Migration Considerations

802.11 Coexistence

- Legacy
  - Frames in 802.11a/g/b format
  - Backwards compatibility
  - 20 MHz channel support only
- Mixed
  - Supports 802.11n HT-mode and legacy clients
  - Legacy preamble followed by option of HT or legacy format
  - 20 and 40 MHz channel support
- Greenfield
  - Supports only 802.11n HT-mode clients – Perhaps different channels
  - Legacy preamble enables 802.11 devices to detect
  - 20 and 40 MHz channel support

Power Options for 802.11n

Power Options

- Cisco Enhanced PoE
  - Full power for dual radios from a single switch port
  - Today on Catalyst 3750-E, 3560-E, 4500 & 6500
- Power injector; AC power
- Standard 802.3af
  - Hang around for the product update!

Power Myth – Beware False Claims!

- 802.3af cannot fully power available 11n silicon
- Alternative solutions fall short:
  - Up to 60% reduction in coverage area
  - Reduction in throughput (disable transmitters, reduce CPU clock rate, etc.)
  - A loss of services (e.g. security)

Wrapping it up

An Architectural Approach - In Summary

- Be ready to explore business requirements, communicate capabilities to your clients.
- Cisco PIN's, CVD's reduce complexity by providing tested templates that are right sized.
- Wireless Security needs to be pervasive from the client to the infrastructure.
- 802.11n it's not just about speed.