



An Architectural Approach to Secure Mobility



Cisco Technology Solutions 2008

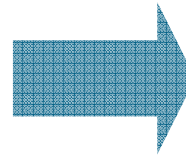
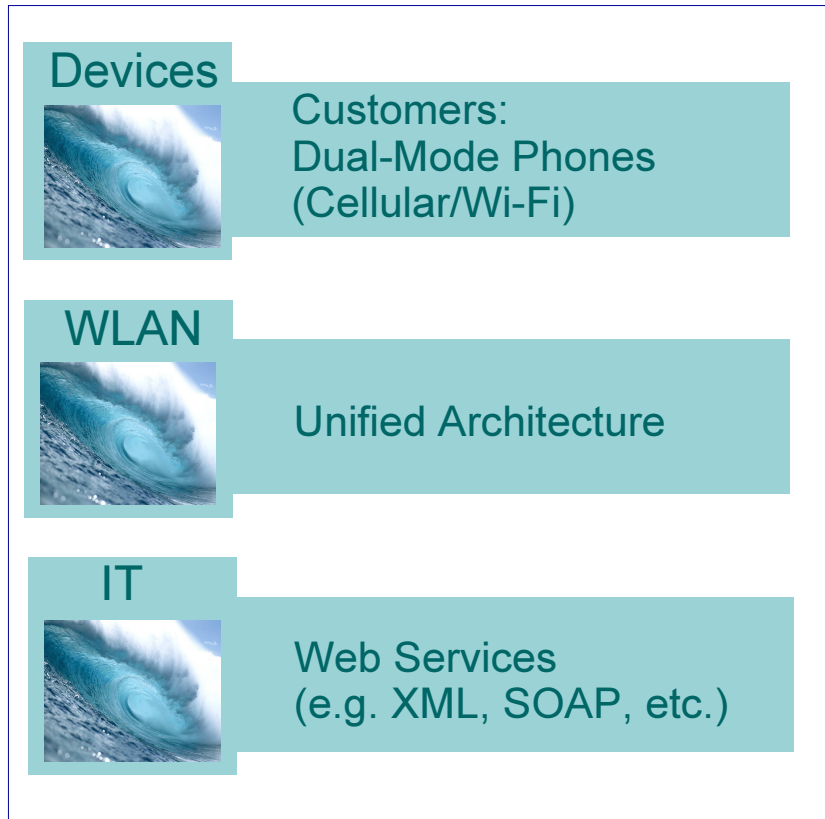
Peter Thomas



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

Greet Customers as They Walk by Store Premises

**Mobile Personal
Assistant Launcher**



**Customer
away from Store**



**Customer
Nearby Store**

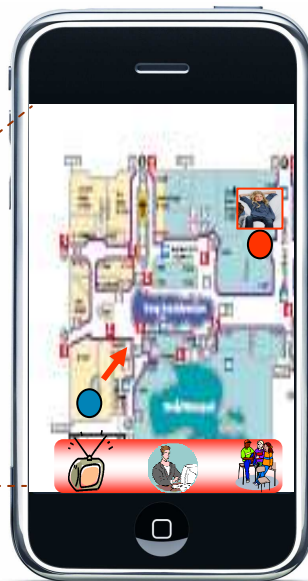



A Better Shopping Experience:

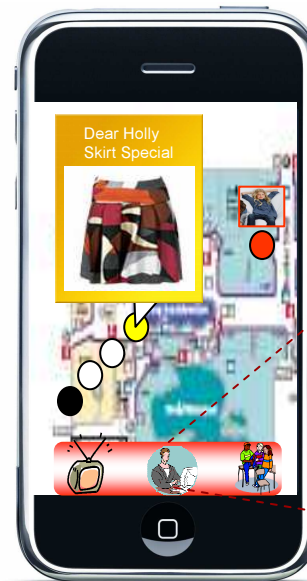
In-Store
Concierge





Store
Navigator




Smart
Ads




Customer
Service



Help Customers Find Items More Easily



**Shopping List
(item lookup)**



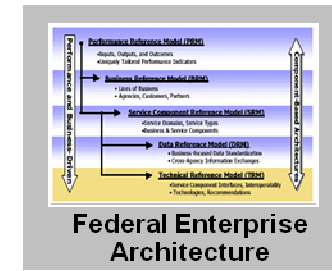
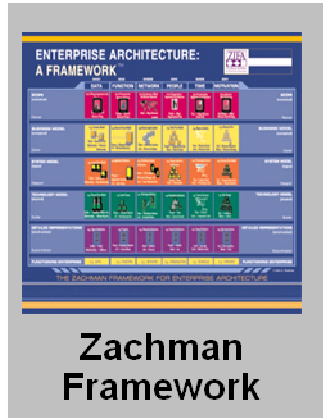
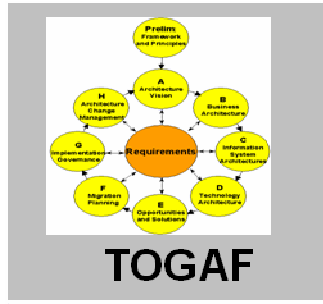
**Store
Navigator**



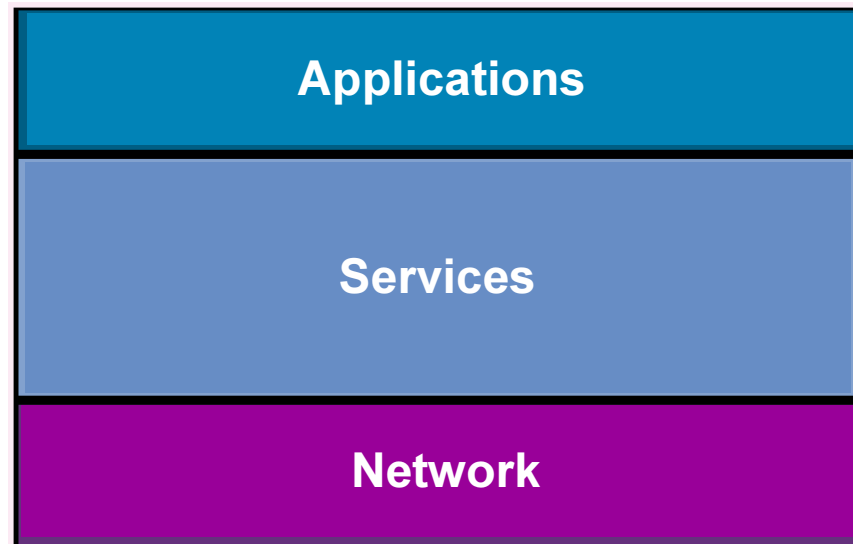
An Architectural Approach



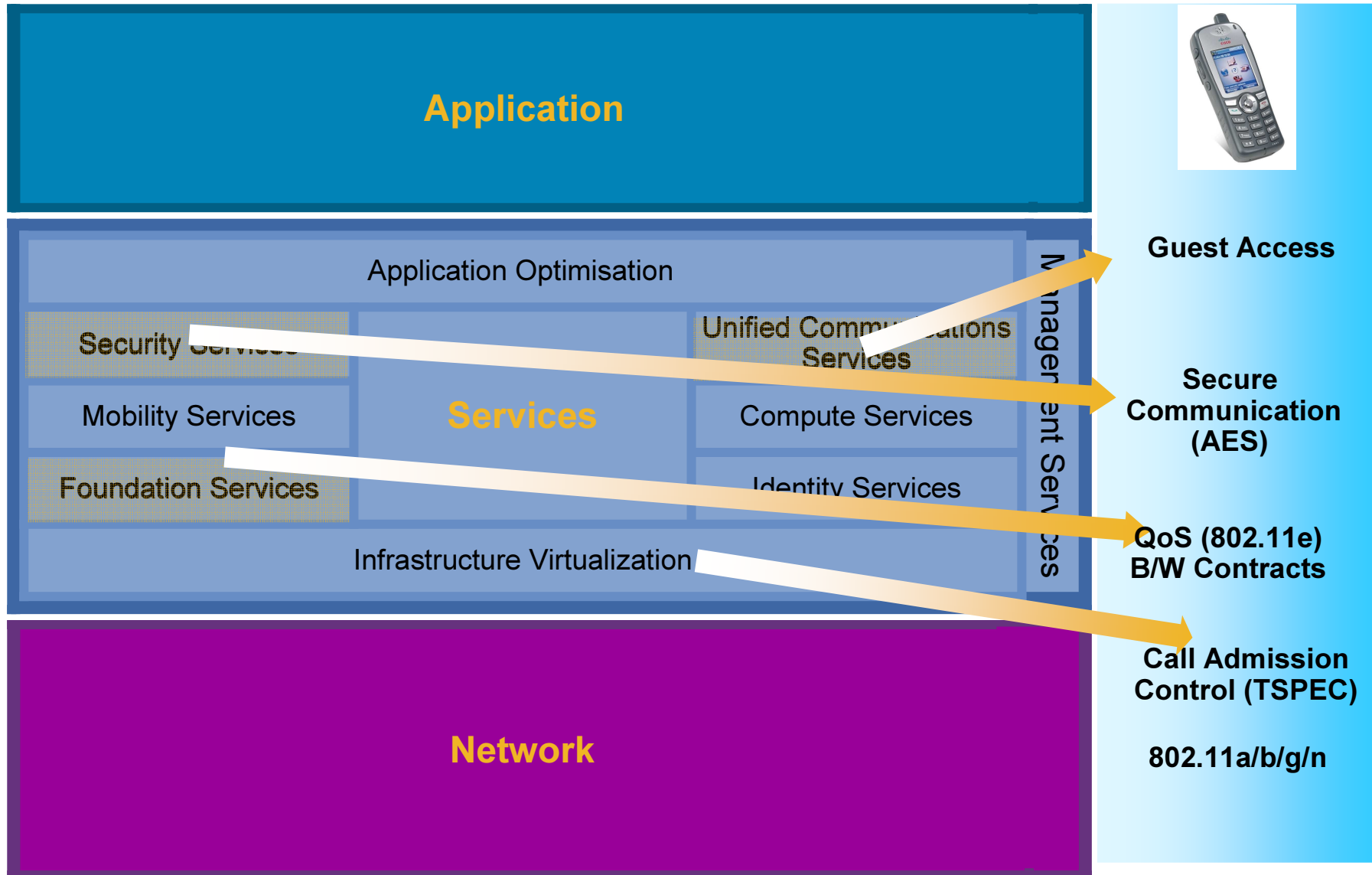
Enterprise Architectures And The Network



More than Just Connectivity



The Network as The Platform for ...

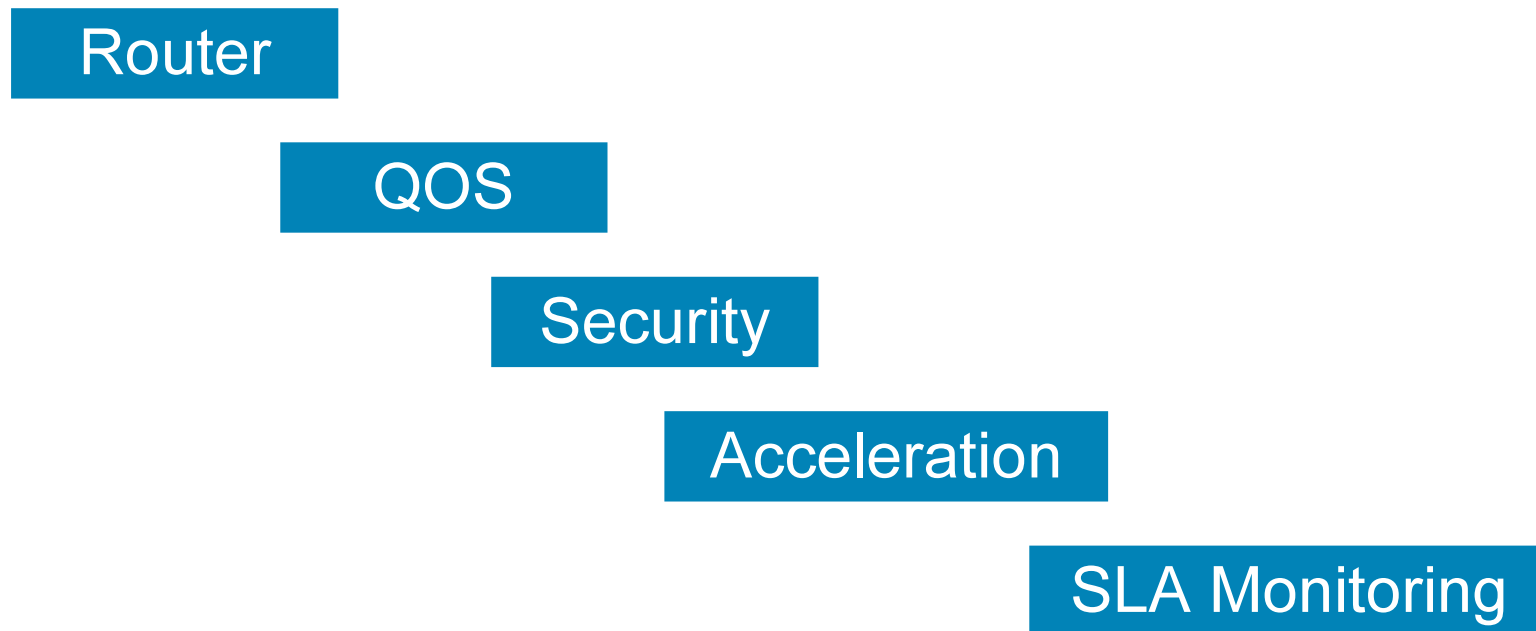


What happens without N/W Architecture

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.

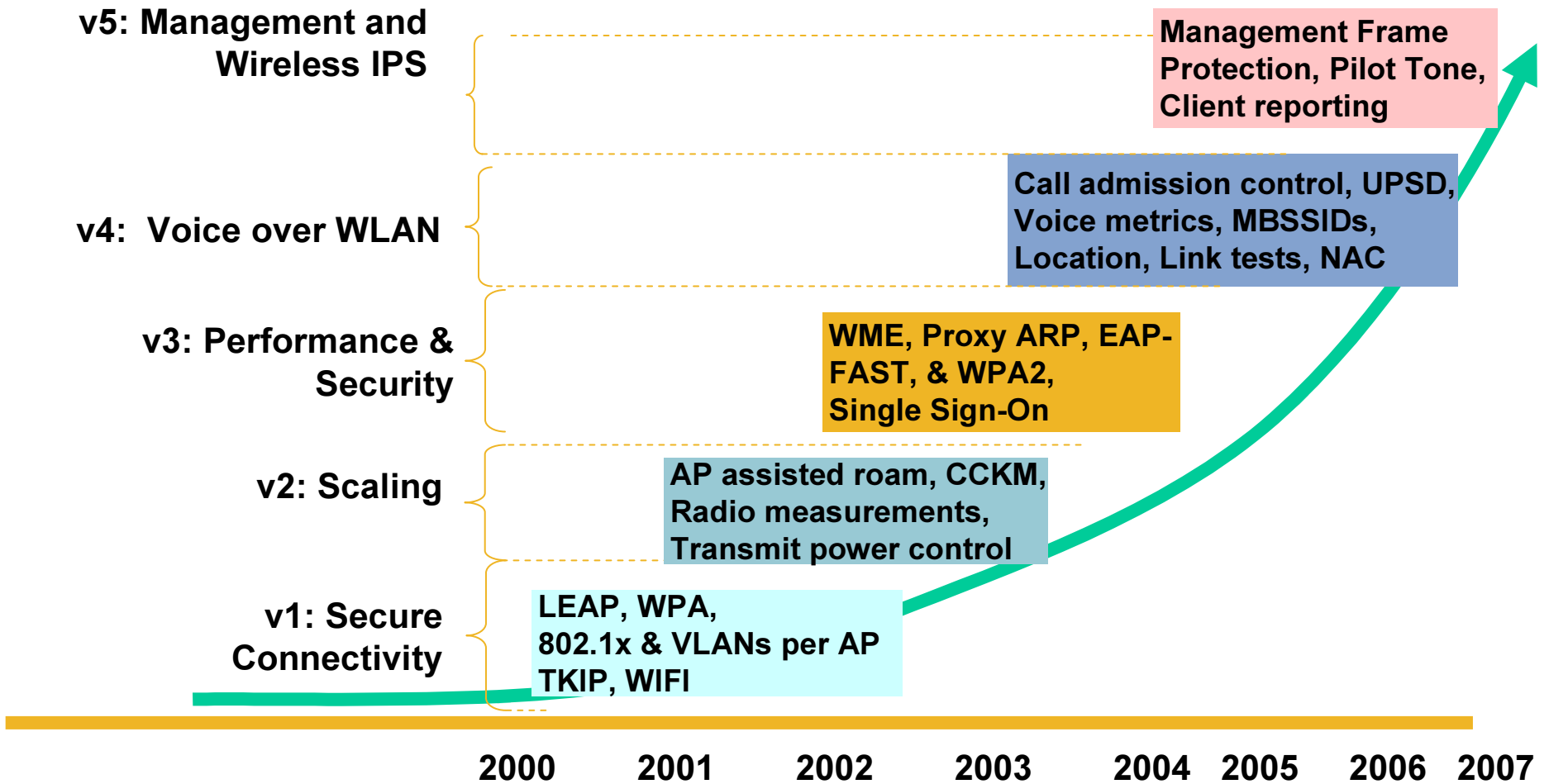
- Coverage areas – indoors and outdoors

- Be aware of what your clients are being sold.

Decouple Client Devices from Infrastructure

Set standards such as CCX compliance to reduce integration risks.

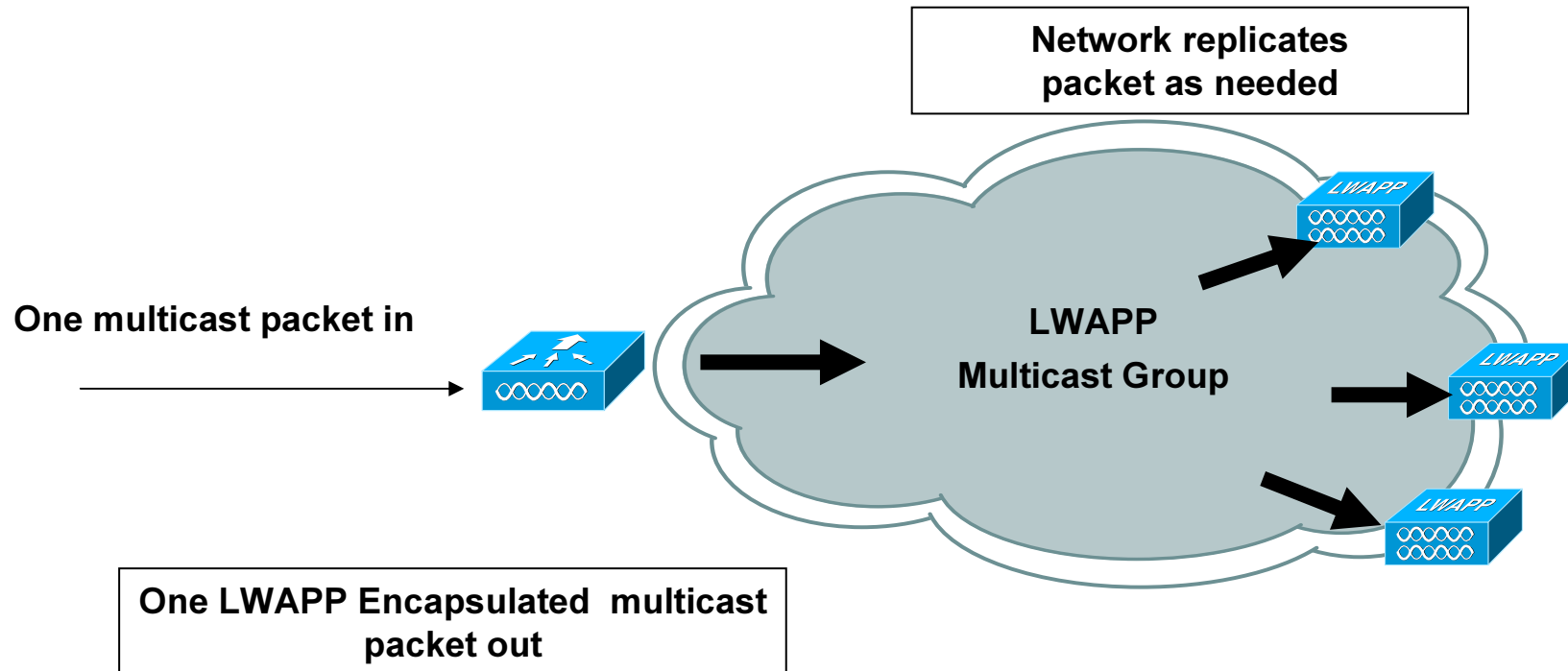
Cisco Client Extensions (CCX) releases 1-5



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



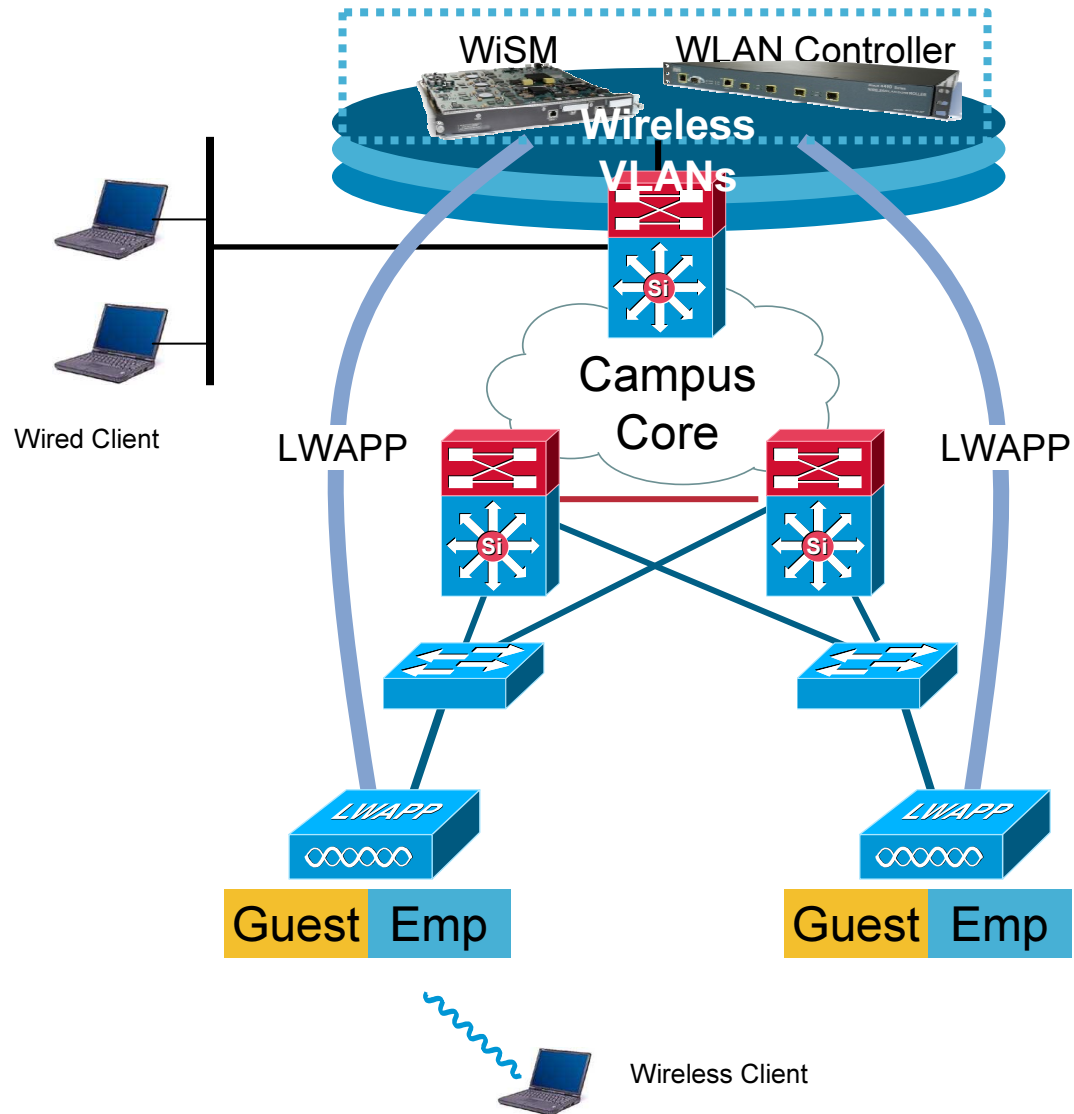
- Improved multicast performance over wireless networks
- Multicast packet replication occurs only at points in the network where it is required, saving wired network bandwidth

Multicast

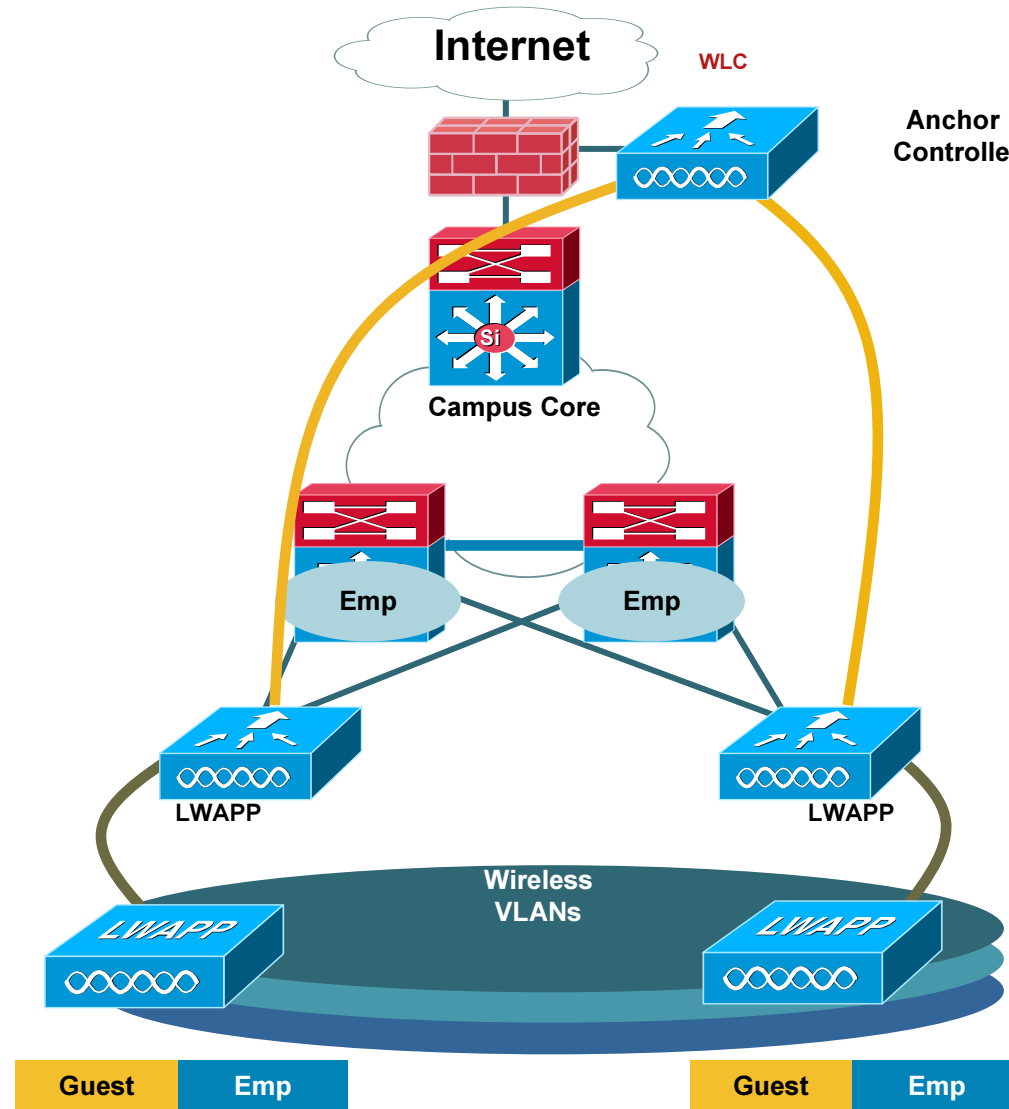
The screenshot displays the Cisco WLC GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar lists various configuration categories, with 'Multicast' selected. The main content area shows the 'Multicast' configuration page, which includes options for 'Enable IGMP Snooping' and 'IGMP Timeout (seconds)'. Below this, the 'Monitor' section is active, showing a 'Multicast Group Detail' view. This view displays the 'Number of Clients' as 2 and lists their MAC addresses: 00:12:f0:7c:a3:47 and 00:12:f0:7c:a3:fd. At the bottom, a 'Layer2 MGID(Multicast Group ID) Mapping' table is shown.

InterfaceName	vlanId	MGID
management	60	0
vlan11	11	9
vlan12	12	10
voice	13	8

Unified Wired and Wireless Guest Access



Unified Wired and Wireless Guest Access





Lobby Ambassador Controls

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains navigation options: AAA, Change Password, Local Password Policy, AAA Mode, Users, Groups, Active Sessions, TACACS+, and RADIUS. The main content area is titled "Users" and has two tabs: "General" and "Lobby Ambassador Defaults". The "Lobby Ambassador Defaults" tab is active, showing "Defaults for creating Guest User accounts".

Configuration fields include:

- Profile: dropdown menu set to "guest"
- User Role: dropdown menu set to "default"
- Lifetime: radio buttons for "Limited" (selected) and "Unlimited"; input fields for "8" Hour and "0" Min.
- Apply To: dropdown menu set to "Controller List"
- Controller List: a table with checkboxes for "IP Address" and "Name", and a row for "172.20.225.138 Cisco_ff:e7:cb".
- Email Id: empty text field
- Description: text field containing "Wireless Network Guest Access"
- Disclaimer: text area containing "Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network"
- Defaults editable: checkbox for "Enable" (unchecked)
- Max User Creations Allowed: checkbox for "Enable" (checked)
- Input: "10" Guest User(s) per "8" hour(s)

At the bottom, a note states: **Not selecting a profile will not configure defaults for this Lobby Ambassador. He/She will still be able to create Guest Accounts.*

Alarm Summary

Category	0	0	0	Count
Malicious AP	0	0	0	34
Coverage Hole	0	0	0	0
Security	3	0	0	0
Controllers	0	2	0	0
Access Points	7	0	2	0
Location	0	0	3	0
Mesh Links	0	0	0	0
WCS	0	0	0	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

All APs
General
General
AP
Local
Ethernet
Base
Sta
AP
Op
Por
Pri
Sec

en1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: tcp.port eq 80

No.	Time	Source	Destination	Protocol	Info
53	6.916738	207.142.131.235	192.168.1.30	TCP	80 > 65155 [ACK] Seq=1 Ack=450 Win=6864 Len=0 TSV=3117138150 TSER=710995743
54	6.961542	207.142.131.235	192.168.1.30	HTTP	HTTP/1.0 304 Not Modified
55	6.961666	192.168.1.30	207.142.131.235	TCP	65155 > 80 [ACK] Seq=450 Ack=422 Win=65535 Len=0 TSV=710995744 TSER=3117138194
56	6.972635	192.168.1.30	207.142.131.235	TCP	65155 > 80 [FIN, ACK] Seq=450 Ack=422 Win=65535 Len=0 TSV=710995744 TSER=3117138194
59	7.239480	207.142.131.235	192.168.1.30	TCP	80 > 65155 [FIN, ACK] Seq=422 Ack=451 Win=6864 Len=0 TSV=3117138473 TSER=710995744
60	7.254723	192.168.1.30	207.142.131.228	TCP	65156 > 80 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=710995745 TSER=0
61	7.522182	207.142.131.228	192.168.1.30	TCP	80 > 65156 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1420 TSV=187437131 TSER=71099574
62	7.522345	192.168.1.30	207.142.131.228	TCP	65156 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSV=710995745 TSER=187437131
63	7.523120	192.168.1.30	207.142.131.228	HTTP	GET /wikipedia/en/f/fb/Ws/icon48.png HTTP/1.1
64	7.794383	207.142.131.228	192.168.1.30	TCP	80 > 65156 [ACK] Seq=1 Ack=375 Win=6864 Len=0 TSV=187437403 TSER=710995745
65	7.796209	207.142.131.228	192.168.1.30	HTTP	HTTP/1.0 304 Not Modified
66	7.796322	192.168.1.30	207.142.131.228	TCP	65156 > 80 [ACK] Seq=375 Ack=338 Win=65535 Len=0 TSV=710995746 TSER=187437404
67	7.797664	192.168.1.30	207.142.131.228	TCP	65156 > 80 [FIN, ACK] Seq=375 Ack=338 Win=65535 Len=0 TSV=710995746 TSER=187437404
68	8.039561	207.142.131.235	192.168.1.30	TCP	80 > 65155 [FIN, ACK] Seq=422 Ack=451 Win=6864 Len=0 TSV=3117139274 TSER=710995744
69	8.039704	192.168.1.30	207.142.131.235	TCP	65155 > 80 [ACK] Seq=451 Ack=423 Win=65535 Len=0 TSV=710995746 TSER=3117139274
70	8.065048	207.142.131.228	192.168.1.30	TCP	80 > 65156 [FIN, ACK] Seq=338 Ack=376 Win=6864 Len=0 TSV=187437674 TSER=710995746
71	8.868153	207.142.131.228	192.168.1.30	TCP	80 > 65156 [FIN, ACK] Seq=338 Ack=376 Win=6864 Len=0 TSV=187438478 TSER=710995746
72	8.868306	192.168.1.30	207.142.131.228	TCP	65156 > 80 [ACK] Seq=376 Ack=339 Win=65535 Len=0 TSV=710995748 TSER=187438478

Frame 47 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: 00:0d:93:ef:49:30 (00:0d:93:ef:49:30), Dst: 00:14:bf:76:2e:ca (00:14:bf:76:2e:ca)

Internet Protocol, Src: 192.168.1.30 (192.168.1.30), Dst: 207.142.131.235 (207.142.131.235)

Transmission Control Protocol, Src Port: 65155 (65155), Dst Port: 80 (80), Seq: 0, Len: 0

```
0000 00 14 bf 76 2e ca 00 0d 93 ef 49 30 08 00 45 00  ...v... ..10..E.
0010 00 3c d3 09 40 00 40 06 52 72 c0 a8 01 1e cf 8e  ...<..@.@. Rr....
0020 83 eb fe 83 00 50 82 b3 18 27 00 00 00 00 a0 02  ....P.....
0030 ff ff a2 98 00 00 02 04 05 b4 01 03 03 00 01 01  ....
0040 08 0a 2a 60 ef 1f 00 00 00 00 00 00 00 00 00 00  ...*.....
```

en1: <live capture in progress> file: /var/tmp/etherByLjIBHbJ9 14 KB P: 80 D: 22 M: 0

What's WCS?

My WCS Home - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Username: pethomas | Logout | Refresh | Print View

Wireless Control System

Monitor Reports Configure Location Administration Tools Help

WCS Home [Edit Tabs](#) [Edit Contents](#)

General Client Security Mesh

Inventory Detail Status

Controllers: [2](#) Radios: [111](#) Location Servers: [1](#)

Client Count

6h 1d 1w 2w 4w 3m 6m 1y Custom

Coverage Areas

Name	Total APs	a/n Radios	b/g/n Radios	OOS Radios	Clients
Cisco San Jose - Site 5	56	56	55	1	473

[View All Maps](#)

Recent Coverage Holes (0)

No Coverage Holes found

Alarm Summary

Category	Count	Severity
Malicious AP	0	0
Coverage Hole	0	0
Security	793	0
Controllers	0	0
Access Points	2	0
Location	0	0
Mesh Links	0	0
WCS	0	0

Client Troubleshooting Tool

- 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

The top screenshot shows the 'Summary' tab for client '00:13:ce:45:db:4a'. The process flow is: 802.11 Association (green), 802.1X Authentication (red), IP Address Assignment (grey), and Successful Association (grey). The 'Problem' section indicates '802.1X Authentication Failure'. The 'Suggested Action' section lists:

- Check Radius server reachable
- Check Clients choice of EAP method is supported by radius server
- Check Clients username/password/cert is valid
- Check Server certificate valid and accepted by client

The bottom screenshot shows the 'Log Analysis' tab for client '00:11:24:a6:6c:d9'. It includes 'Start', 'Stop', and 'Clear' buttons. Below is a 'Select LogMessages' list:

- 802.11 Initialization (19)
- 802.1X Authentication (58)
- IPM Messages(2)
- DHCP Messages (18)
- AAA Messages(0)
- All (67)

 A table of log messages is displayed:

Time	Severity	Controller	Message
43	INFO	172.20.227.130	Received Access-Challenge from the RADIUS server for the client
43	INFO	172.20.227.130	Message sent from radius server to client.
43	INFO	172.20.227.130	EAP response from client to AP received .
43	INFO	172.20.227.130	Received Access-Reject from the RADIUS server for the client.
43	INFO	172.20.227.130	Received EAP Response Identity packet from the client with eap failure.
38	INFO	172.20.227.130	Received EAP Response Identity packet from the client

Client Troubleshooting

Wireless Control System

Troubleshooting Client '00:40:96:ad:0d:1b'

Summary | Log Analysis | Event History | Test Analysis | Messaging | Event Log

802.11 Association | Open Authentication | IP Address Assignment | Successful Association

Problem
None

Suggested Action
None

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

Wireless Control System

Troubleshooting Client '00:40:96:ad:0d:1b'

Summary | Log Analysis | Event History | Test Analysis | Messaging | Event Log

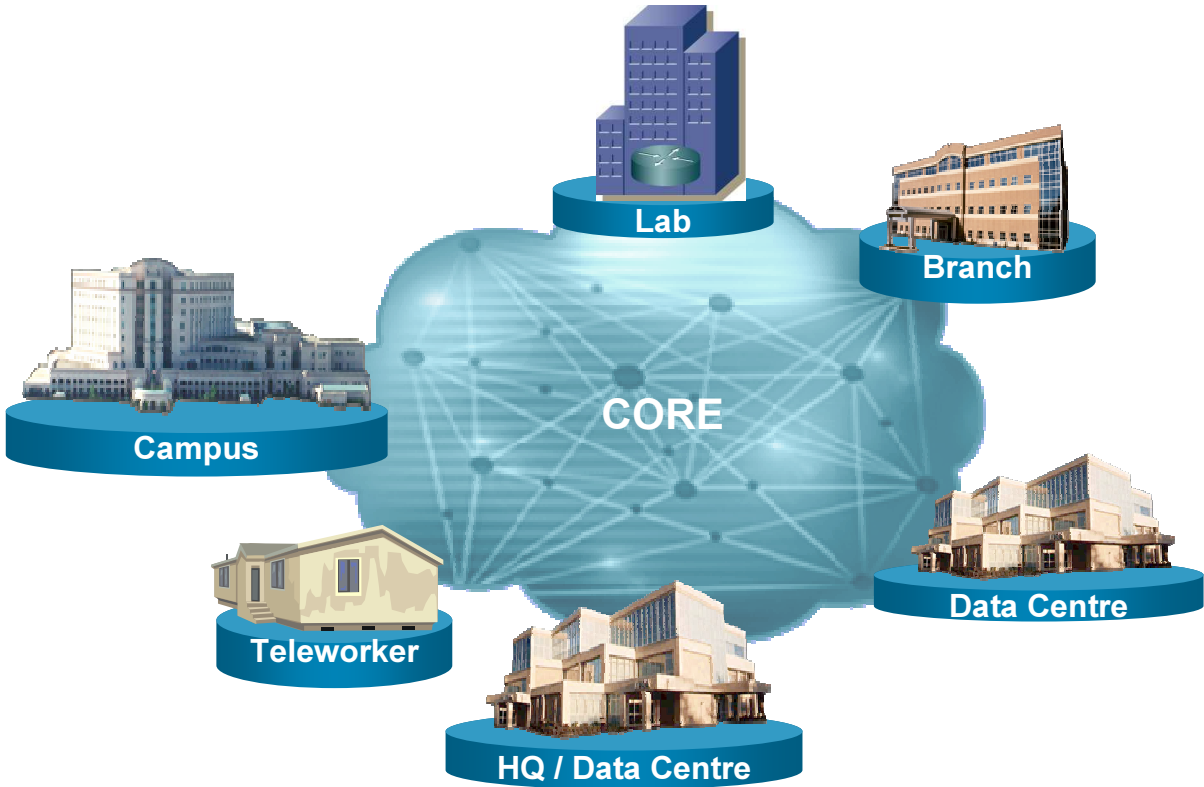
The following tests are available for clients. Use the checkboxes to select the test(s) you would like to perform, then click **Start**. Click **Stop** to halt the tests. When a test is completed, click on the test status to view the results.

Select	Diagnostic Test	Input	Status	Results
<input checked="" type="checkbox"/>	DHCP		Not initiated	None
<input checked="" type="checkbox"/>	IP Connectivity		Not initiated	None
<input checked="" type="checkbox"/>	DNS Ping		Not initiated	None
<input type="checkbox"/>	DNS Resolution	Name to resolve: <input type="text"/>	Not initiated	None
<input checked="" type="checkbox"/>	802.11 Association	AP name: <input type="text" value="AP1240-Edgewood-802.11a"/> Profile: <input type="text" value="apps-dc"/>	Not initiated	None
<input type="checkbox"/>	802.1x Authentication		Not initiated	None
<input type="checkbox"/>	Profile Redirect	Client Profile Number: <input type="text"/>	Not initiated	None

Start **Stop** **Frame**

Results:

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...













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

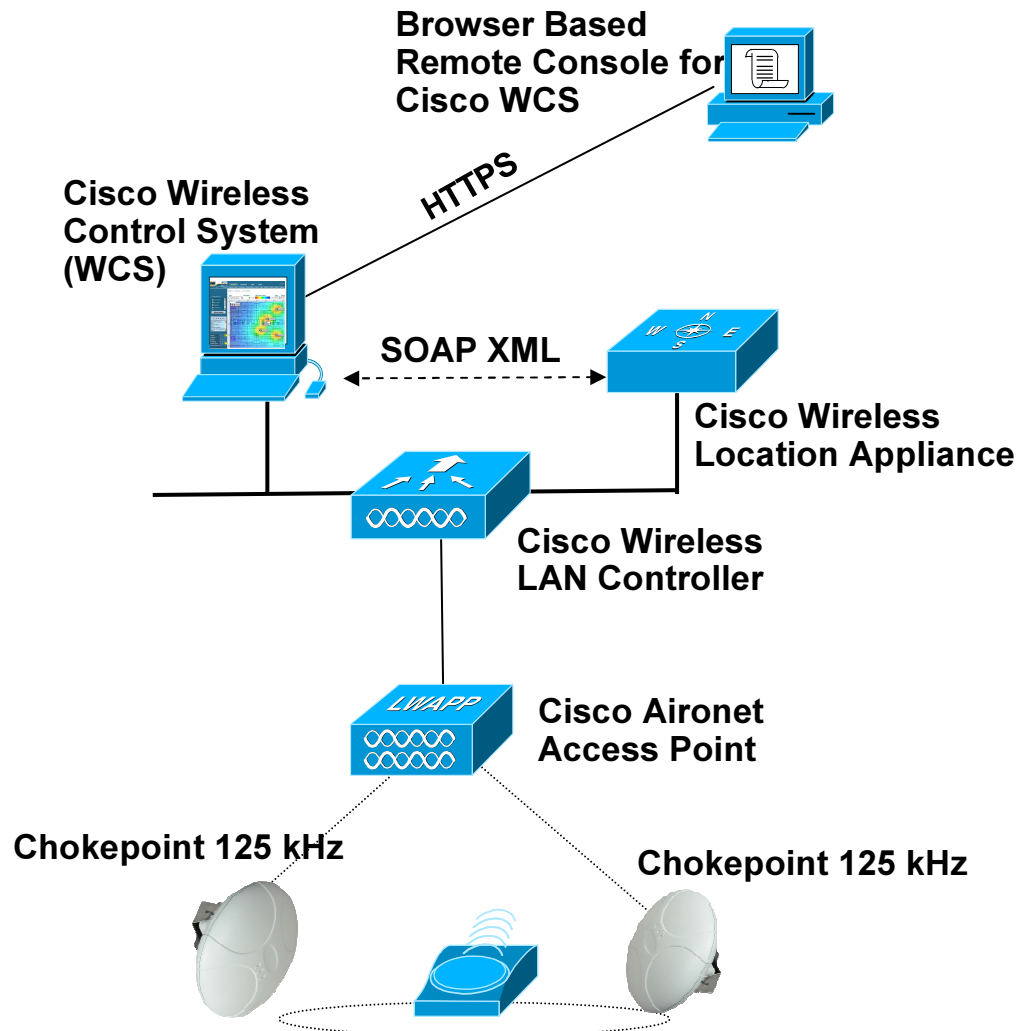
- Remember Minority Report?
- Interactive Signage
- What makes up that solution
- Applications – safety compliance

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.



Safety - Is your certification current?



**Safety Certification
Expiry**

Peter Thomas

**Stand back from the Coffee
machine! Your coffee drinking
certification is about to expire!**

Contact Coffee Operations 555



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

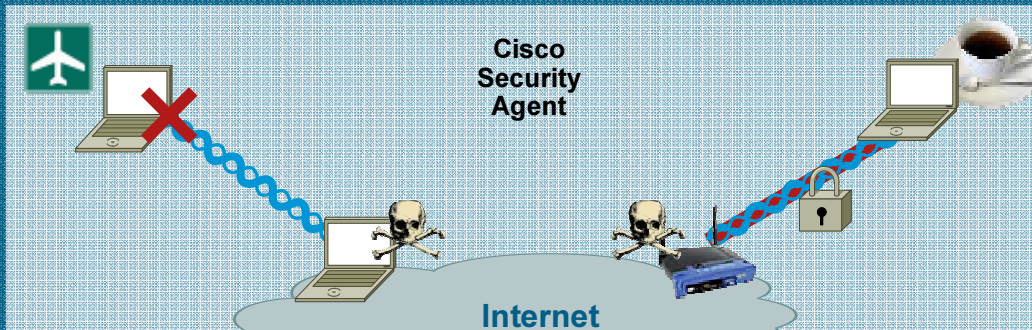
- Lightest touch on PCs – visitors may not have rights
- Compromise – provide Authentication but not confidentiality. Some enterprises using pre-shared keys to provide privacy.
- Using Lobby Ambassador capabilities – ability for designated team to create time-bombed accounts

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

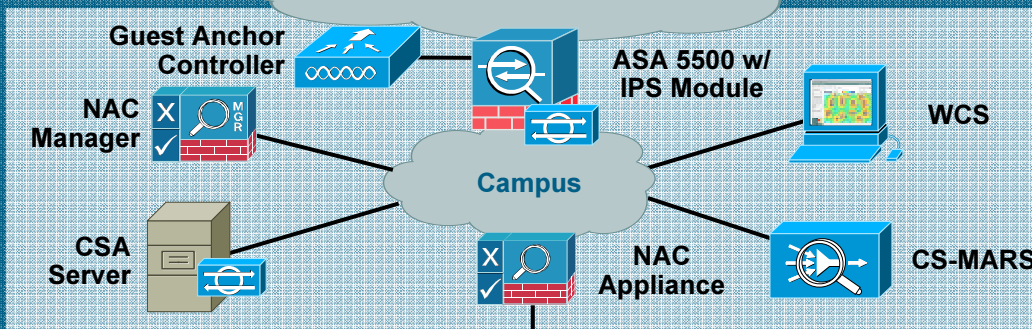
Untrusted
Public



Endpoint Protection

- Host intrusion prevention
- Endpoint malware mitigation

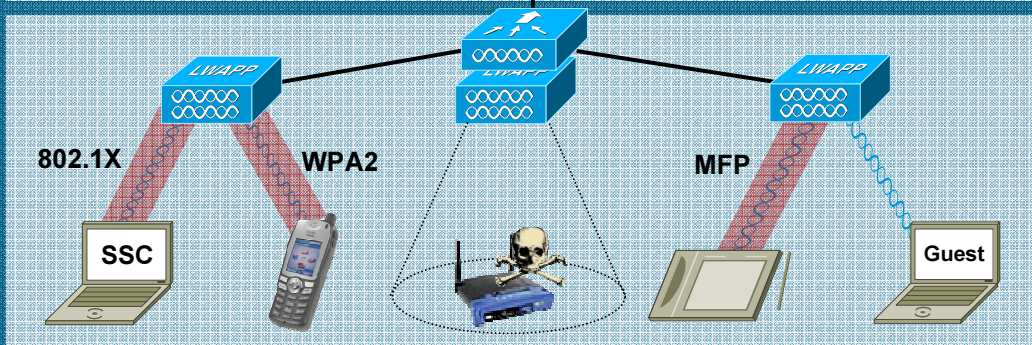
Trusted
Wired



Traffic and Access Control

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

Trusted
Wireless

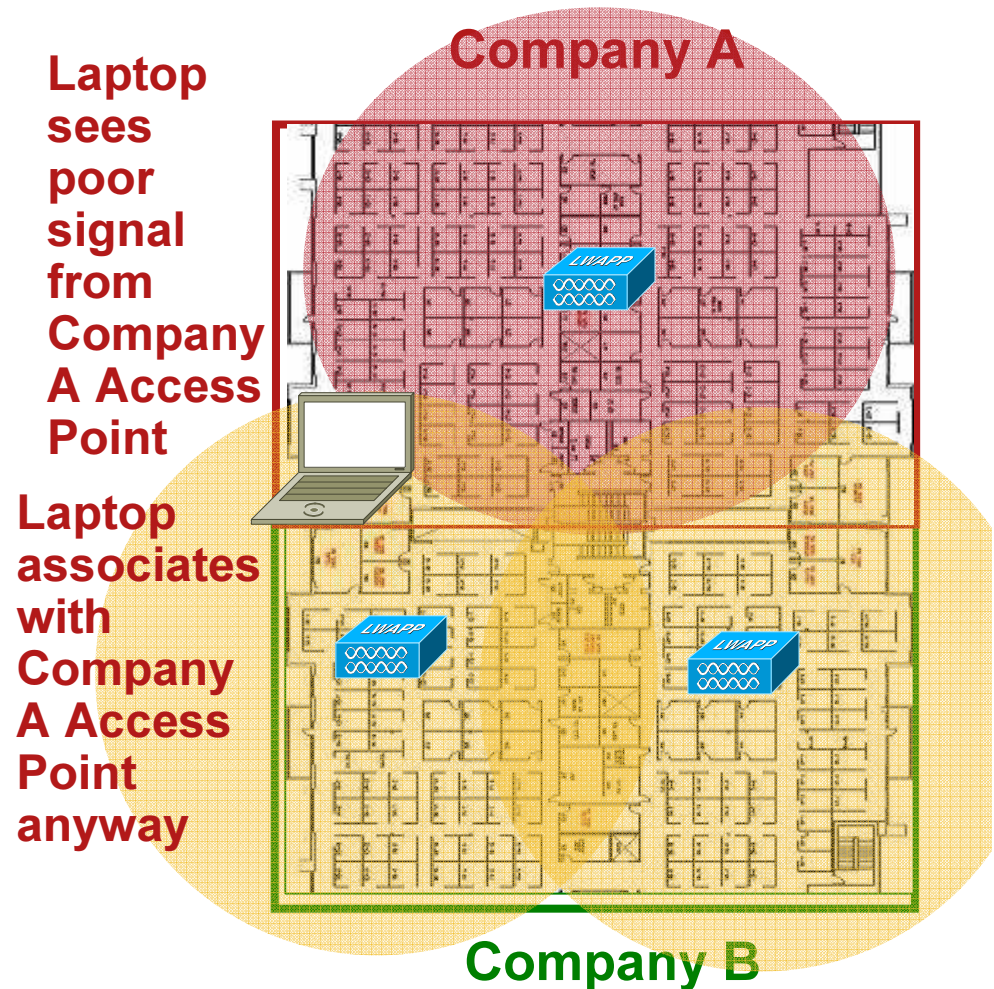


WLAN Security Fundamentals

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

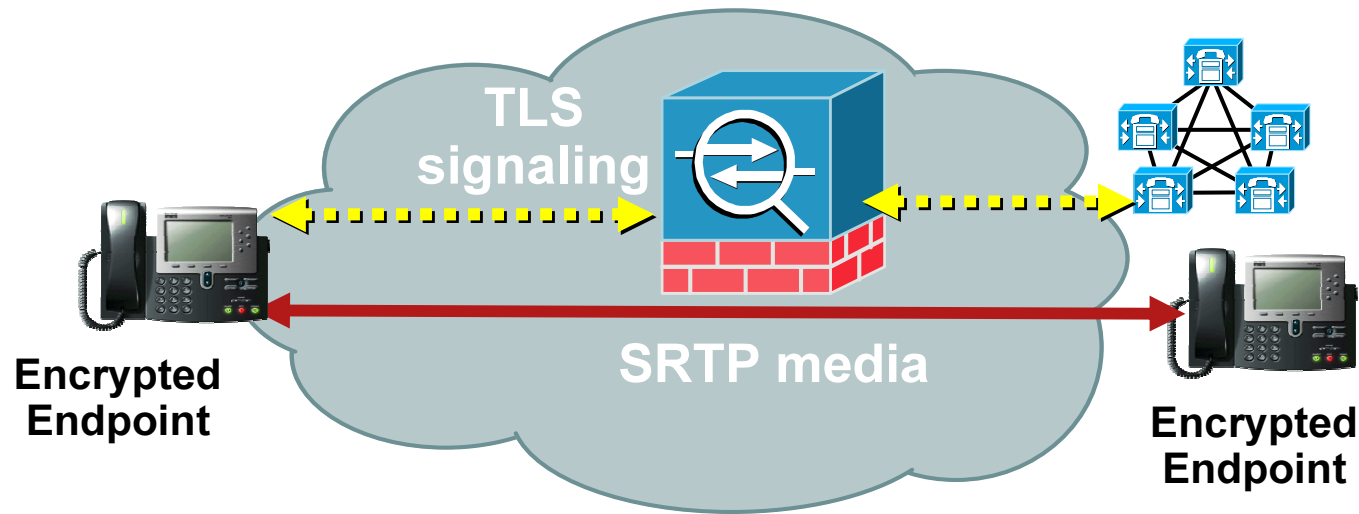
CSA Protects the Wireless Laptop

- 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

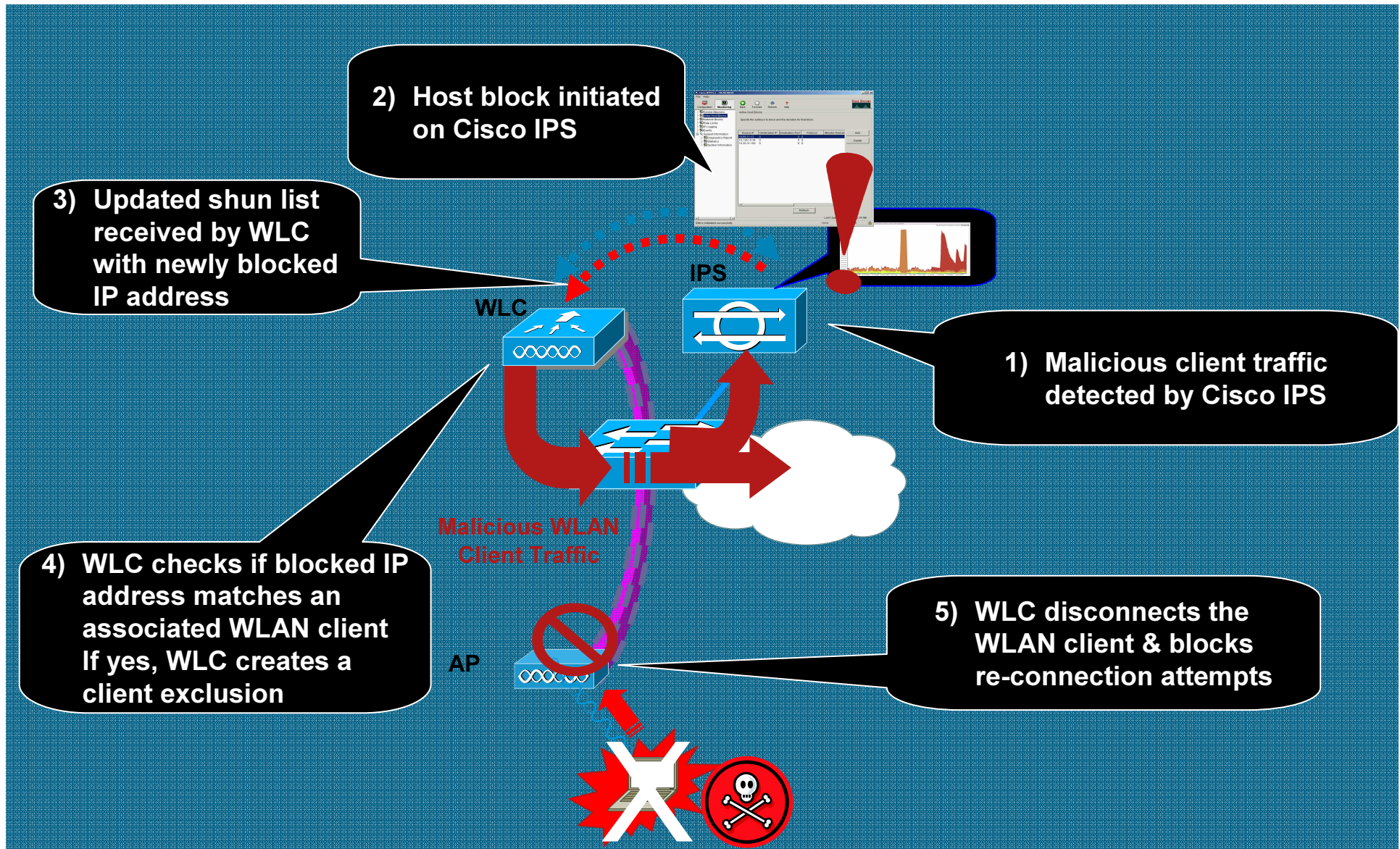
Solving the Firewall & Encryption Integration Problem



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

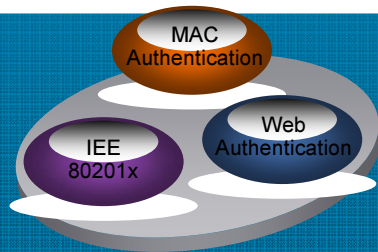
- **Maintains integrity and confidentiality** of call while enforcing security policy through advanced SIP/SCCP firewall services
- **TLS signaling is terminated and inspected**, then re-encrypted for connection to destination (leveraging integrated hardware encryption services for scalable performance)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

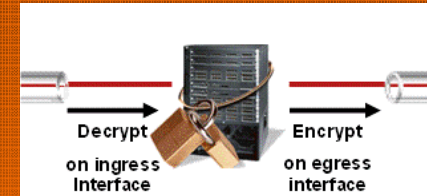
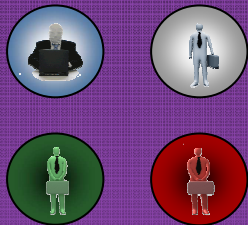
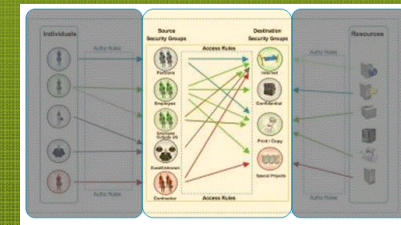


Secure Campus Access Control



Converged Policy Framework

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



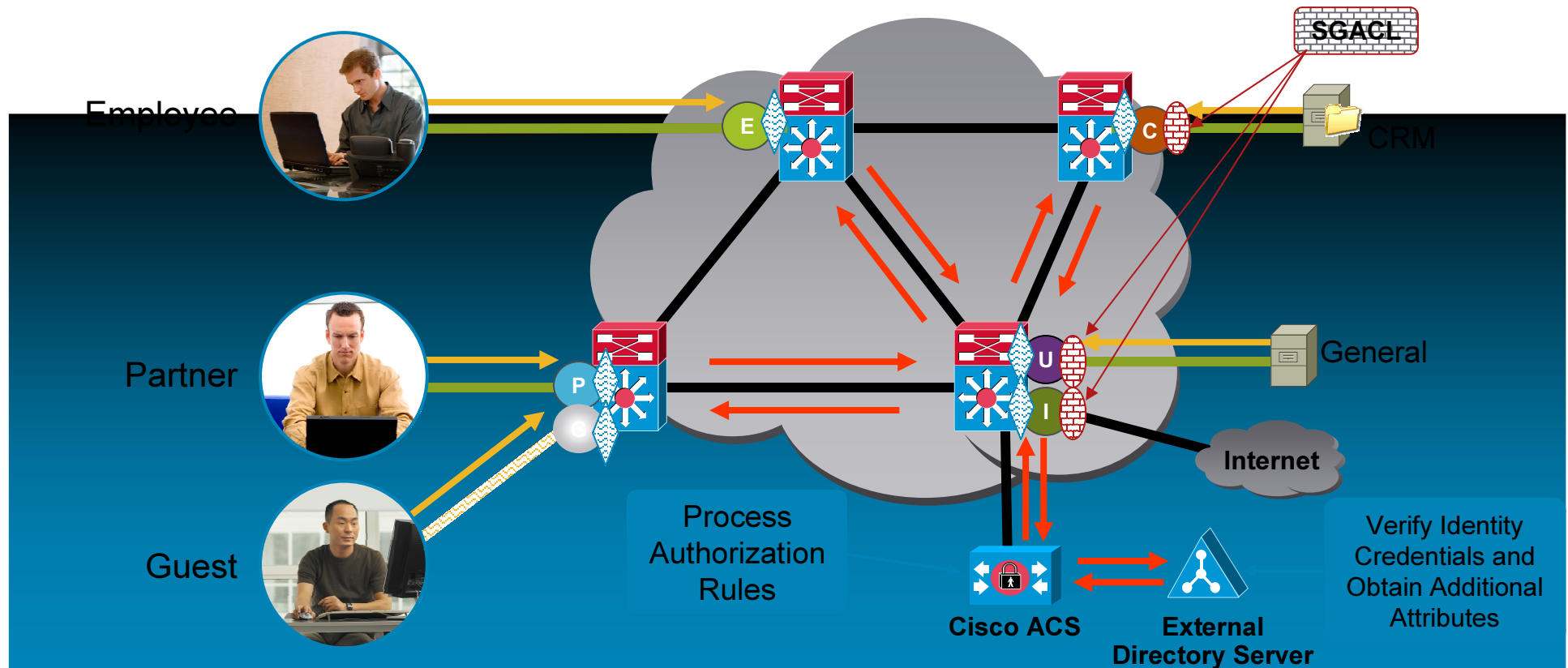
Transforming From Topology-aware to Role-aware Access Control

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

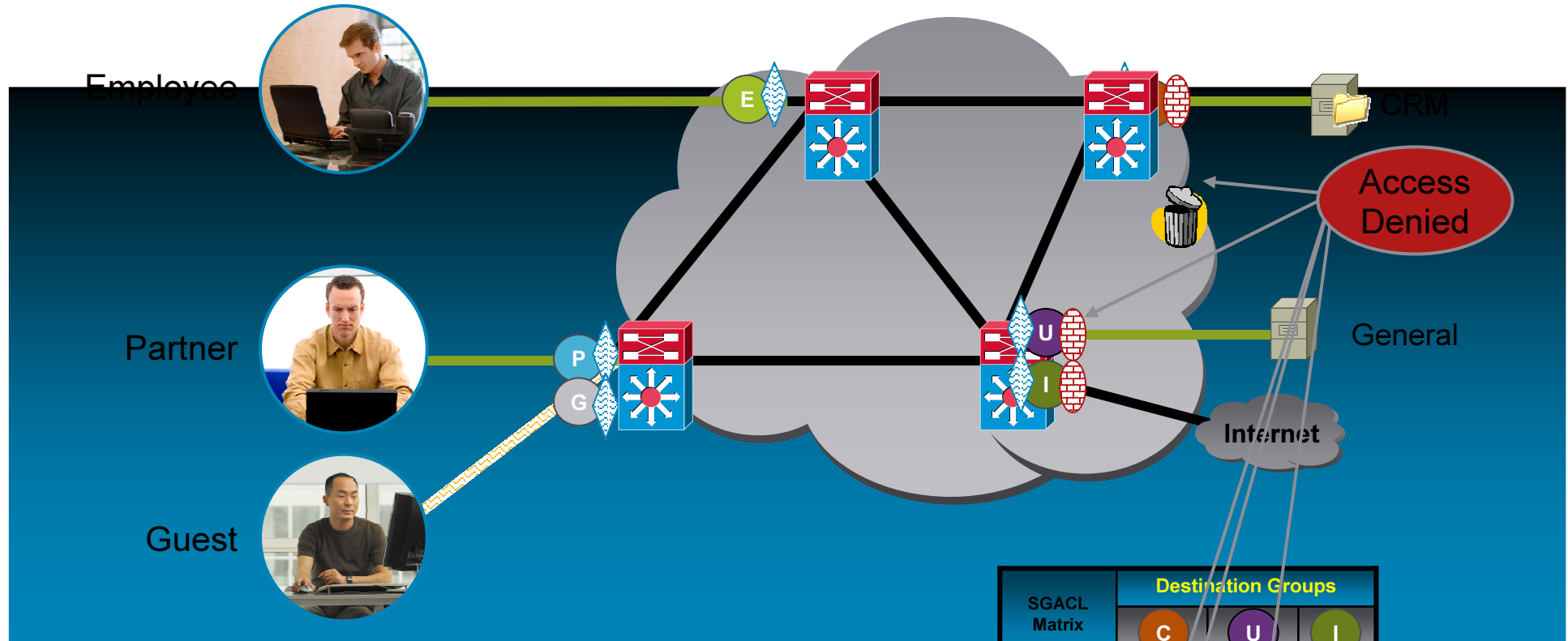


Legend

Link/Port Status		Security Group Classifications			
	Unauthenticated		Employee Group		Confidential Group
	Failed Authentication		Partner Group		Unrestricted Group
	Authenticated		Guest Group		Internet Group
	Shutdown		Ingress Tagging		Egress Filtering

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

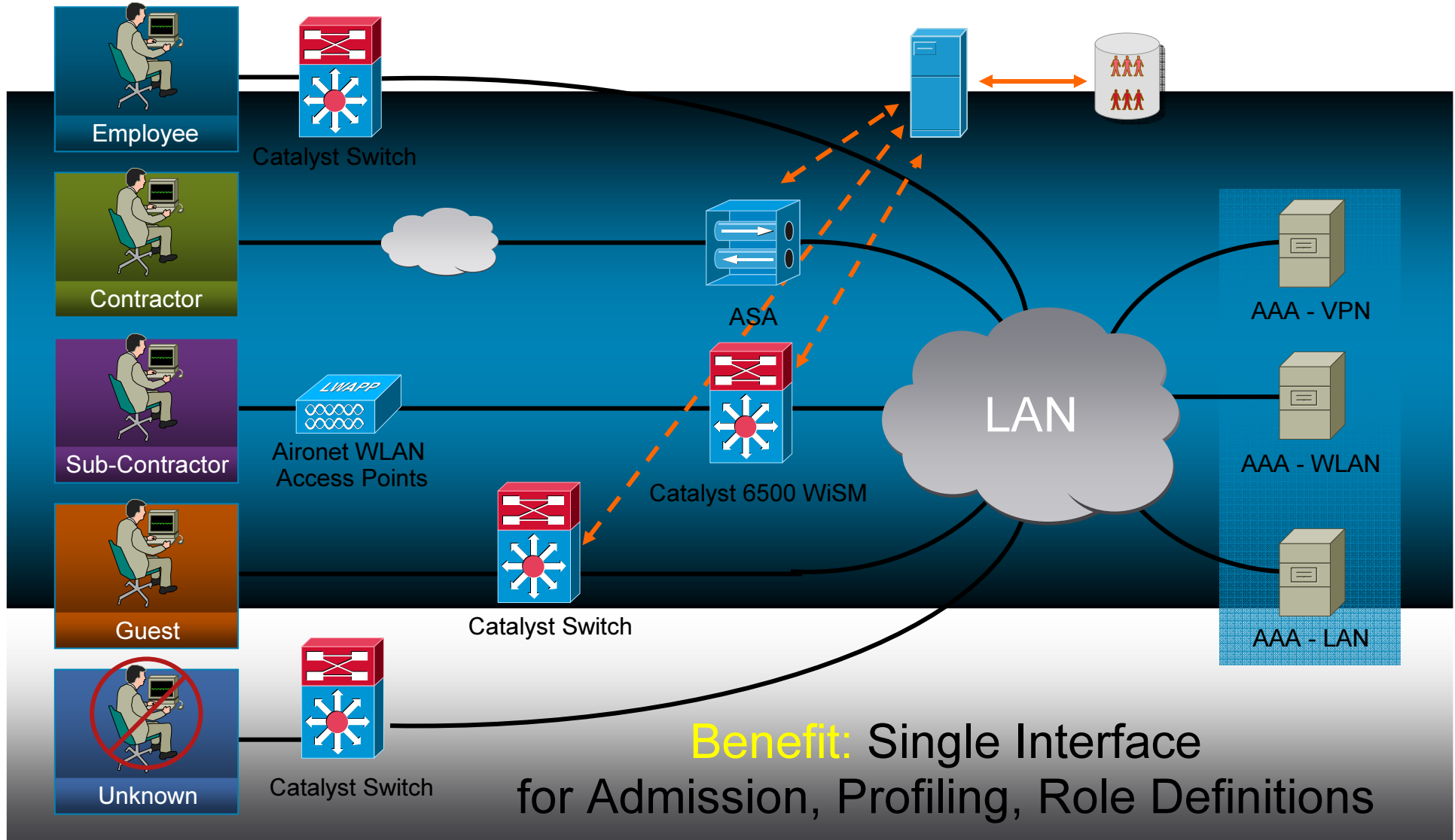


Legend

Link/Port Status		Security Group Classifications			
	Unauthenticated		Employee Group		Confidential Group
	Failed Authentication		Partner Group		Unrestricted Group
	Authenticated		Guest Group		Internet Group
	Shutdown		Ingress Tagging		Egress Filtering

SGACL Matrix	Destination Groups		
	C	U	I
Source Groups			
E			
P			
G			

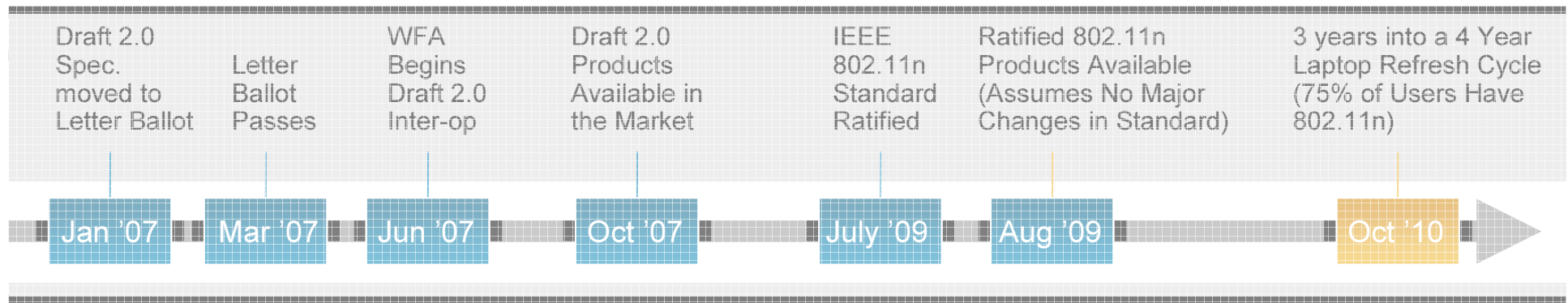
Converged Policy Framework:



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

MIMO

40Mhz
Channels

Packet
Aggregation

Backward
Compatibility

Aspects of 802.11n

MIMO

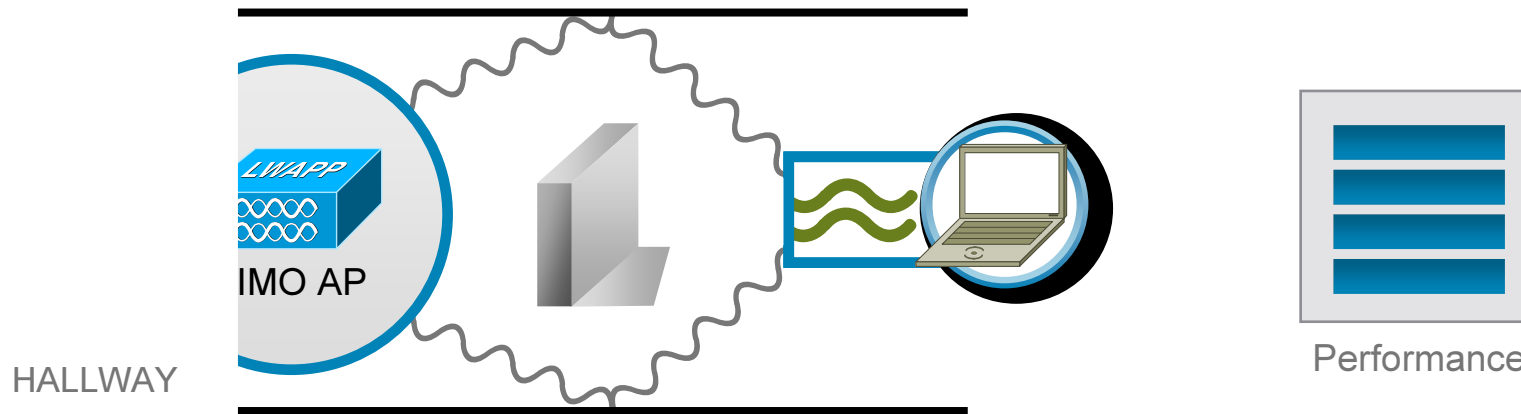
40MHz Channels

Packet Aggregation

Backward Compatibility

MIMO (Multiple Input, Multiple Output)

With Beamforming Transmits in Phase, Increase of Signal Strength
 Without Beamforming Transmits out of Phase, Decrease of Signal Strength



Performed by Transmitter (Talk Better)	Ensures Signal Received in Phase	Increases Receive Sensitivity	
--	----------------------------------	-------------------------------	--

Beam Forming

Maximal Ratio Combining

Spatial Multiplexing

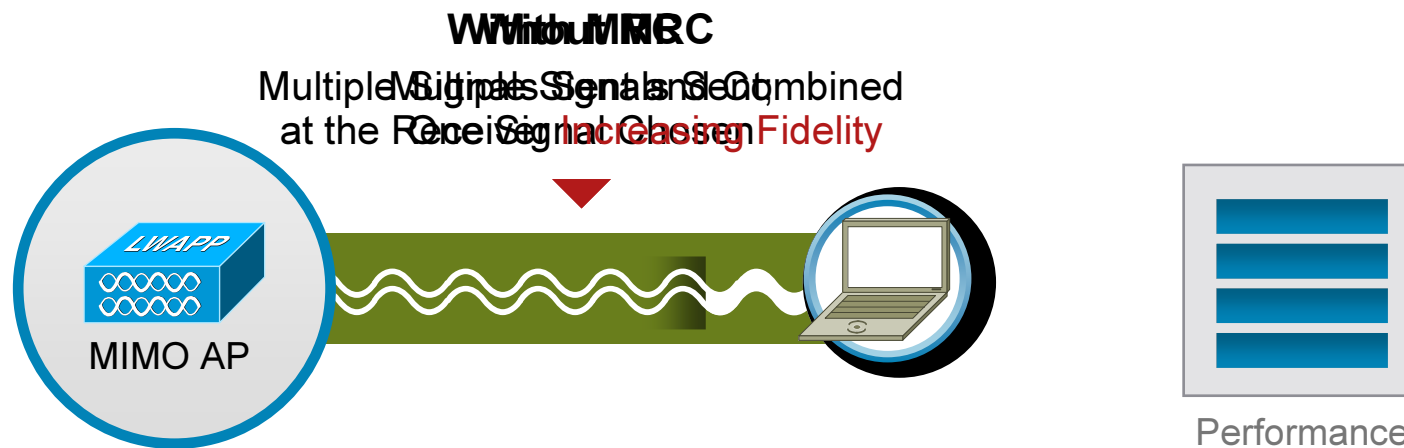
Aspects of 802.11n

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

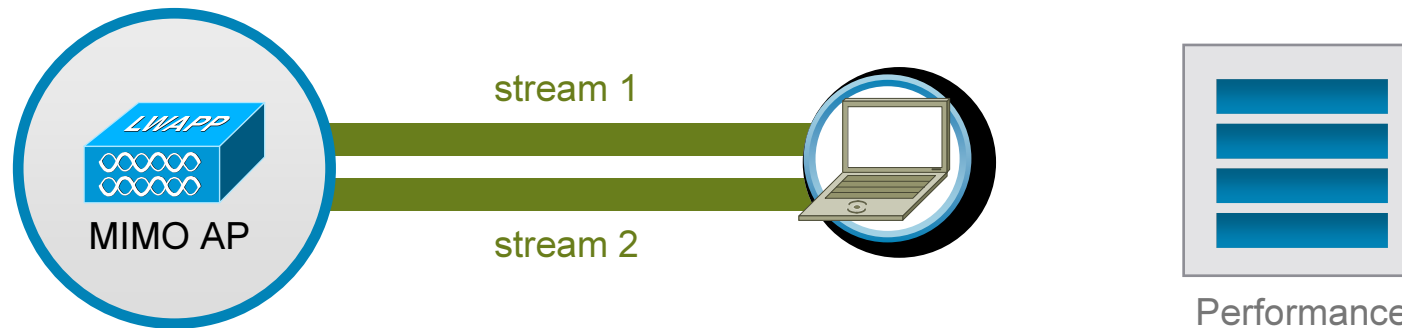
40MHz Channels

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

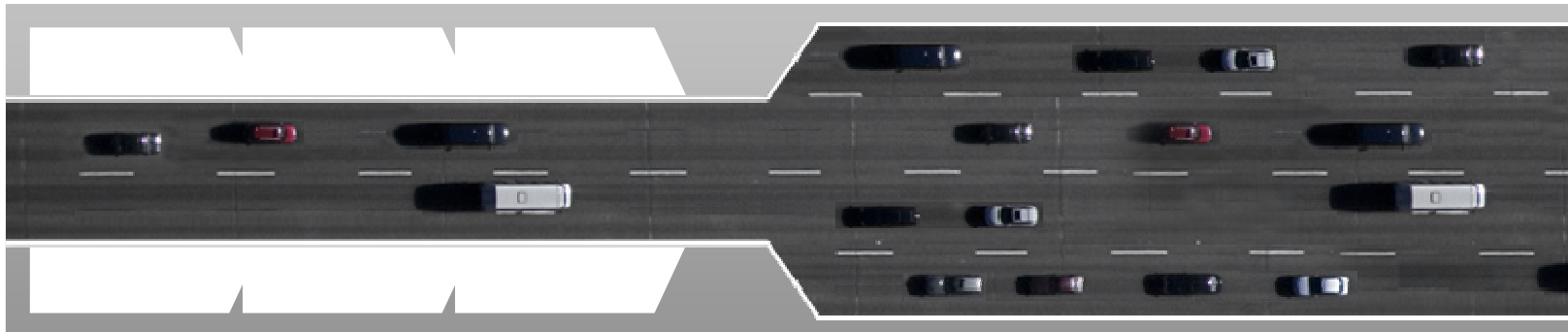
40MHz Channels

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



Without Packet Aggregation

802.11n
Overhead

Data
Unit
Packet

802.11n
Overhead

Data
Unit
Packet

802.11n
Overhead

Data
Unit
Packet

802.11n
Overhead

Data Unit

Packet

Packet

Packet

With Packet Aggregation

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

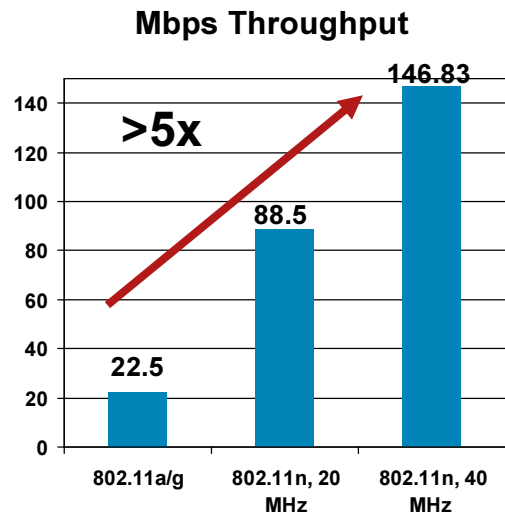
802.11n

It's About a Whole Lot More Than Speed

Throughput

5x more throughput

Enhanced file transfer and download speeds for large files

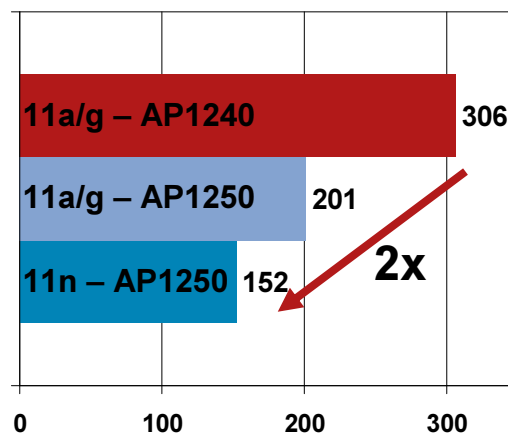


Reliability

2x more reliable

Lower latency for mobile unified communications

Average Packet Retries

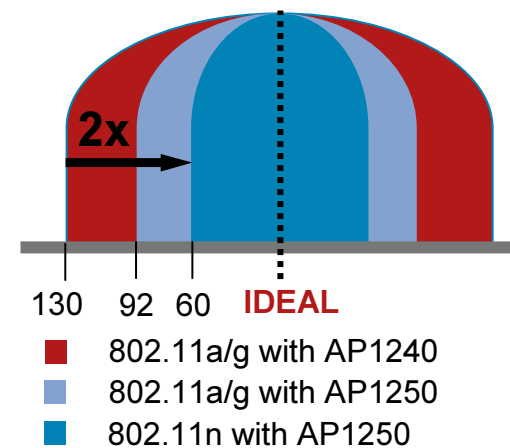


Predictability

2x more predictable

More consistent coverage and throughput for mobile applications

Predictability of Throughput Standard Deviation of Packet Retries

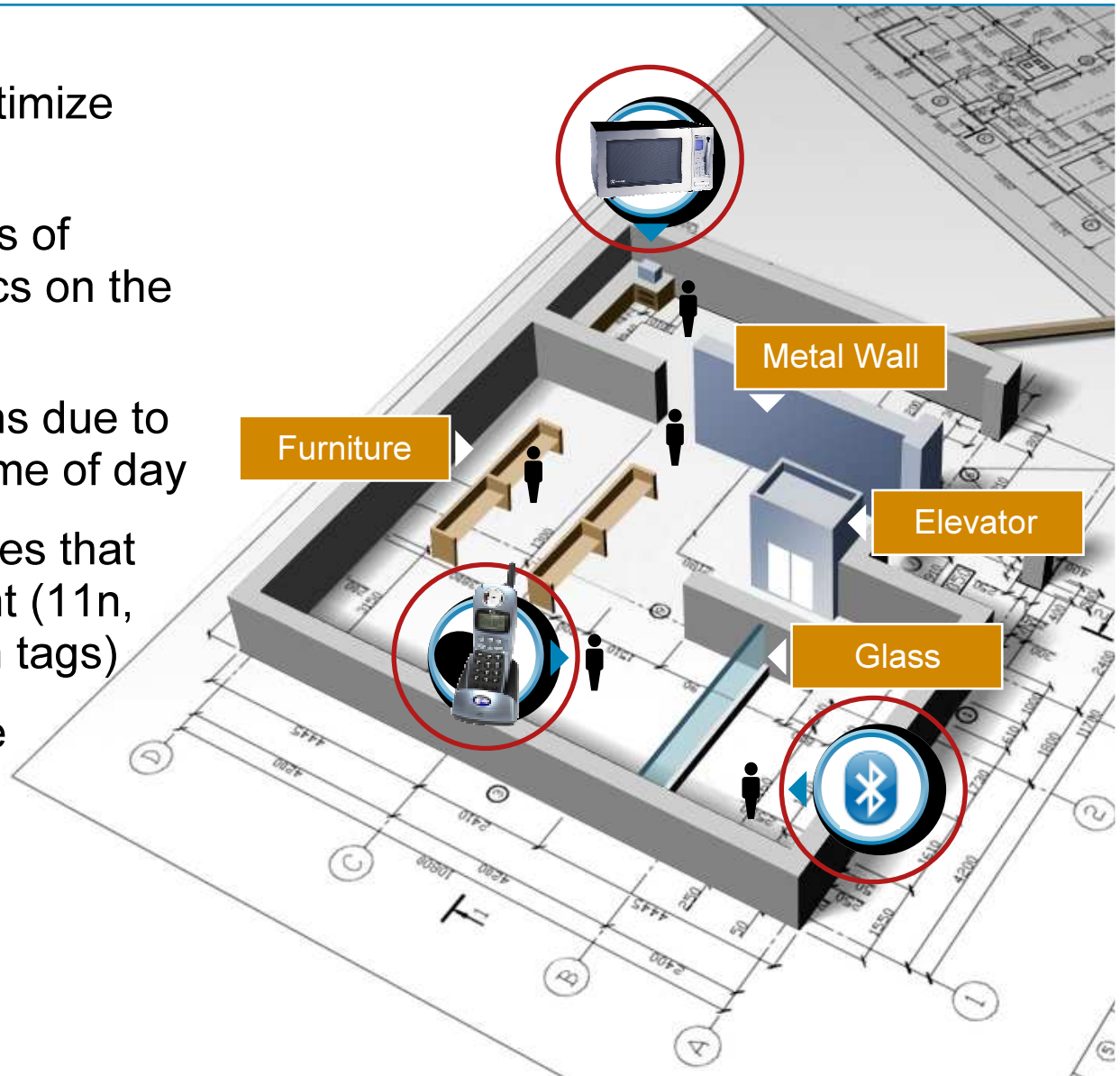


802.11n Design and Deployment



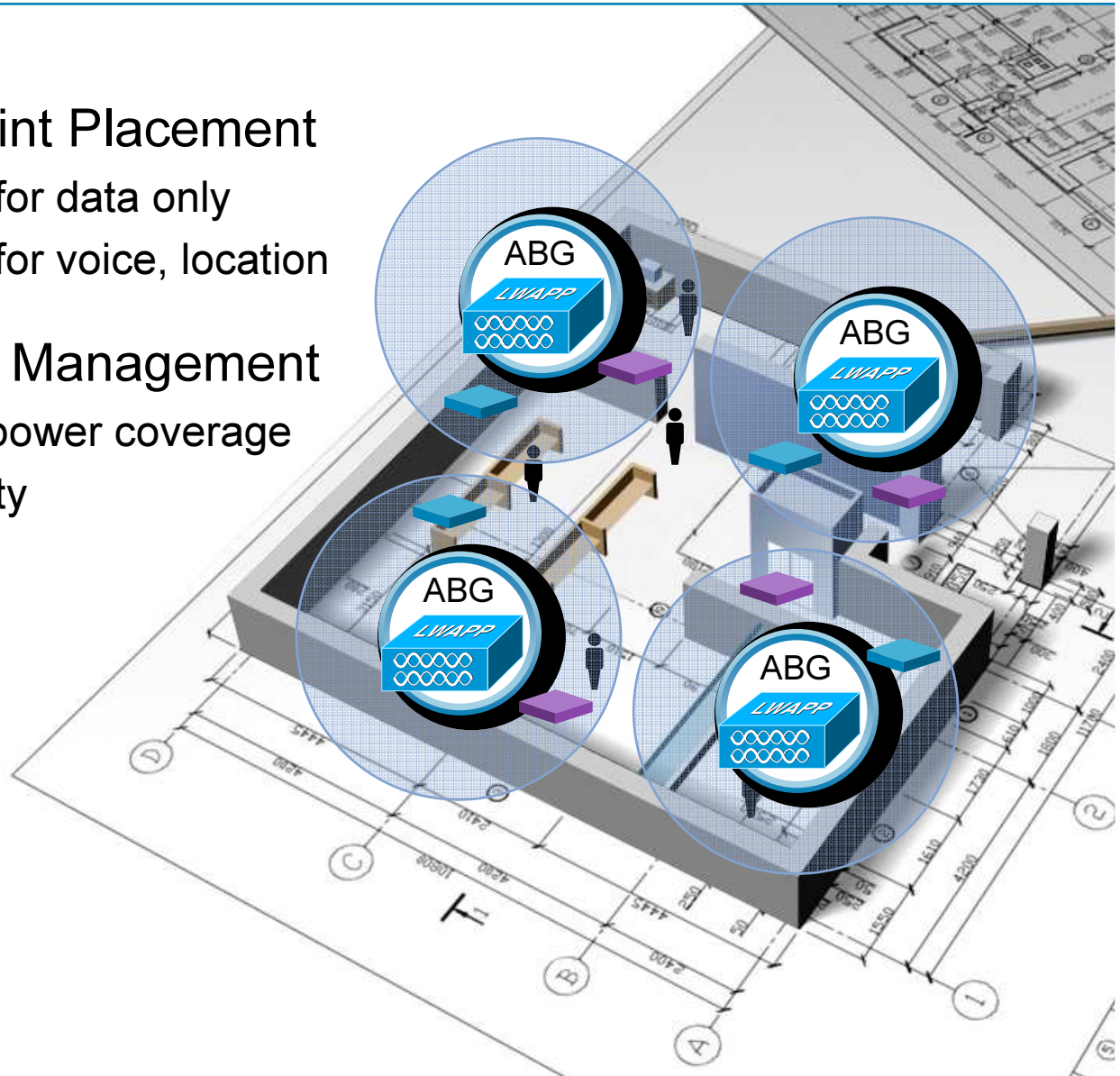
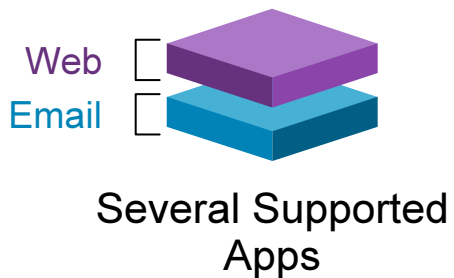
Site Survey Prepares for 802.11n

- 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



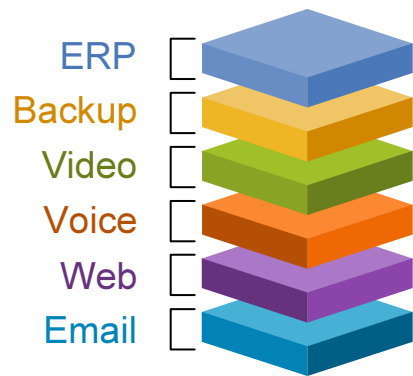
Access Point Placement

- ▶ **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



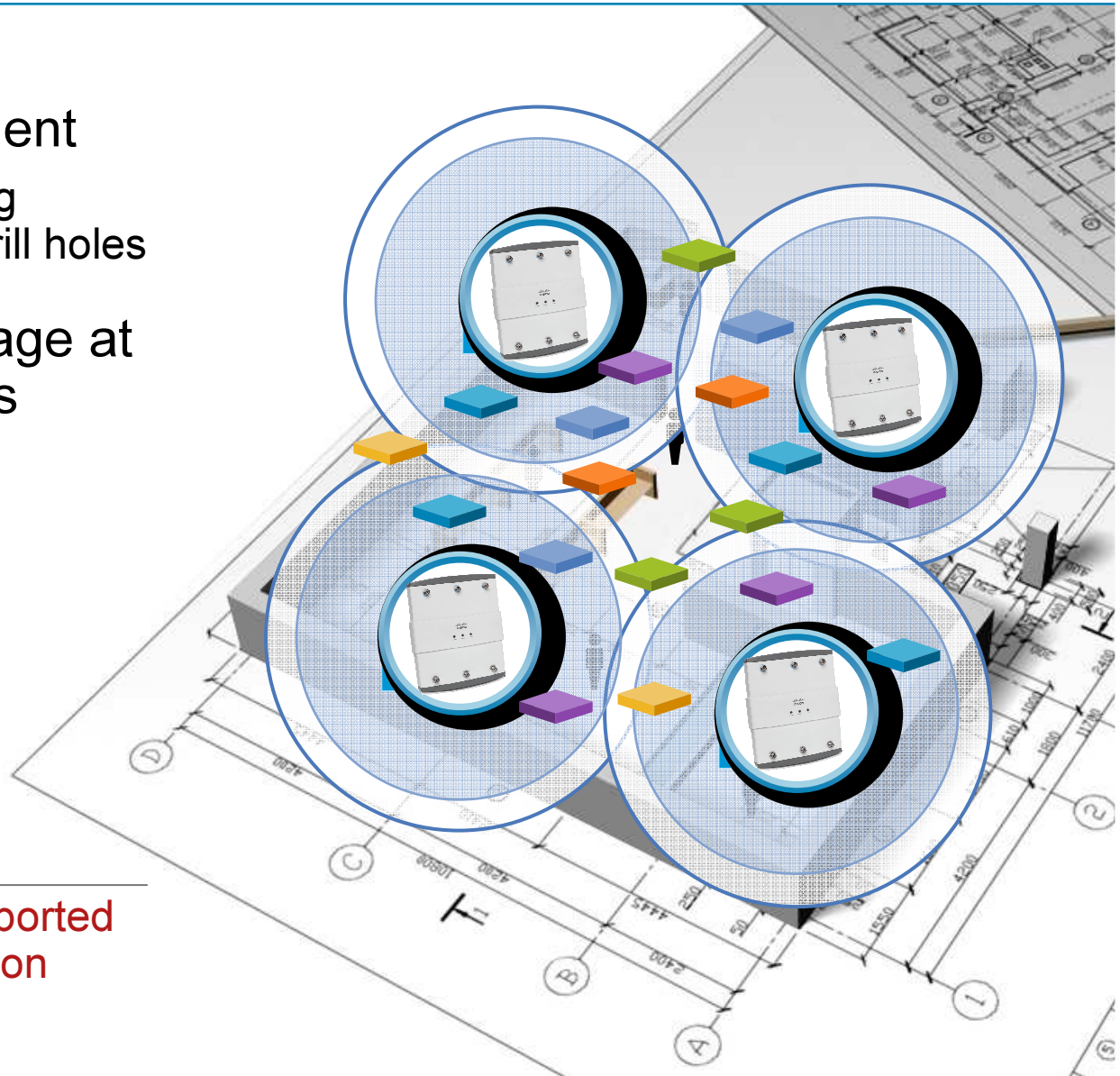
Access Point Placement

- ▶ 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

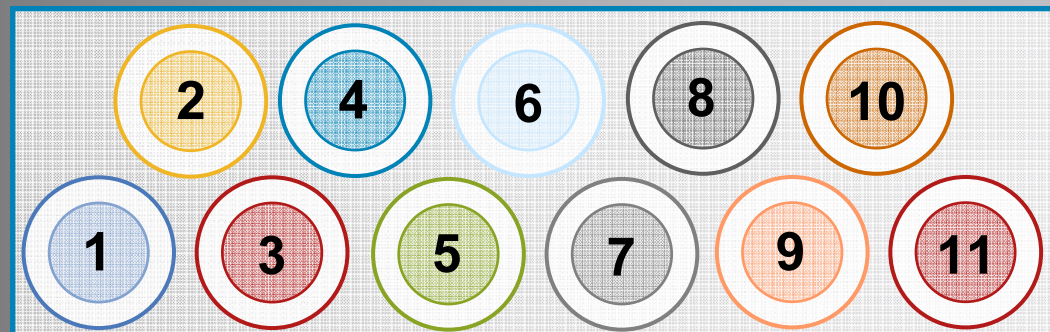
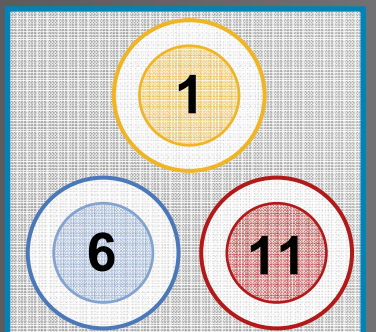
More available spectrum—greater number of channels

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

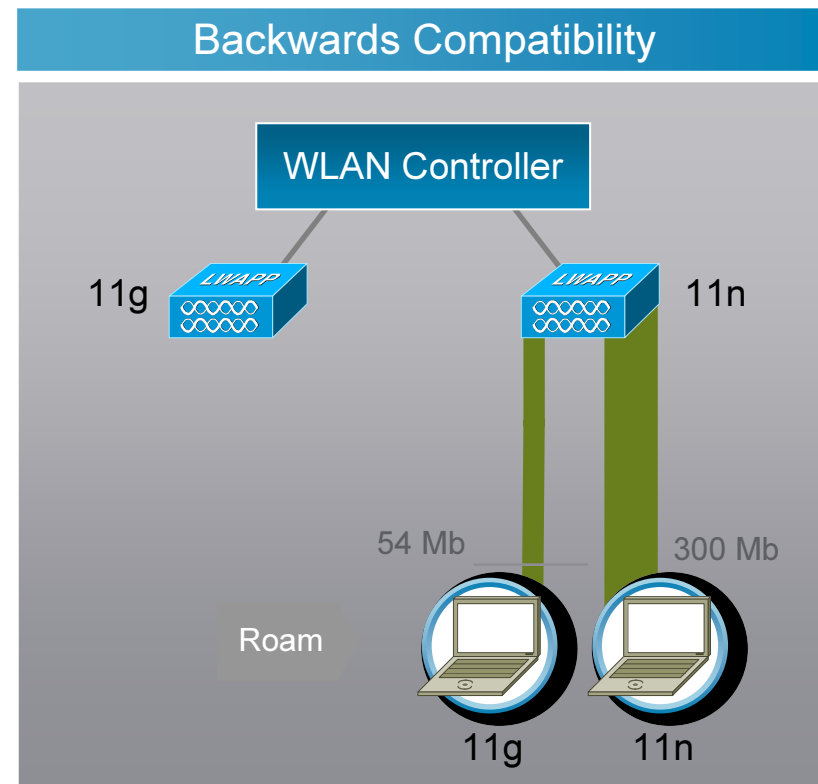
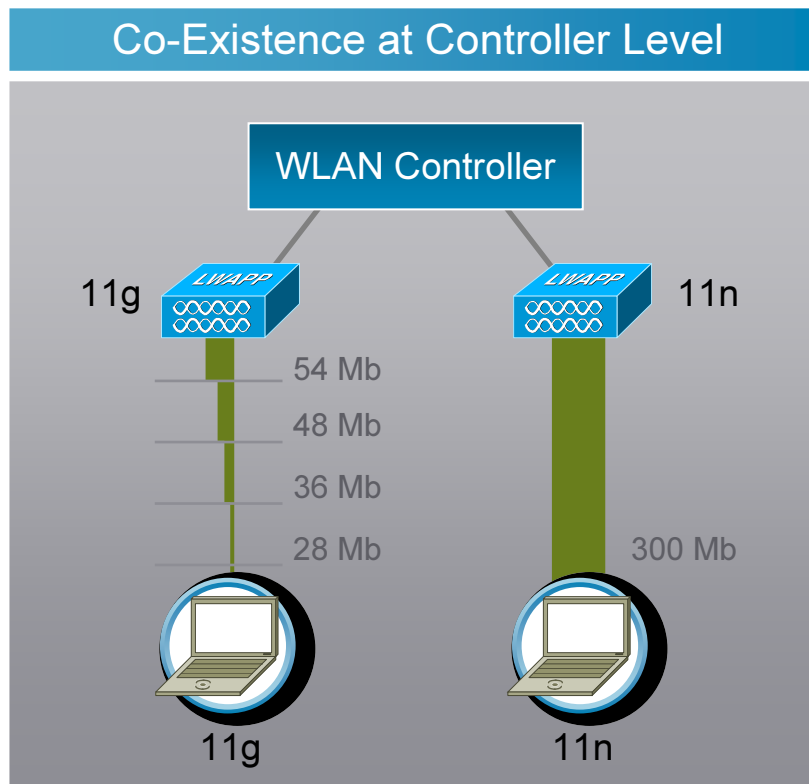
Ideal for legacy apps (handhelds, scanners, med. applications)



Backward Compatibility & Co-Existence

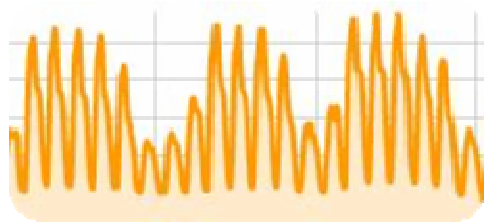
- Co-existence of ABG/N APs
- Benefits of 11n accrue to ABG clients

MIMO benefits ABG clients on the AP receive side from MRC

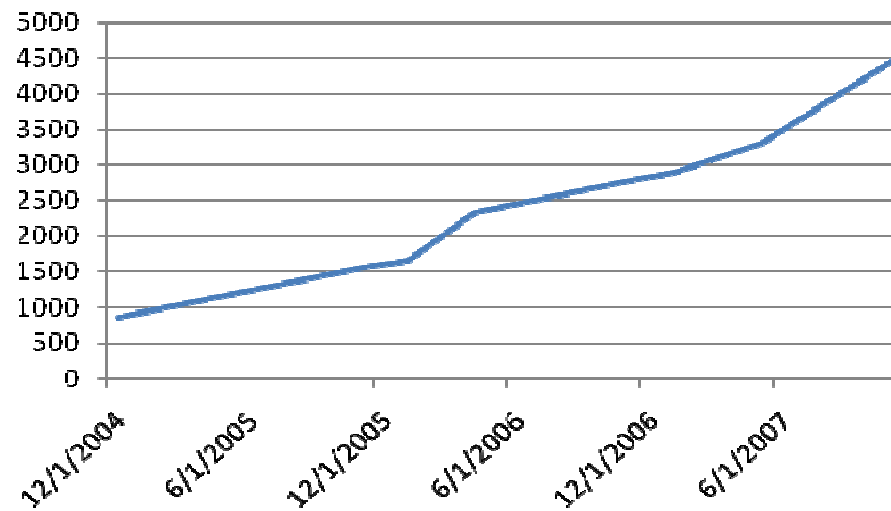


Duke University – 802.11n Experiences

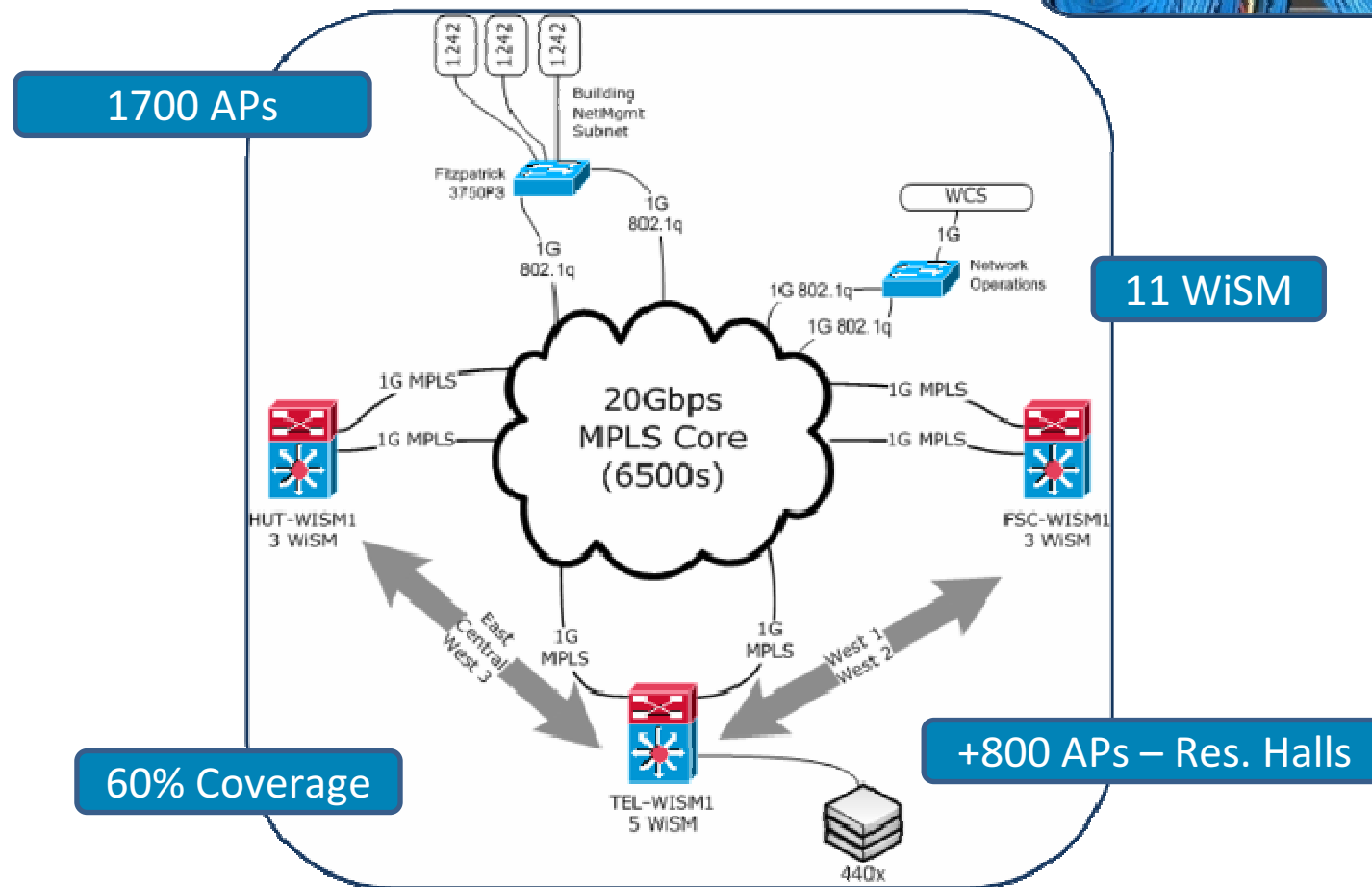
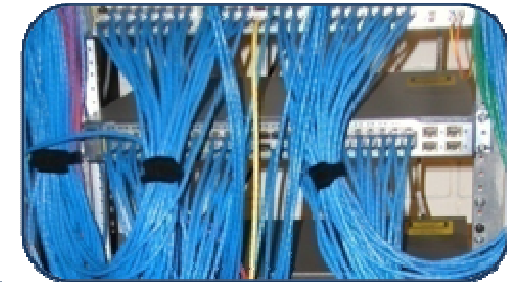
- Increase in wireless connectivity
- Decrease in wired use
 - Public wired ports (library) completely unused
- Increased need for mobility



Peak Simultaneous Wireless Users



Current infrastructure



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.



