Acceso Unificado en el Campus Universitario

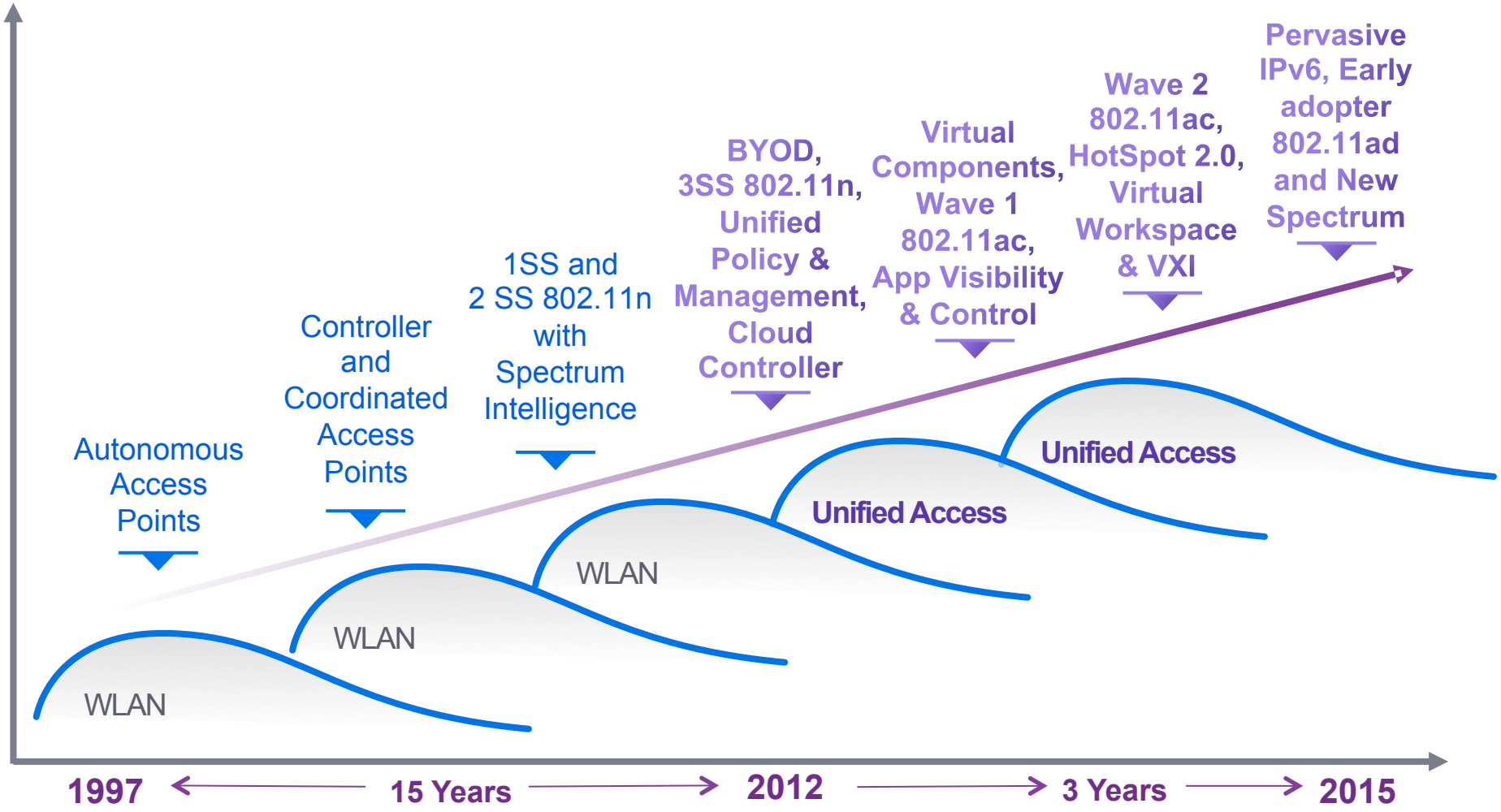
One Policy – One Management – One Network

Juan Antonio Castilleja – Systems Engineer

Higher Education Unified Access

ANYWHERE ANYTIME ANY DEVICE

Unified Access Trends



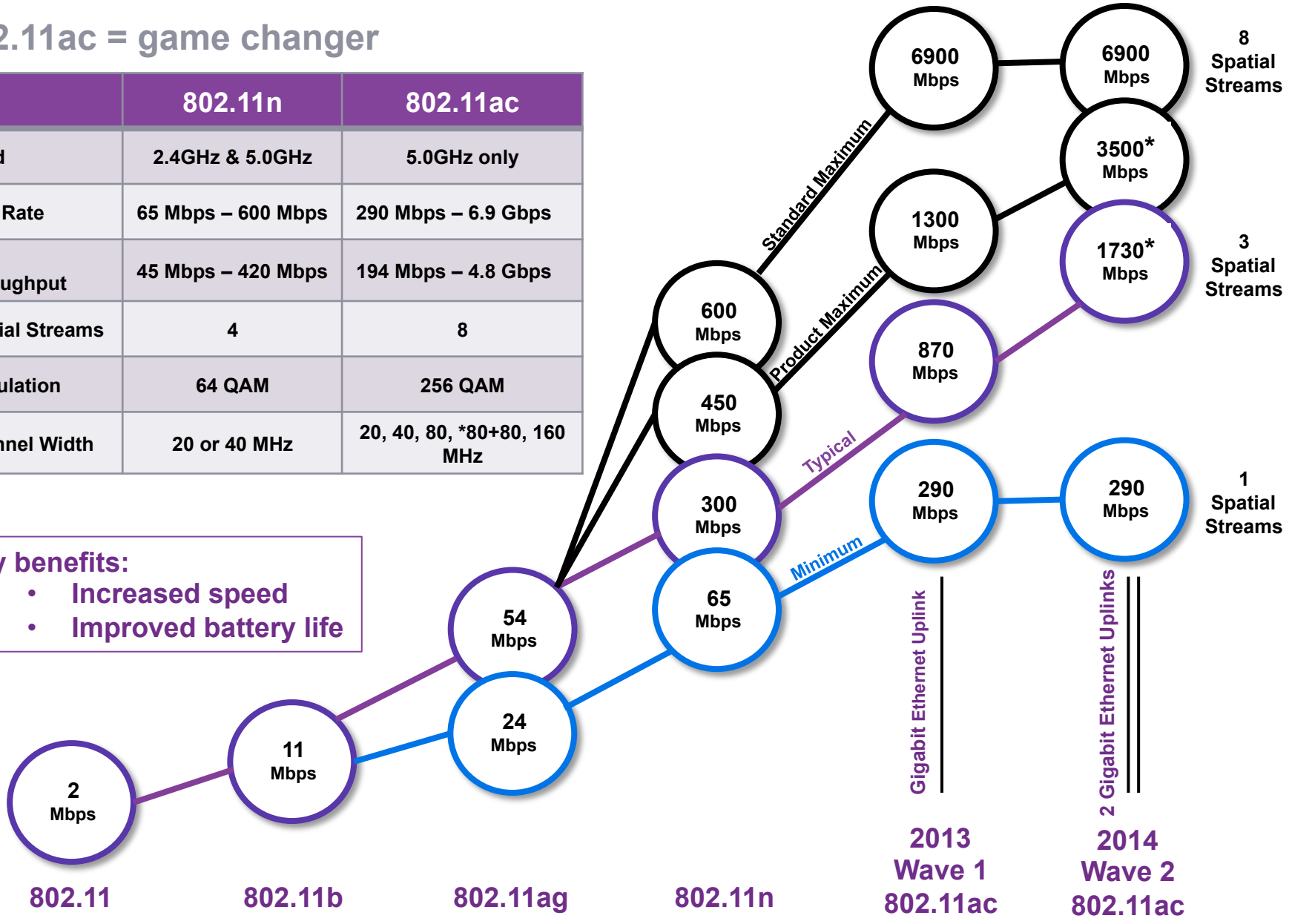
Unified Access Trends

802.11ac = game changer

	802.11n	802.11ac
Band	2.4GHz & 5.0GHz	5.0GHz only
PHY Rate	65 Mbps – 600 Mbps	290 Mbps – 6.9 Gbps
MAC Throughput	45 Mbps – 420 Mbps	194 Mbps – 4.8 Gbps
Spatial Streams	4	8
Modulation	64 QAM	256 QAM
Channel Width	20 or 40 MHz	20, 40, 80, *80+80, 160 MHz

Key benefits:

- Increased speed
- Improved battery life

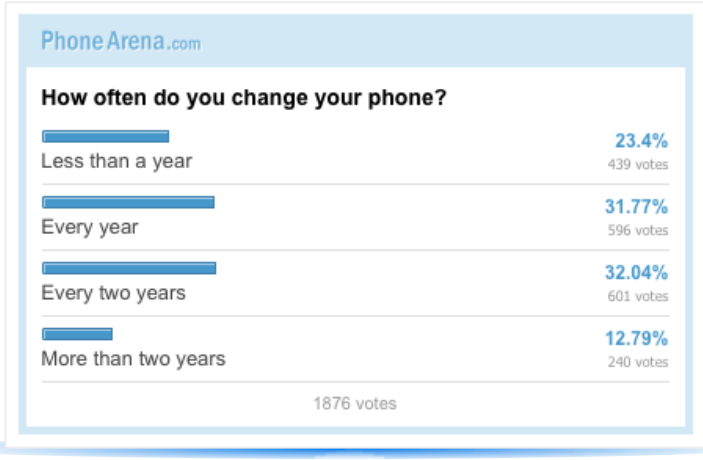


* Assumes 160MHz channel width is available and usable

Unified Access

Higher Education - Drivers

- Majority of new network devices will have no wired port
- Users are starting to bring 5+ or more WLAN devices each
- Mobile devices have become an extension of an individuals personality
- Users will change devices more frequently than in the past
- Guest access with accountability has become a must do



Unified Access

Higher Education - Assumptions

- Wi-Fi is not Ethernet – Shared medium, limited channels, etc.
- Plug in any device that does not move (printers, smartboards, etc.)
- Users will have 5+ WLAN devices (laptop, tablet, phone, game, DVR, etc.)
- Users will expect Wireless to become as predictable as the Wired Network
- Users will expect to simply onboard any WLAN device they want
- You eventually will have to apply security policy to every user and device
- Guest Access must be isolated and accounted for always

Unified Access

Higher Education User Profiles

Guest

- BYOD – Wireless
- Account sponsorship
- Acceptable use agreement
- Internet access only
- Rate & Time limited
- Identity based accountability and access logging

Student

- BYOD – Wired & Wireless
- Acceptable use agreement
- Internet access and restricted resources access
- Data Loss Prevention
- Identity based accountability and access logging.

Faculty

- BYOD – Wired & Wireless
- User Directory
- VPN access
- VDI / VXI access
- Voice, Video, Data
- Unrestricted corporate access
- Data Loss Prevention
- Mobile Device Management
- Identity based accountability and access logging.

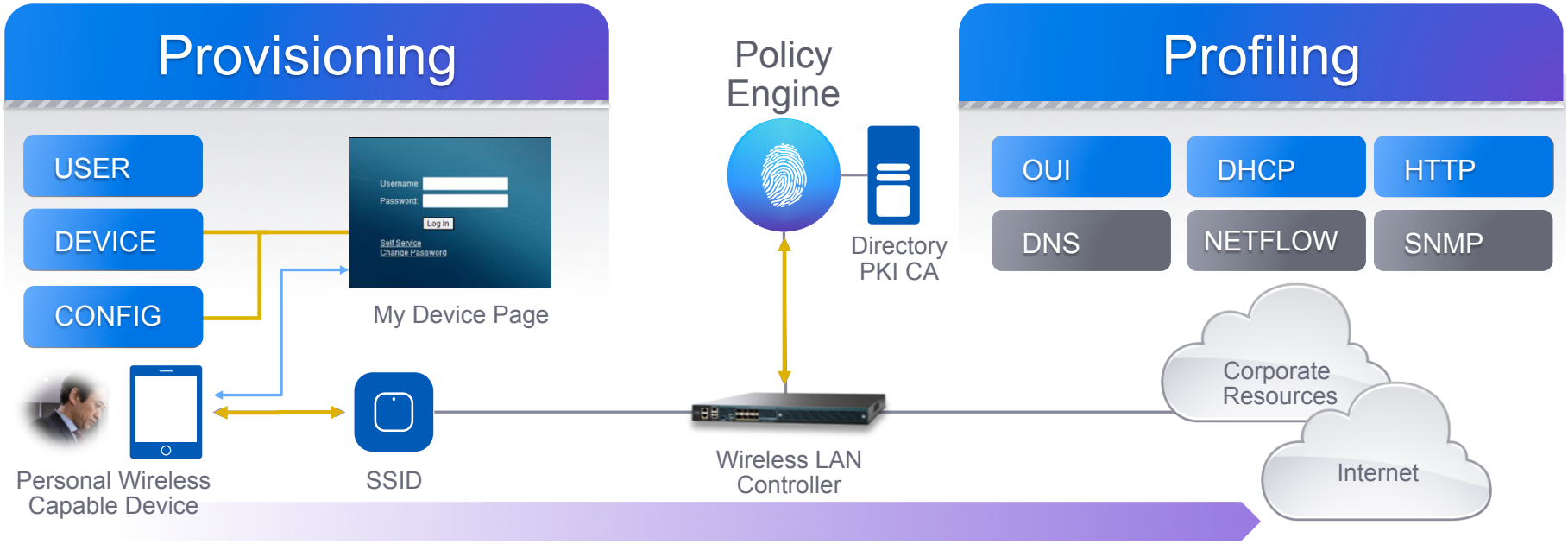
Unified Access

Use Profiles with Key Functionality

Key Functionality	Guest	Student	Faculty
AAA	✓	✓	✓
Guest Management	✓	✓	✓
Wi-Fi Profiling	✓	✓	✓
Wired Profiling		✓	✓
Wi-Fi Provisioning		✓	✓
Wired Provisioning		✓	✓
Wi-Fi & Wired Posturing			✓
VDI / VXI			✓
Mobile Device Management			✓

Unified Access

Example Faculty User Walkthrough—Wireless

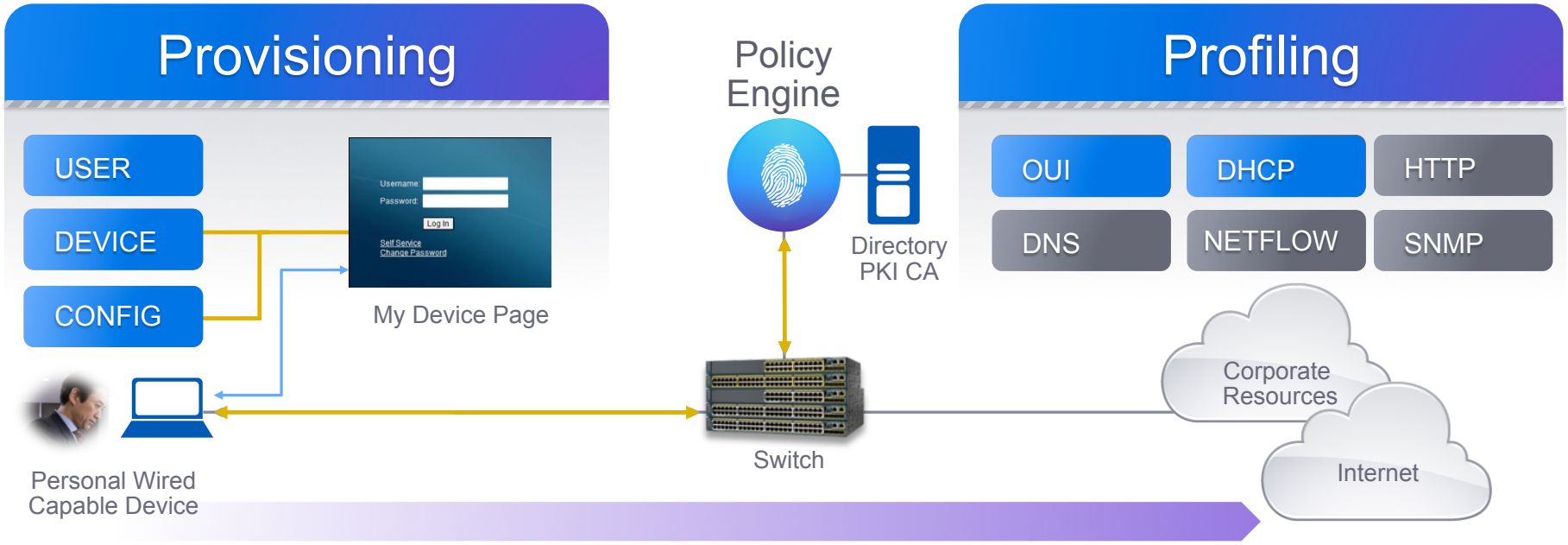


Personal Device Profiling and Provisioning

1. AAA—Authentication, Authorization and Accounting (RADIUS)
2. Profile Device using multiple probes (OUI + DHCP + HTTP)
3. User is redirected to “My Device Page” and walked through provisioning
4. Device is provisioned for University Wi-Fi Network access
5. Device associates securely to University SSID and granted access

Unified Access

Example Faculty User Walkthrough—Wired



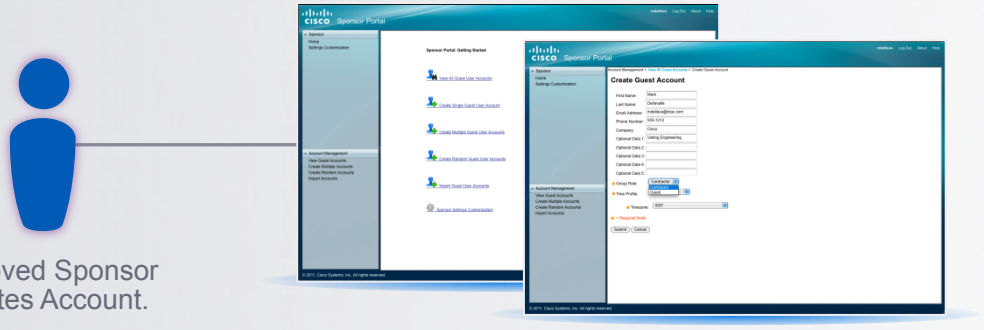
Personal Device Profiling and Provisioning

1. AAA - Authentication, Authorization and Accounting (RADIUS)
2. Profile Device using multiple probes (OUI + DHCP)
3. User is redirected to “My Device Page” and walked through provisioning
4. Device is provisioned for University Wired Network access
5. Device connects securely with appropriate access policy

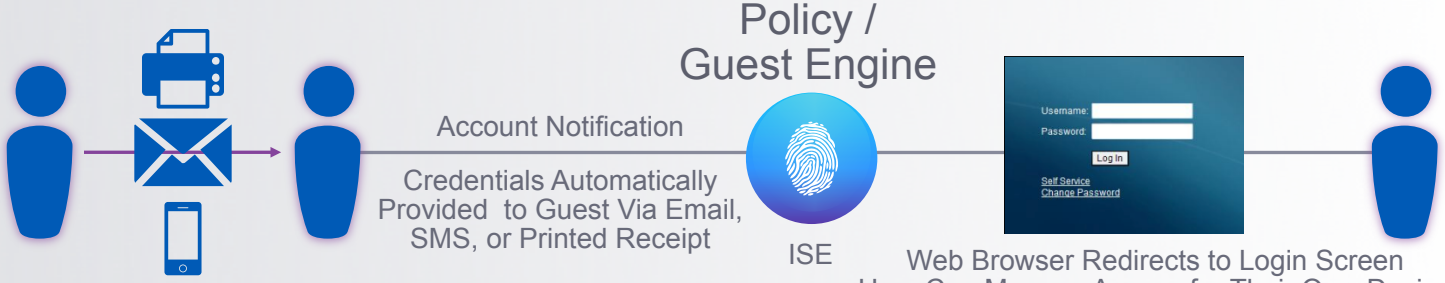
Unified Access

Example Higher Education Walkthrough—Guest

Account Sponsorship



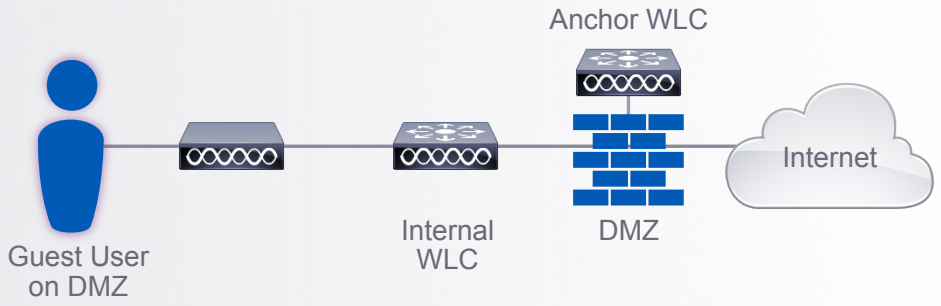
Captive Portal



Access Granted

Successful Authentication

- Isolated Guest Network on DMZ
- Role Based Policy Applied
- User granted access to Internet



Unified Access

What is success?

- **CONTROL - when you have "One" Policy Management for all users and devices**
  - *Unified Policy Management = Identity Services Engine + TrustSec / Secure Group Access*
- **VISIBILITY - when you have "One" Network Management of all users, devices, and components**
  - *Unified Network Management = Cisco Prime Infrastructure*
- **PREDICTABILITY - when you have "One" high performance, utility-grade Unified Access Network**
  - Stateful Switchover, *Radio Resource Management, CleanAir, ClientLink, BandSelect, and VideoStream*
- **BALANCE - when you have operational balance between Wired ports and Wireless radios**

2.4 GHz Centric Wi-Fi (802.11gn)

- Pervasive coverage in 2.4 GHz
- No coverage gaps in 2.4 GHz
- Consistent signal (RSSI) in 2.4 GHz
- 1 Access Point per 2,500 square feet

or

- 1 Access Point per 24 ports of Switching
- Gigabit Ethernet uplink per Access Point required

5.0 GHz Centric Wi-Fi (802.11n and 802.11ac)

- Pervasive coverage in 5.0 GHz
- No coverage gaps in
- Consistent signal (RSSI) in 5.0 GHz
- 1 Access Point per 1,000 square feet of

or

- 1 Access Point per 12 ports of Switching
- 2 Gigabit Ethernet uplinks per Access Point required

Unified Access

Checklist / Timeline for Success

	Now	Soon	When Required
Unify Wired+Wireless Policy and Network Management - IPv4+IPv6	✓		
Scale Wi-Fi for capacity for 2.4 GHz	✓		
Scale DHCP, DNS, AAA, PPP, and Guest services for capacity	✓		
Implement Wireless (AAA+Profiling+Provisioning+ Guest)	✓		
Scale Wi-Fi for capacity for 5.0 GHz		✓	
Implement Wireless (AAA+Profiling+Provisioning+Guest+ Mobile Device Management)		✓	
Implement Wireless+Wired (AAA+Profiling+Provisioning+Posturing +Guest+Mobile Device Management)			✓

Cisco's Unified Access

Higher Education
One Policy – One Management – One Network

Cisco's Unified Access Network

Simplify IT Operations – Best of Breed – Best in Class

One Policy

- **Unified Policy**
  - Wired, Wireless, and VPN
  - Corporate & personal assets
  - *MDM integration
- **Context-based Control**
  - Who, what, which, when, where, and how
  - Advanced segmentation
- **User-specific Services**
  - Self-service on-boarding
  - Simplified guest handling
  - Location-based services

One Management

- **Unified Management**
  - Single pane of glass view
  - Users, devices, threats, location, policy, posture
- **Operational Efficiency**
  - Intelligent troubleshooting
  - Automated reporting
  - IPv4 and IPv6 support
- **Lifecycle Management**
  - Plan, Deploy, Monitor, Troubleshoot, Remediate, Optimize

One Network

- **Wired+Wireless+VPN**
  - Best in class Wireless
  - Best in class Switching
  - Application visibility/control
- **Sub-second Convergence**
  - LAN Stateful Switchover
  - LAN Non-Stop Forwarding
  - WLAN Stateful Switchover
- **Deployment Flexibility**
  - Virtualized components
  - Secure Group Access
  - Smart Operations

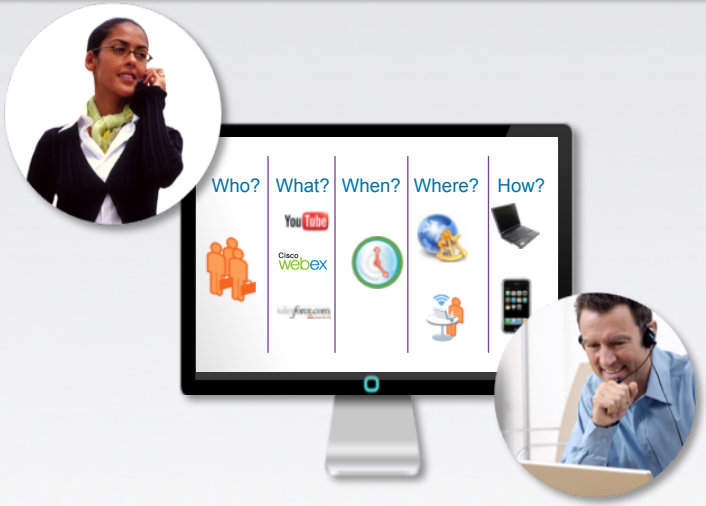
One Policy – Identity Services Engine

Industry's First Context-Based Wired+Wireless+WAN Policy/Guest Management

BEFORE
Separate policy and guest management

Wired | Wireless | WAN

AFTER
Unified context-based policy management
for employees and guests across the network



Account for every device and block unwanted devices

AAA + Profiling, Provisioning, and Posturing = Secure BYOD

Simple | Unified | Automated

Cisco ISE–Provides Unparalleled Control

One Policy

5 Dimensions of Policy and Provisioning

User	Device	Access Method	Location	Time	Policy
Guest	Personal Device	Wireless	Classrooms	M–S 8 am–6 pm	Captive Portal DMZ Guest Tunnel
			Library		Guest VLAN
Student	Personal Device	Wired	Anywhere	Anytime	Student VLAN
		Wireless	Anywhere	Anytime	Student ACL
Faculty	Faculty Device	Wired	Anywhere	Anytime	Faculty VLAN
	Personal Device	Wireless	Anywhere	Anytime	Faculty ACL
		VPN		Anytime	

IF $Identity AND $Device AND $Access
AND $Location AND $Time THEN $Policy

One Policy

Use Cases

Control who connects… no certificates (employee, contractor, guest)

Control who connects… with certificates (employee, contractor, guest)

Control who and what device connects… (corporate or personal device, My Device page / self-registration)

Control who with what device and which access method they connect to… (Wireless, Wired, or VPN)

Control who with what device and which access method and from where they connect… (conference room, contractor cubicles, etc.)

Control who with what device and which access method and from where and when they connect… (time of day, day of week, etc.)

Control who with what device and which access method from where and when and if they are safe to connect… (virus scan, prohibited process, service pack level, etc.)

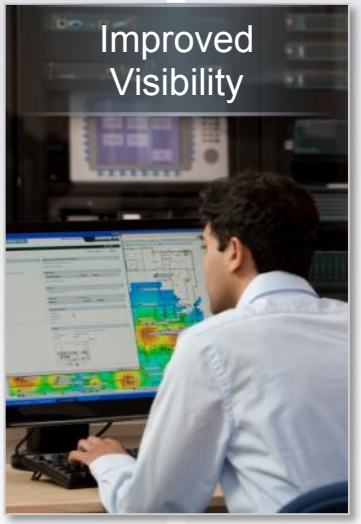
Control and assign quality of service based on device and applications

One Management – Prime Infrastructure

Single Pane of Glass View and Management of WLAN – LAN - WAN

BEFORE
Separated management

- Siloed Inefficient Operational Model
- Repetitive Manual correlation of data
- Error Prone Consumes time and resources



AFTER
Comprehensive user and Unified Access network
Visibility & advanced troubleshooting

WLAN

LAN

WAN
+
Identity

- Simple Improves IT efficiency
- Unified Single view of all user access data
- Advanced Troubleshooting Less time and resources consumed

Cisco Prime Infrastructure – Provides Unparalleled Visibility

One Management

Use Cases

Visualize and manage who connects…

Visualize and manage who and what device connects…

Visualize and manage who with what device and which access method they connect to…

Visualize and manage who with what device and which access method and from where they connect…

Visualize and manage who with what device and which access method and from where and when they connect…

Visualize and manage Cisco and non-Cisco Wired and Wireless network components

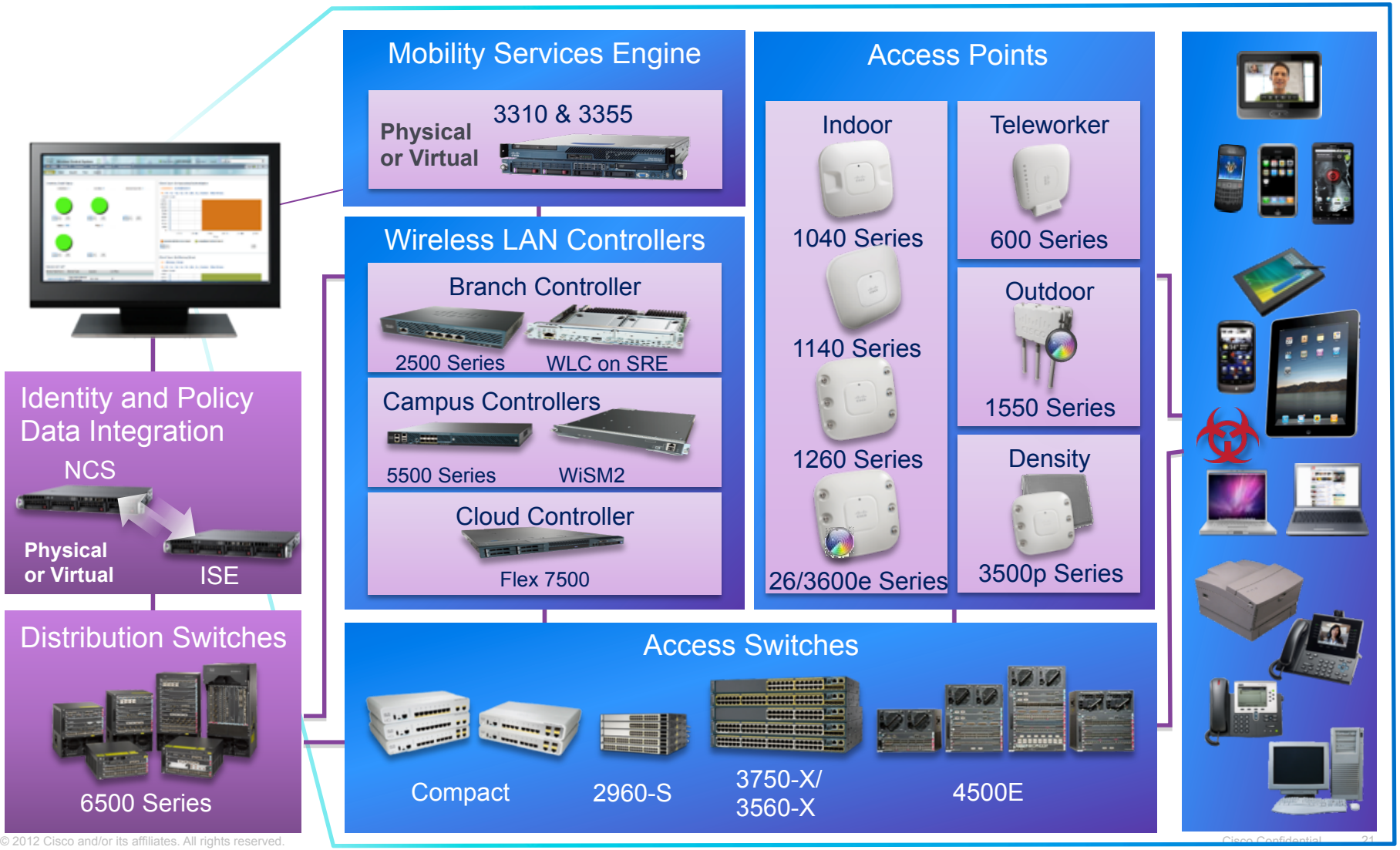
Troubleshoot IPv4 and IPv6 clients and components with automated scripts

Execute complete lifecycle management – planning to decommissioning – from one application

Automate comprehensive usage reports to stakeholders

One Network

Control and Visibility for IT - Predictability for Users



Cisco's Unified Access

Innovations

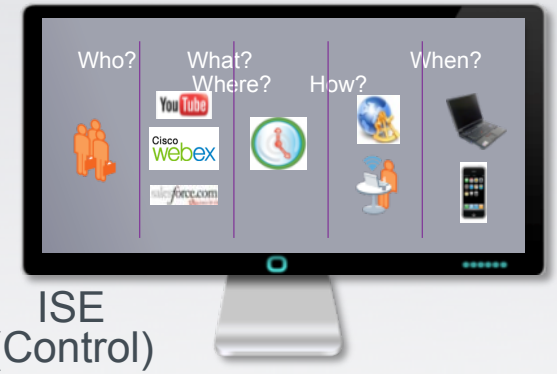
Cisco's Unified Access Innovations

Best in Class and Best of Breed

Unified Access Innovations (Predictability)

CleanAir	Chip level proactive and automatic interference mitigation
ClientLink	Chip level proactive and automatic electronic beamforming
Radio Resource Management	Automatic advanced RF shaping and management
VideoStream	Wired multicast efficiency over a Wireless network
TrustSec - Secure Group Access	Simplified user and resource based segmentation – independent of topology
Application Control & Visibility	Identify, analyze, and optimize application traffic
Stateful Switchover	Sub second WLAN & LAN convergence
AnyConnect	Always-On context-aware VPN connectivity

Policy & Network Management



ISE (Control)

Prime (Visibility)

Cisco's CleanAir Technology

Industry's First Chip Level Proactive and Automatic Interference Protection

BEFORE
Wireless interference decreases reliability and performance

AFTER
CleanAir mitigates RF interference improving reliability and performance

Cisco CleanAir–Improves Performance and Predictability

Why is Cisco's CleanAir Technology so Unique?

High Resolution Interference Detection, Classification, and Mitigation at Chip Level

Detect | Classify | Locate | Mitigate

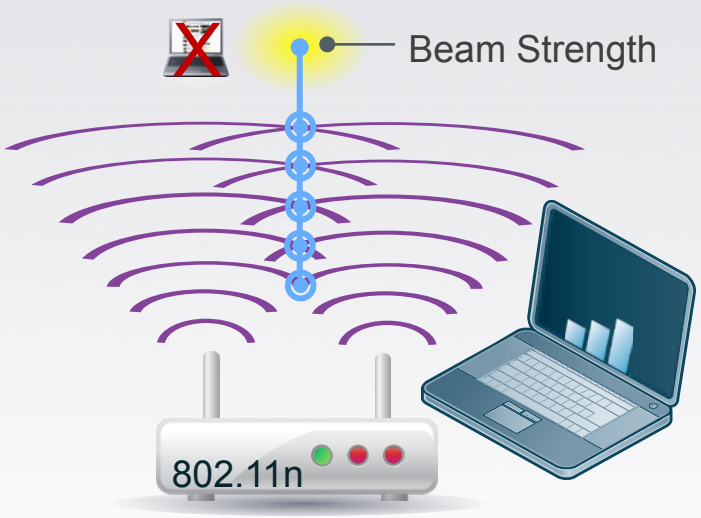
- CleanAir Radio ASIC
- Detect Wi-Fi and non-Wi-Fi interference sources
- Assess impact to Wi-Fi performance
- Proactively change channels when interference occurs
- Monitor air quality

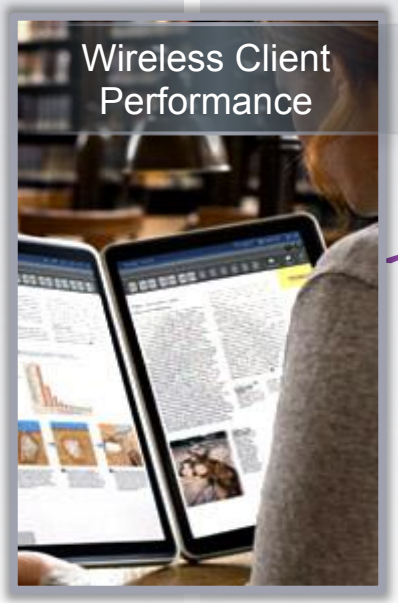
Cisco's ClientLink/ClientLink 2.0 Technology

Advanced Beam Forming Technology Improves Wireless Client Performance

BEFORE
Beam not directed towards clients resulting inconsistent performance

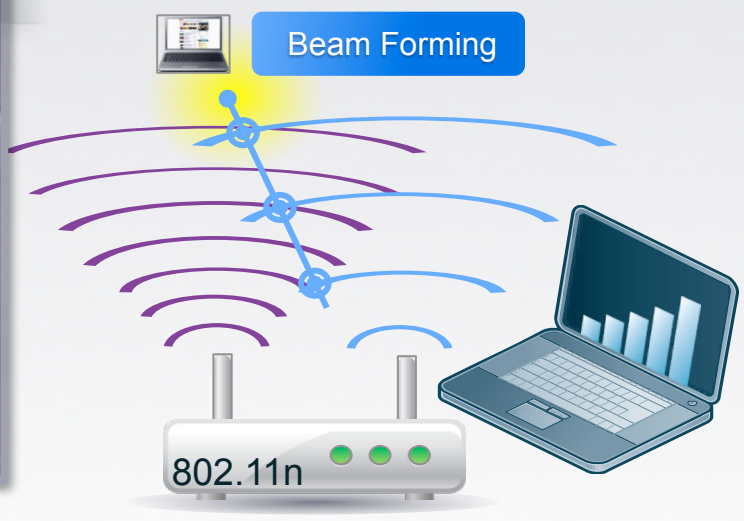
802.11a/g (ClientLink)
802.11a/g/n (ClientLink 2.0)





AFTER
Beam directed towards client resulting in consistent experience and better performance

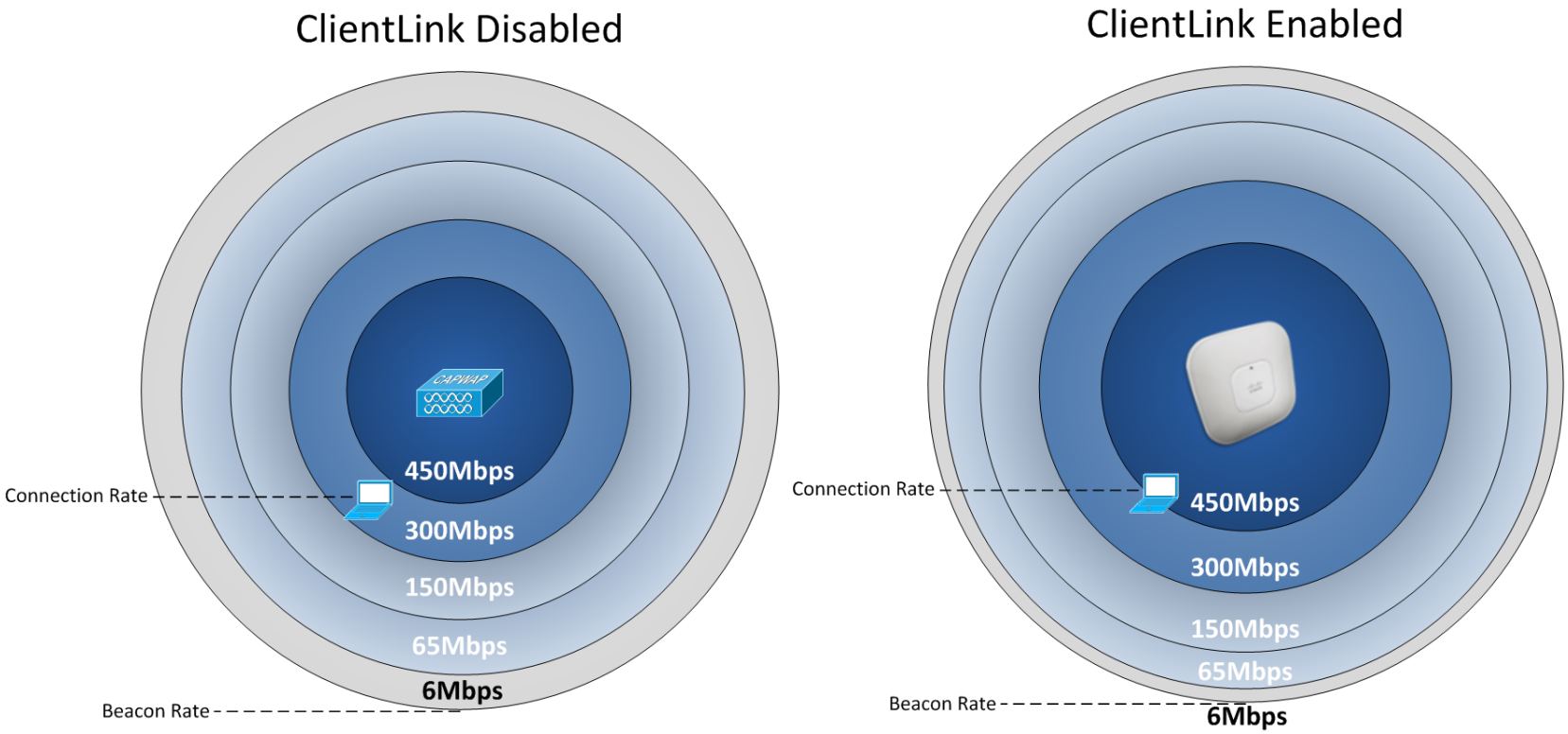
802.11a/g (ClientLink)
802.11a/g/n (ClientLink 2.0)



Cisco ClientLink—Improves Predictability and Performance

Why is Cisco's ClientLink 2.0 so Unique?

Reduces Coverage Holes/Improves both Upstream and Downstream

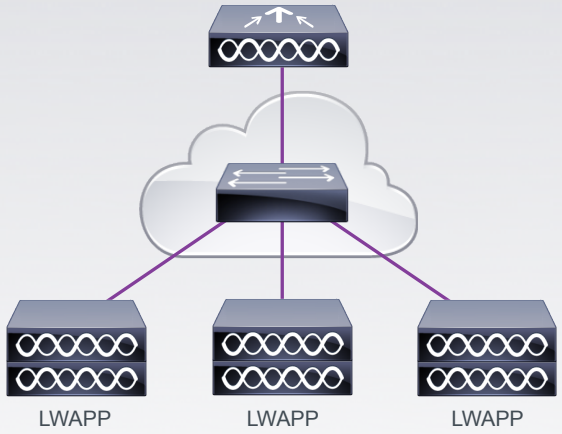


Cisco ClientLink 2.0 —Improves Predictability and Performance

Cisco's Radio Resource Management

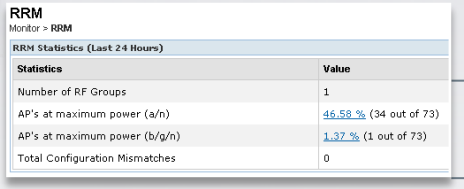
Simplify IT Operations with Automatic/Dynamic RF Management

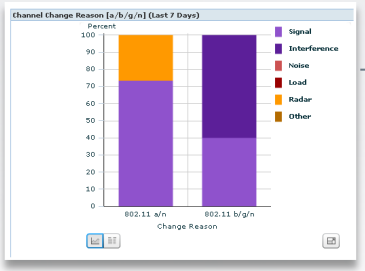
BEFORE
Manual RF management



- ✗ Manual Channel Assignment
- ✗ Manual Transmit Power Adjustment
- ✗ Manual Coverage Hole Detection/Mitigation

AFTER
Dynamic RF management





Channels

Power

Coverage

- ✓ Dynamic Channel Assignment
- ✓ Dynamic Transmit Power Adjustment
- ✓ Dynamic Coverage Hole Detection/Mitigation

Cisco RRM—Improves Predictability and Performance

Why is Cisco's RRM Technology so Unique?

- DCA—Dynamic Channel Assignment

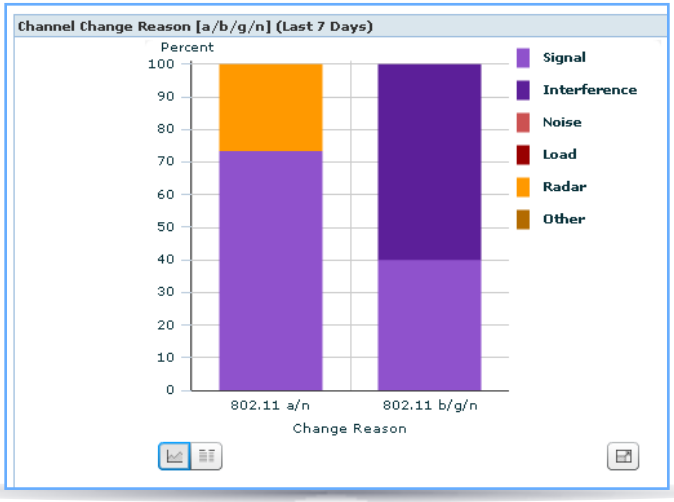
  Changes in "channel / air quality" are monitored, and Access Point channel assignment is changed when deemed appropriate to preserve predictability

- TPC—Transmit Power Control

  Transmit Power is adjusted down or up based on radio to radio pathloss calculation when deemed appropriate to preserve predictability

- CHDM—Coverage Hole Detection and Mitigation

  Transmit Power is adjusted up on Access Points when coverage holes are detected and deemed appropriate to preserve predictability



Cisco's VideoStream Technology

Wired-Like Video Delivery over Wireless

BEFORE
Manual RF Management

Dean | Classroom | Sports Event

AFTER
Dynamic RF Management

Dean | Classroom | Sports Event

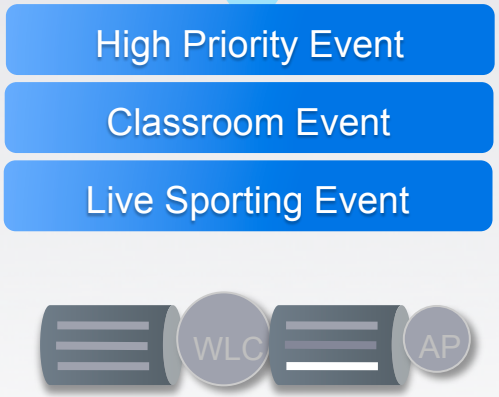
Cisco VideoStream—Improves Predictability and Performance

Why is Cisco's VideoStream so Unique?

We Optimize End-to-End Video Starting at the Access Point

Multicast to Unicast Conversion at the AP

Selectable Stream Prioritization



Resource Reservation Prevents Oversubscription

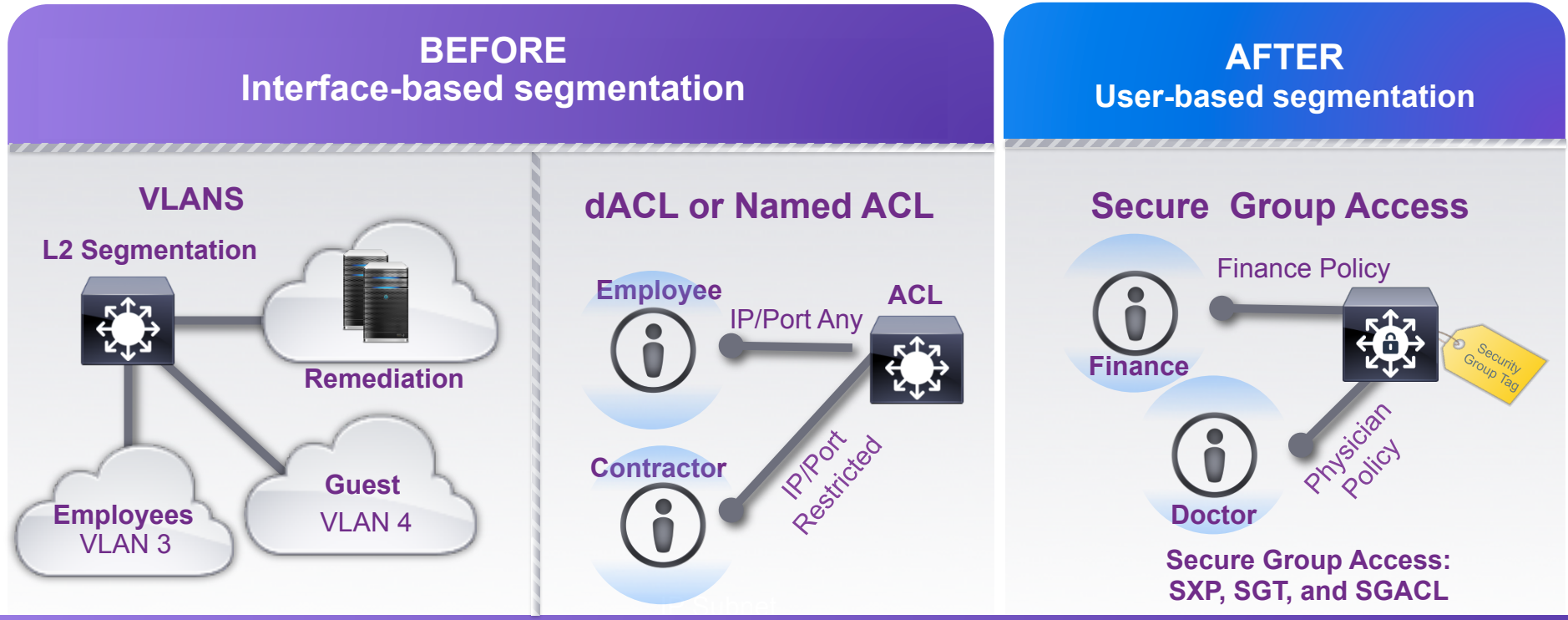
Miercom

Tested for 30X Less Bandwidth Consumed and Double the Performance of Competitors

Cisco's TrustSec & Secure Group Access

Multiple option for policy and segmentation:

- **VLANs** – interface-based Layer 2 segmentation
- **Downloadable ACL (wired) or Named ACL (wireless)** – interfaced based Layer 2,3&4 segmentation
- **Secure Group Access –** user and resource based Layer 2,3&4 segmentation – independent of topology

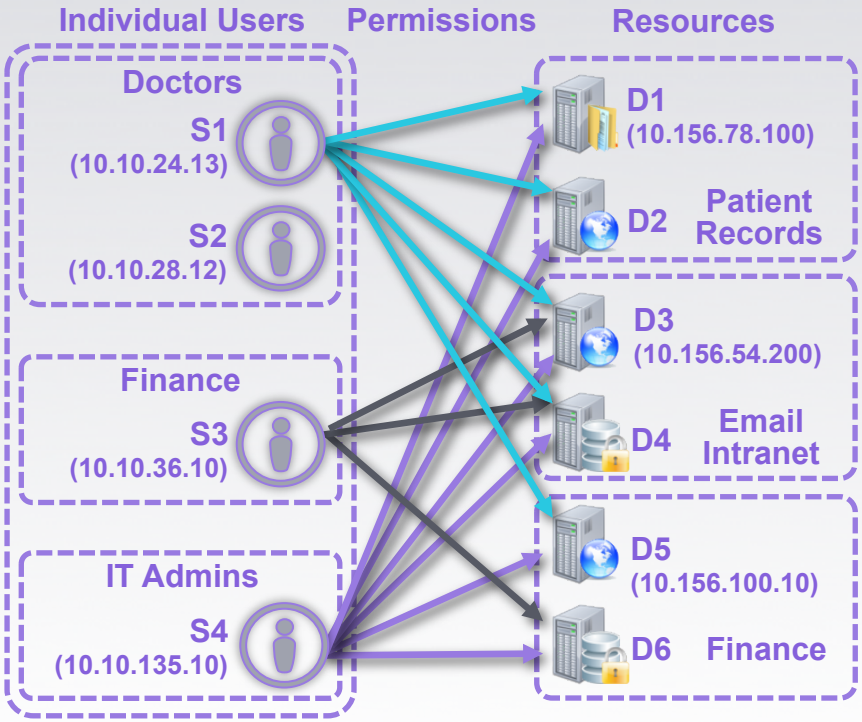


Cisco SGA—User & Resource based Segmentation

Cisco's TrustSec & Secure Group Access

User and resource based segmentation – independent of topology

BEFORE
Interface-based segmentation



AFTER
User and Resource based segmentation

	Intranet Portal	Email Server	Financial Servers	Patient Records
Doctor	Web	IMAP	No Access	Web File Share
Finance	Web	IMAP	Web	No Access
IT Admin	Web, SQL, SSH	Full Access	SQL	SQL

- Simple Simplifies ACL creation
- Simple Simplifies ACL management
- Simple SGA provides user and resource based segmentation - independent of topology

Cisco SGA—User & Resource based Segmentation

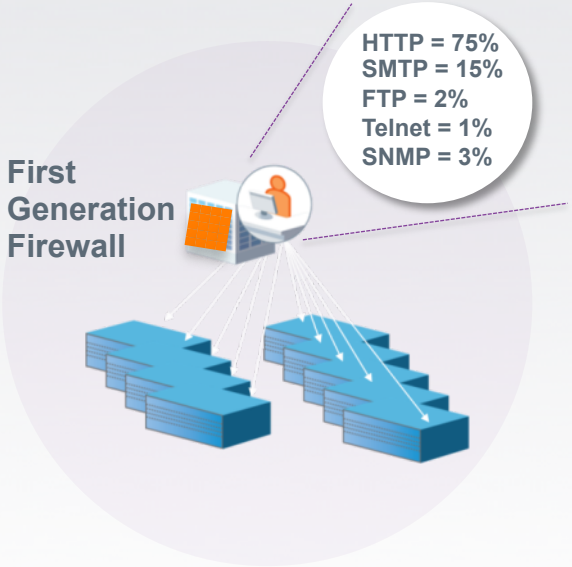
Cisco's Application Visibility and Control

Identify, Analyze, and Optimize Application Traffic

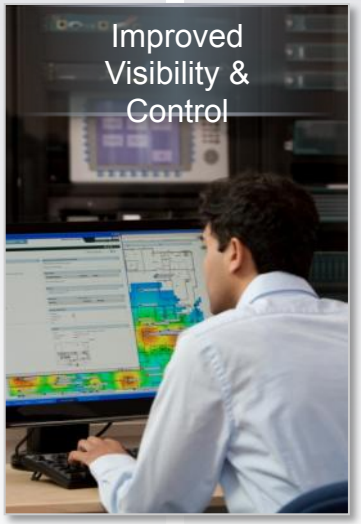
BEFORE

Application View & Control based on L4 Firewall sessions

Visibility to the port level interaction but not the applications running within the port



FW L4 Session Visibility and Control

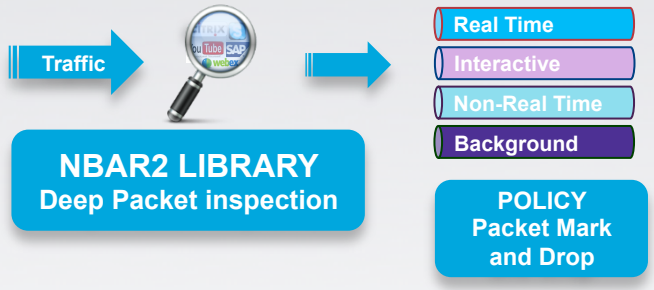


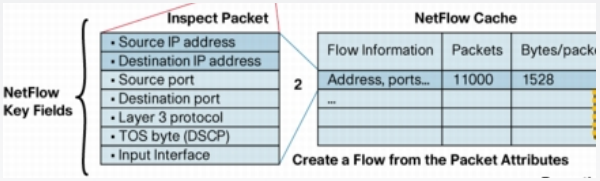
AFTER

Network Based Application Recognition - **NBAR2**

Deep Packet Inspection and App ID

Wireless LAN Controller





View, Control and Troubleshoot - End User Application Experience

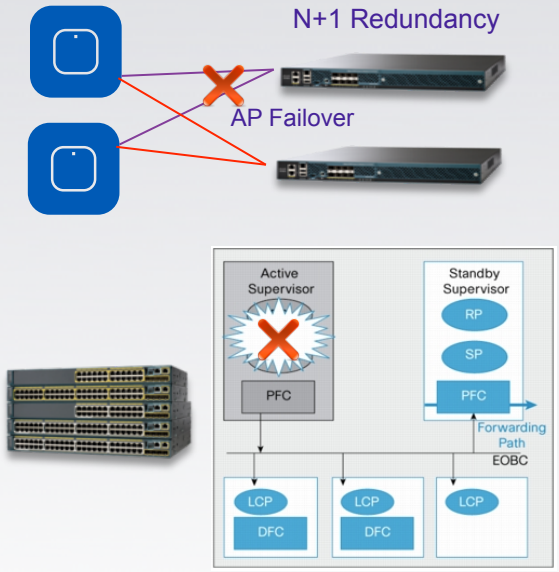
Cisco WLAN AVC and Prime Assurance Provides Unparalleled Visibility & Control

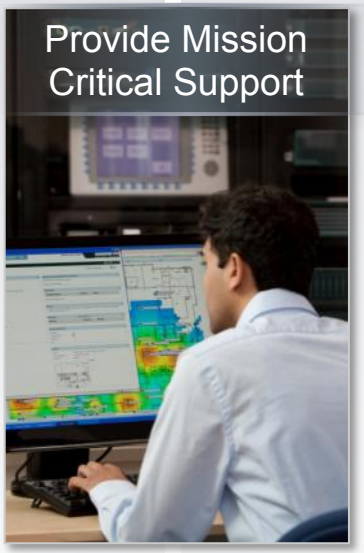
Cisco's Stateful Switchover

Sub second recovery / convergence for both WLAN and LAN

BEFORE

WLAN & LAN recovery / convergence times significantly different

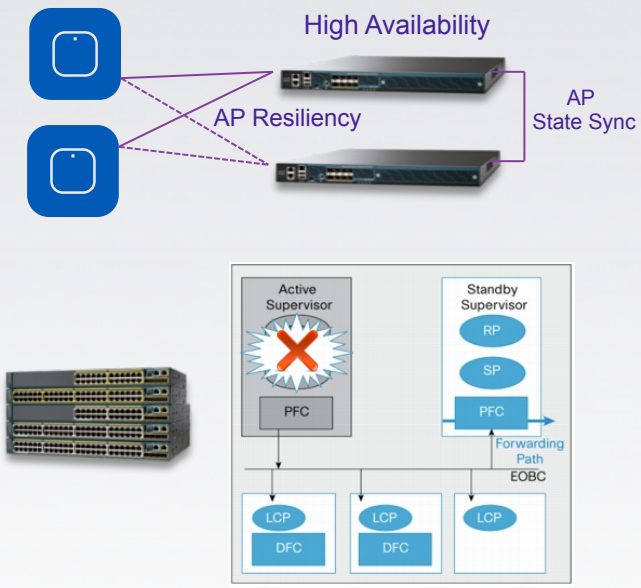




- ✗ WLAN 30+ second recovery / convergence
- ✓ LAN Sub second recovery / convergence

AFTER

WLAN & LAN recovery / convergence times are both sub second



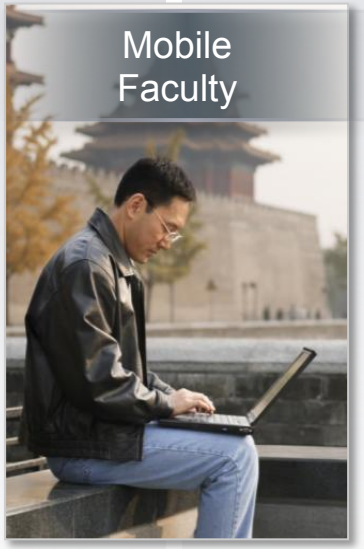
- ✓ WLAN Sub second recovery / convergence
- ✓ LAN Sub second recovery / convergence

Cisco SSO—Improves Predictability

Cisco's AnyConnect Technology

Industry's First Context-Based and Persistent VPN Connectivity

BEFORE
Unmanaged devices—
risk of data loss and lack of access



AFTER
Always-on VPN connectivity

- Acceptable Use
- Access Control
- Data Loss Prevention

Cisco AnyConnect—Always On VPN Connectivity

Acceso Unificado en el Campus Universitario

One Policy – One Management – One Network

Juan Antonio Castilleja – Systems Engineer