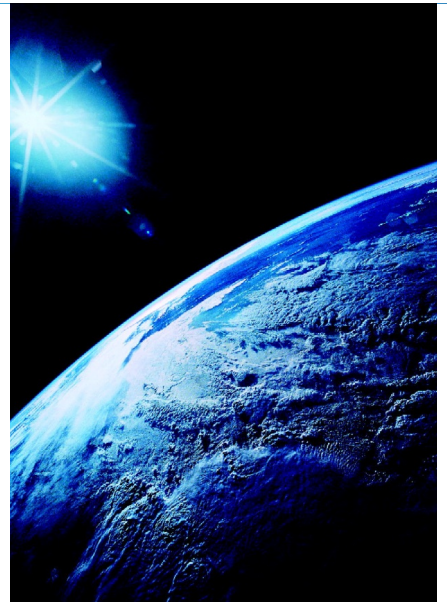
Cisco Connect

Brussels, Belgium
April 18 2013

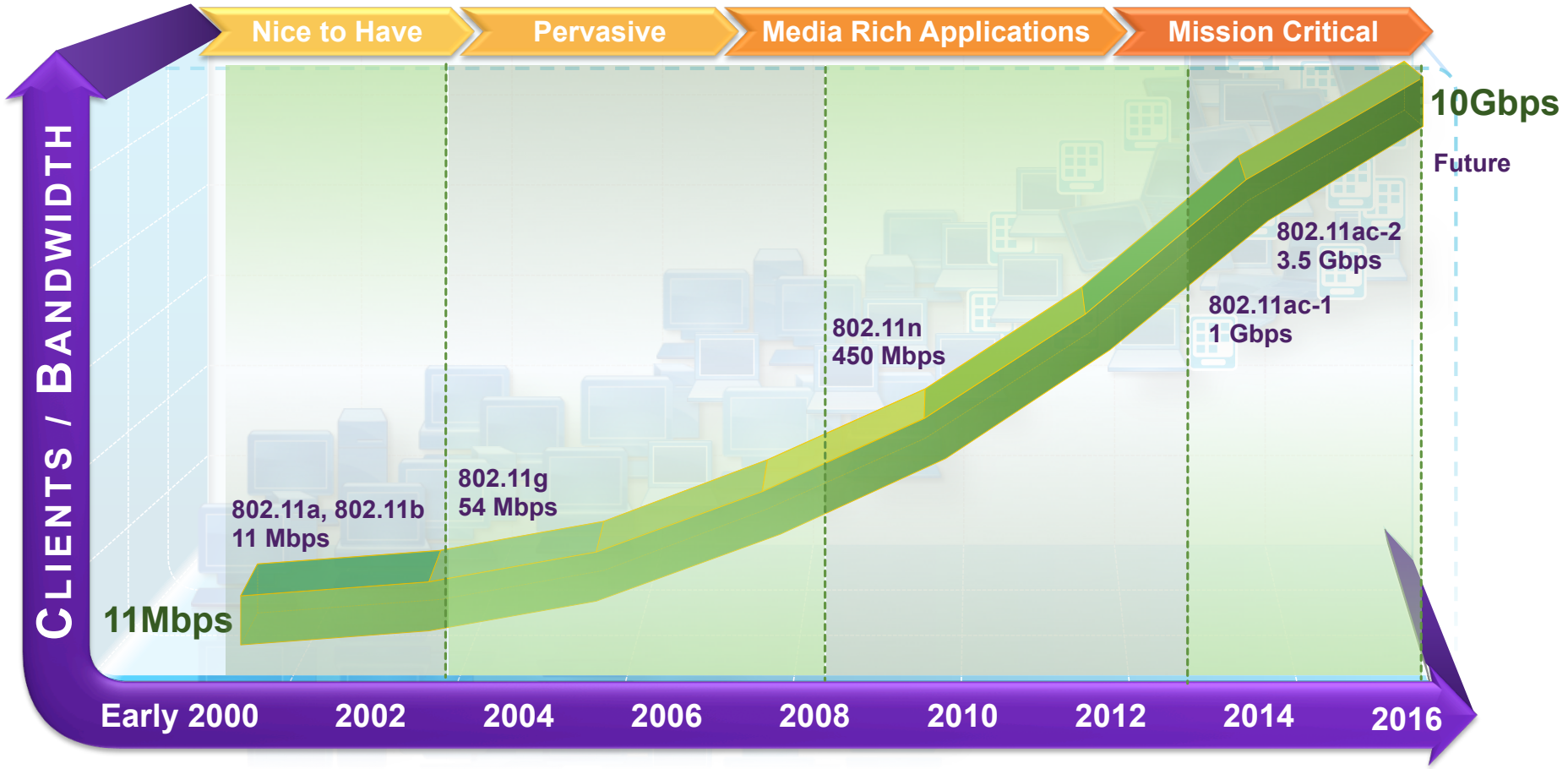
Unified Access:
One Network, One Policy and One Management



Marchal Sebastien

Partner System Engineer

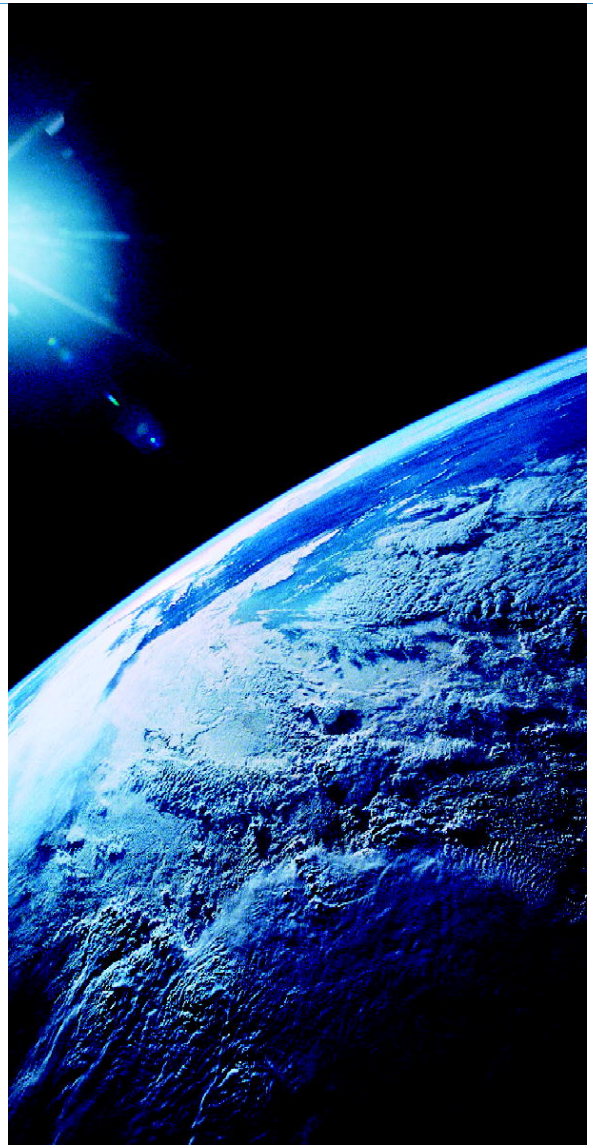
Wireless Standards – Past, Present, and Future



Unified Access

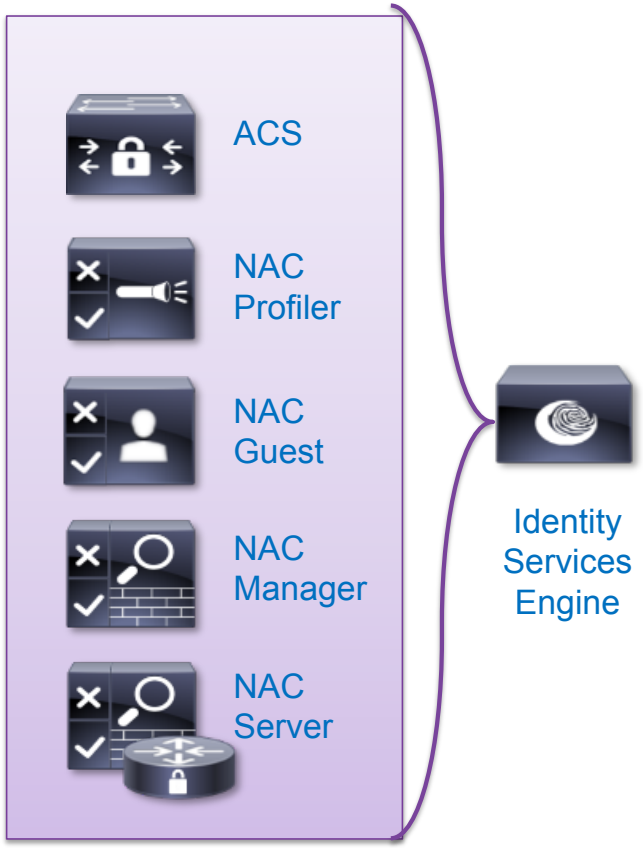
Uncompromised User Experience on Any Workspace

One Policy



Identity Services Engine

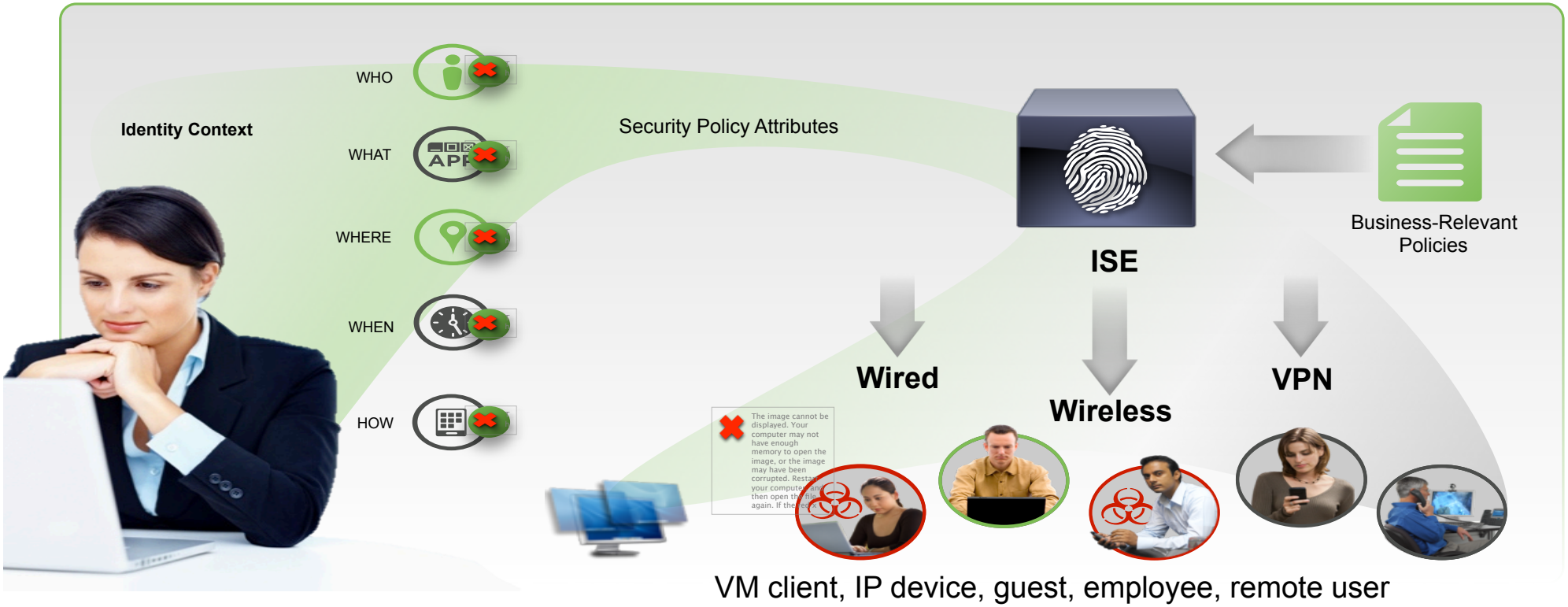
Policy Server Designed for Unified Access



- Centralized Policy
- Guest Access Services
- Device Profiling
- Device Onboarding
- Native Supplicant Provisioning
- Posture Assessment
- Monitoring / Troubleshooting
- Reporting

Cisco Identity Services Engine (ISE)

All-in-one Enterprise Policy Control



Replaces AAA & RADIUS, NAC, guest mgmt & device identity servers

Secure Access: Classification Attributes

Who?	 Employee	 Attacker	 Guest
What?	 Personal Device	 Company Asset	
How?	 Wired	 Wireless	 VPN
Where?	 @ Starbucks	 Headquarters	
When?	 Weekends	 (8:00am – 5:00pm) PST	

Context Aware Access
ISE Authorization Policy Example

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Black List	if **Blacklist**	then Blackhole Traffic
✓	Profiled Cisco IP Phones ISE	if **Cisco-IP-Phone**	then Cisco_IP_Phones_ISE
✓	Printers	if **HP-Color-LaserJet-4700** OR **Xerox-Phaser-6010n**	then Printers
✓	Corp Workstation	if (Wireless_Access_ISE AND Wired_802.1X_ISE AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Computers AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User failed and machine succeeded AND Session:PostureStatus EQUALS Compliant AND NewYork)	then AD_Login
✓	Employee and Corp_Workstation	if (Wireless_Access_ISE AND Wired_802.1X_ISE AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Users AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User and machine both succeeded AND Session:PostureStatus EQUALS Compliant AND NewYork)	then Employee
✓	Registered Devices	if **RegisteredDevices** AND (Wired_802.1X_ISE AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID)	then BYOD Access
✓	Personal Devices	if **Employee** AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2	then BYOD Provisioning
✓	VPN	if VPN	then VPN Employee
✓	Guest	if **Guest** AND Bussiness Hours	then Internet Only
✓	Default	if no matches, then DenyAccess	

What is Profiling ?

NMAP

NetFlow

HTTP

SNMP

DHCP

LLDP

Radius

Collection

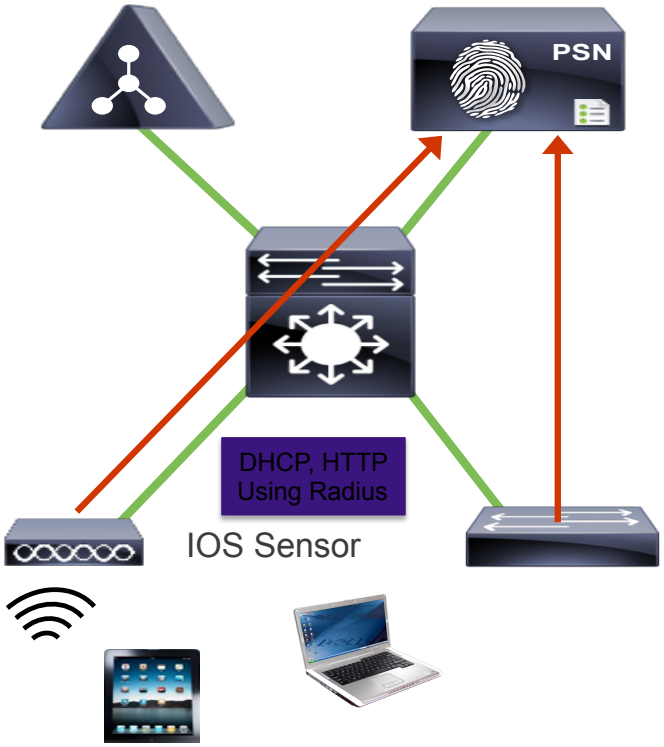
Process of collecting data to be used
for identifying devices
Uses Probes for collecting device attributes

Classification

Classifies based on Device fingerprint

Collection: Getting traffic to Probes:
IOS Sensor

What?



Advantages: improved scalability and simplified deployment

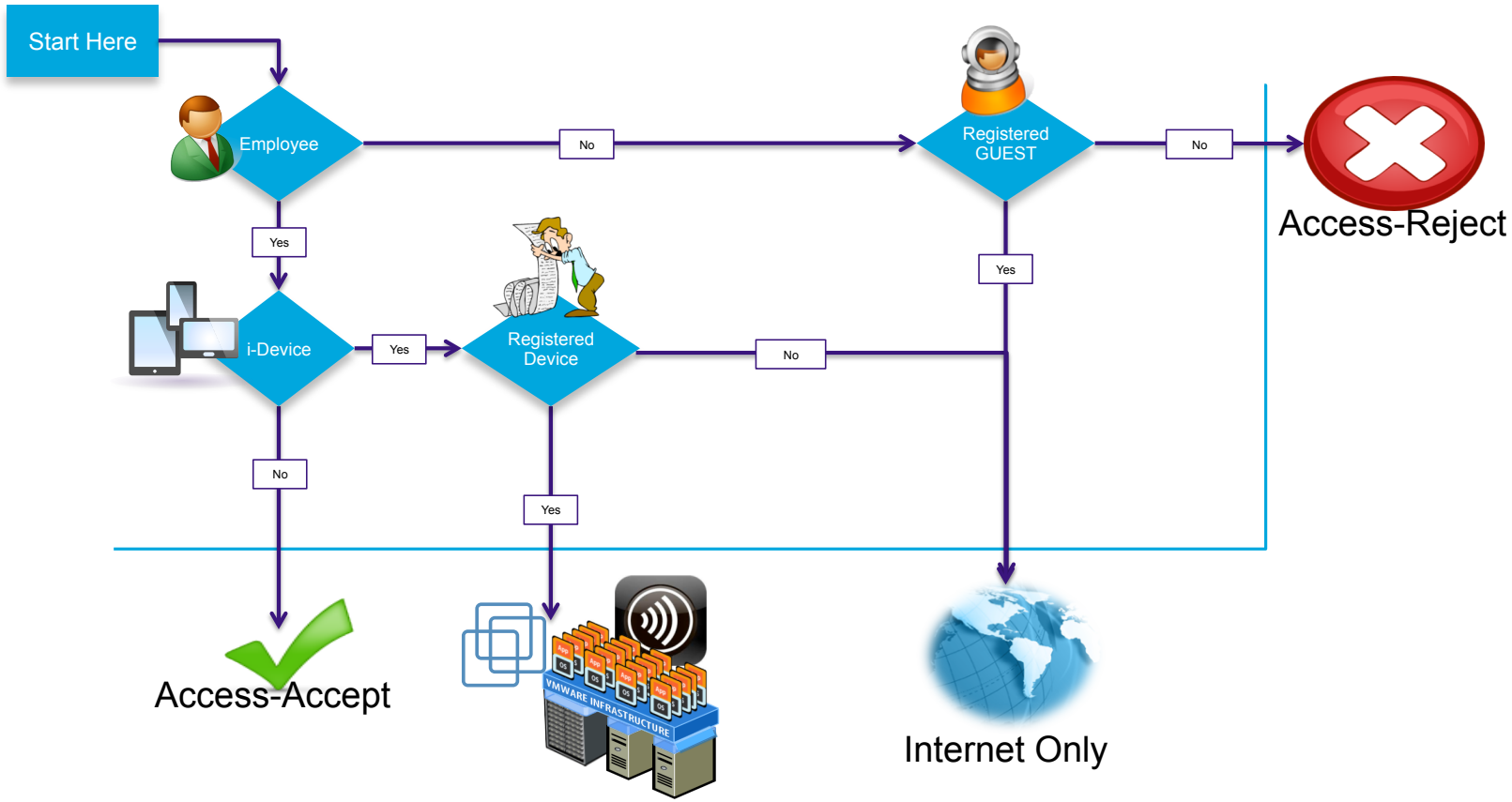
- Aggregate and forward profiling information over existing RADIUS traffic between NAD and ISE
- IOS switches collect DHCP, LLDP and CDP data.
- WLC collect HTTP. DHCP data.
- Data sent to ISE as cisco-av-pair using RADIUS accounting updates.

- Supported on IOS 15.0(1)SE1 for Cat 3K
- Supported on IOS 15.1(1)SG for Cat 4K
- WLC 7.2.11

```
Configuration Commands:

device-sensor accounting
device-sensor notify all-changes
```

What makes a Access policy?

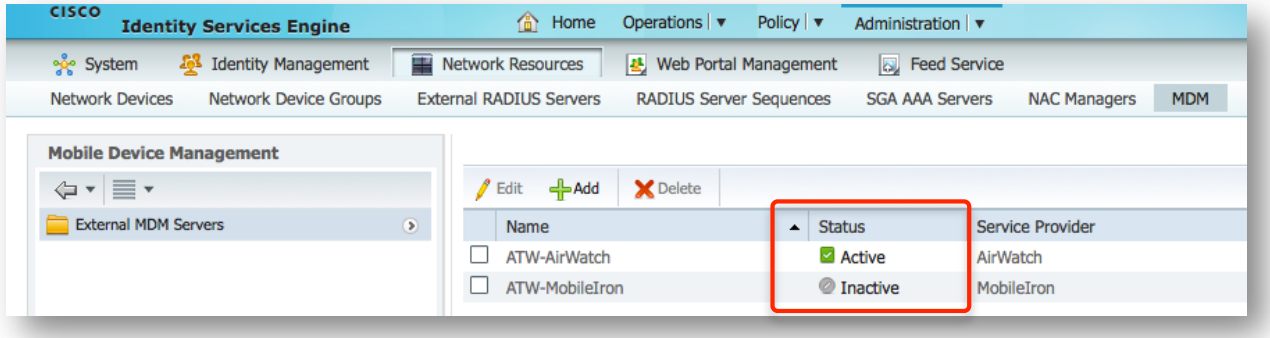


BYOD -> MDM ?

MDM Vendors

Requires API in MDM Server

Only ONE may be active at a time in ISE



Cisco Published API Specs to 4 Vendors:

- AirWatch Version 6.2
- Mobile Iron Version: 5.0
- ZenPrise Version: 7.1
- Good Version: 2.3

Initial Vendors

MobileIron

airwatch™

ZENPRISE

Good

SAP

Attributes from MDM

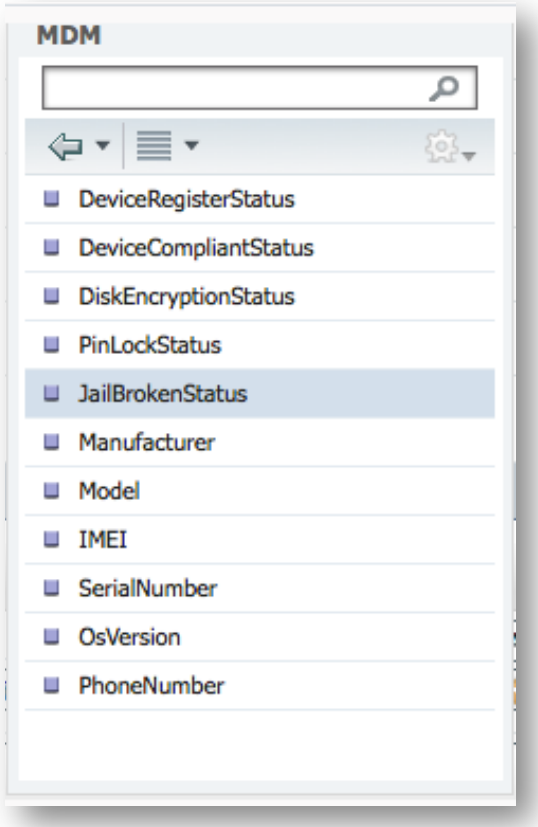
With the API, we can query on:

General Compliant or ! Compliant (Macro level) -or-

- Disk encryption is one
- Pin lock
- Jail broken

Bulk re-check against the MDM every 4 hours.

- But we are not using the cached data in the AuthZ
- If result of Bulk Re-check shows that a device is no longer compliant – we will send a CoA to terminate session.
- Works same with all 4 vendors.

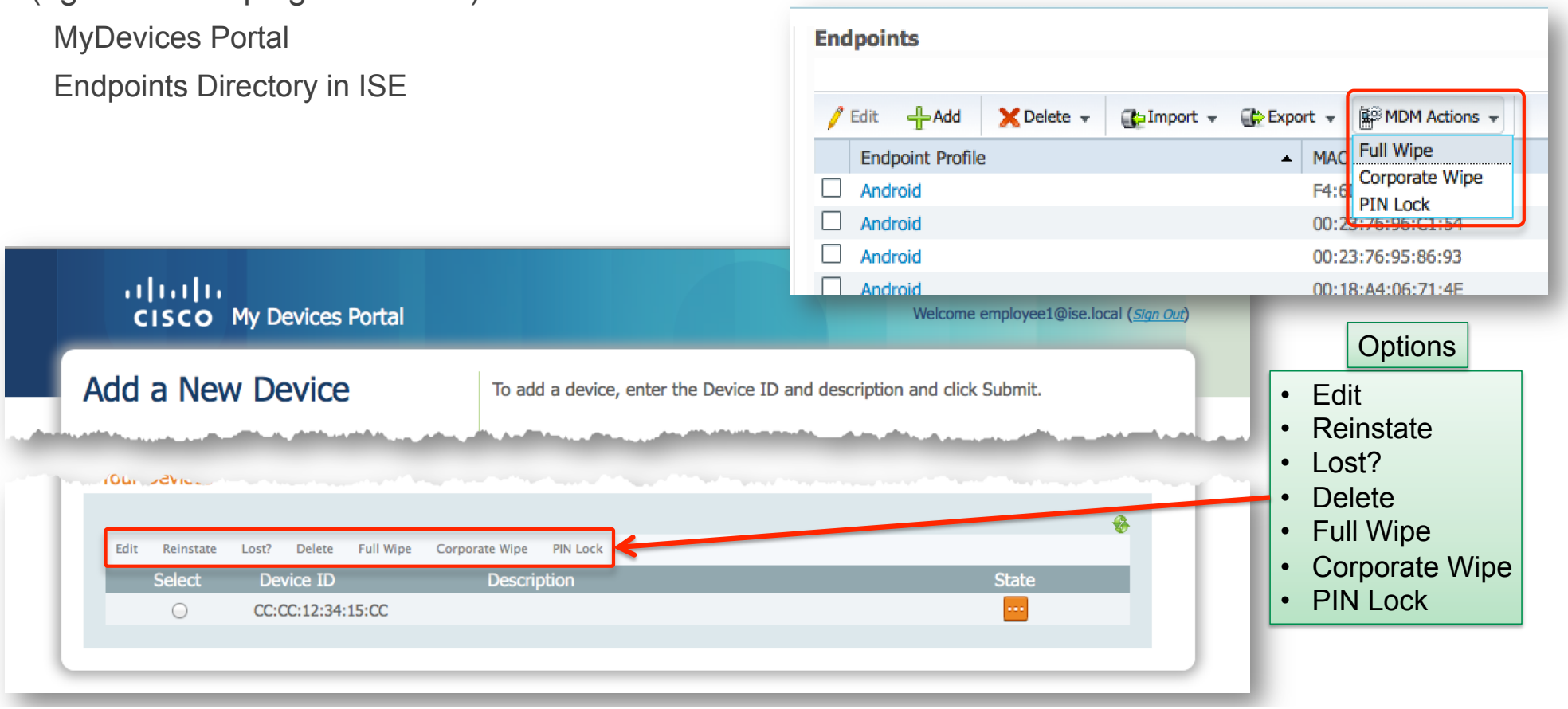


MDM Integration / My Devices Portal

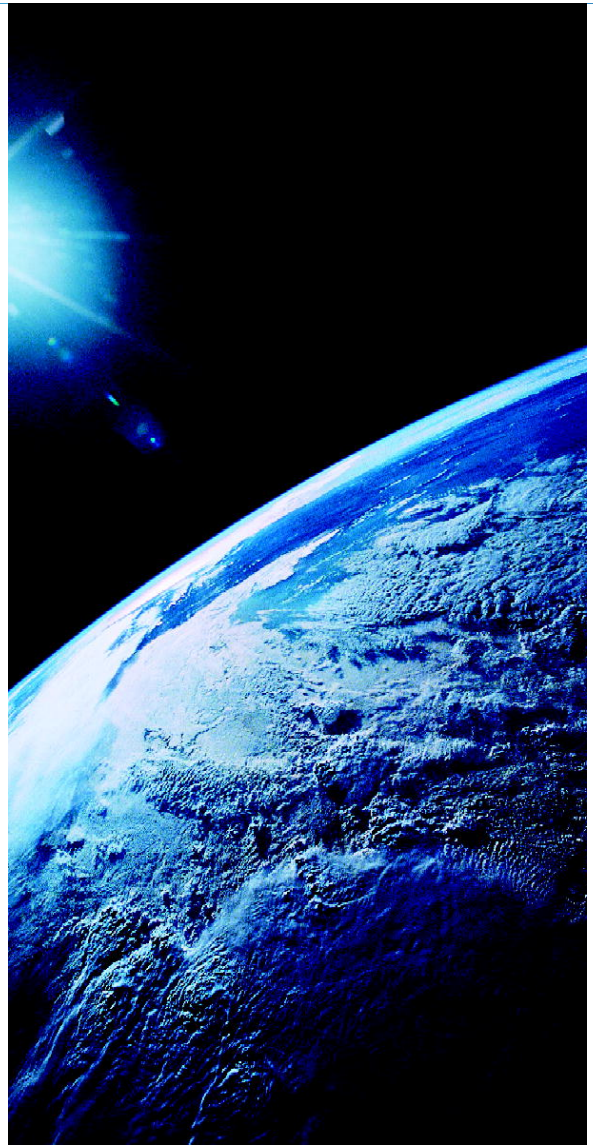
Ability for administrator and user in ISE to issue remote actions on the device through the MDM server (eg: remote wiping the device)

MyDevices Portal

Endpoints Directory in ISE

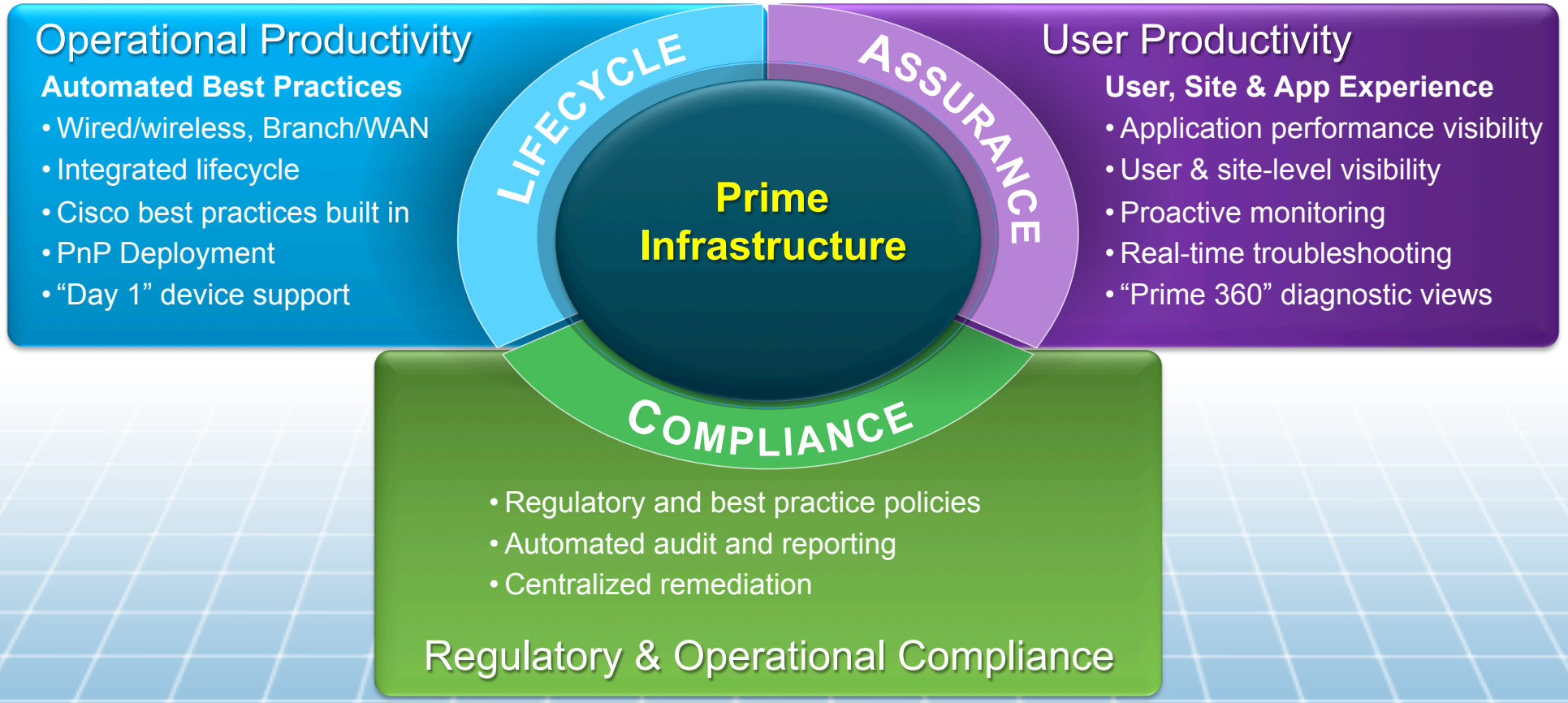


One Management



One Management with Cisco Prime Infrastructure

Integrated Wired/Wireless Lifecycle and Assurance Management



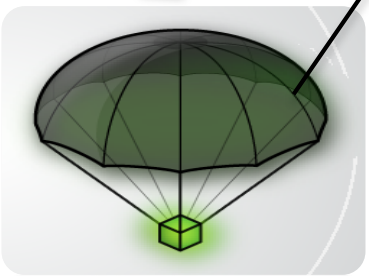
Lifecycle approach

- monitor fault
- monitor for performance
- troubleshoot
- manage configuration backup
- upgrade devices

design

- prepare template for configuration
- prepare template for monitoring
- describe enterprise organization in the management platform

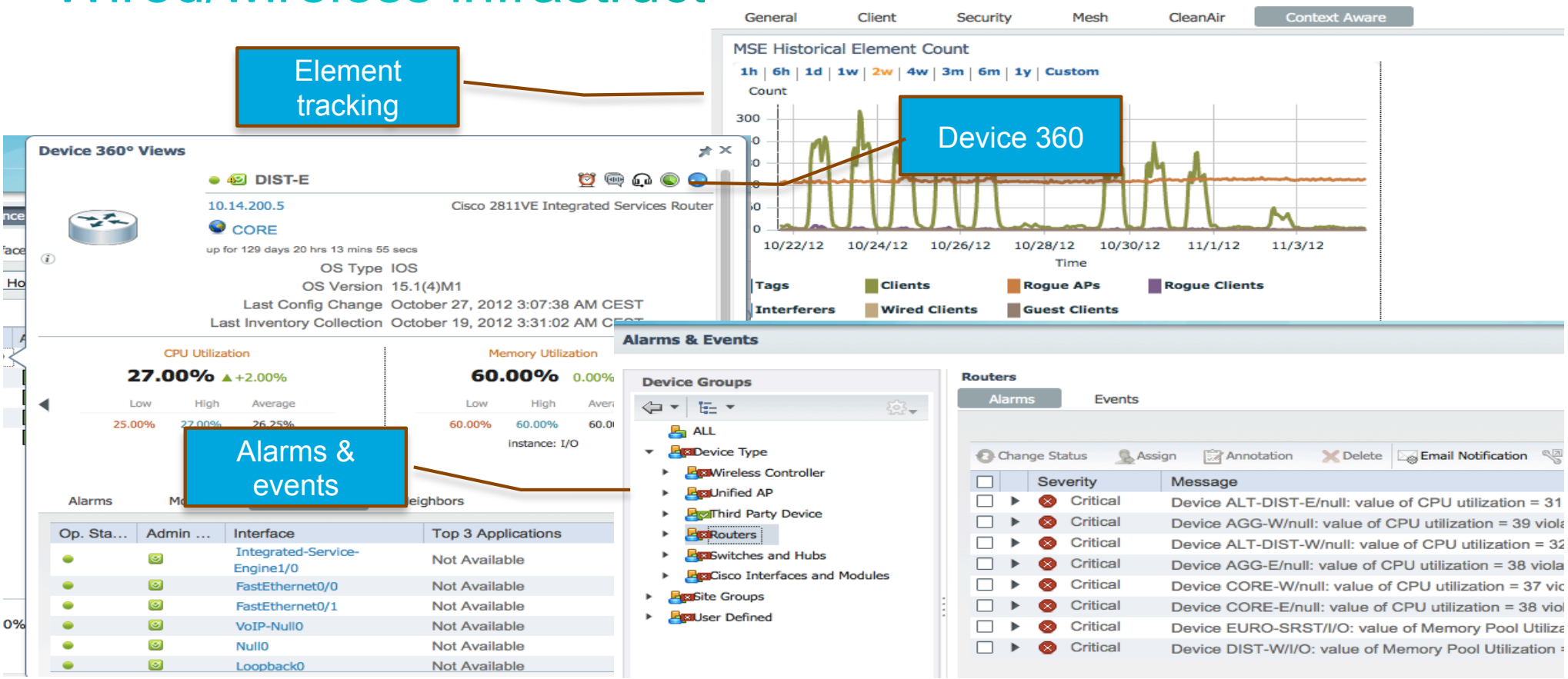
operate



deploy

- deploy templates

Wired/wireless infrastructure monitoring



Identity Service Engine (ISE) Integration

Client Type and Policy Visibility

Single pane of glass view and lifecycle management for Wired and Wireless

IP Address	User Name ▲	Type	Vendor	Device Name	Endpoint Type	Protocol	Interface
10.20.1.101	Jack		Intel	5508	Microsoft-Workstation	802.11n(5GHz)	data
10.20.1.103	Jack		Dell	CoreSwitch.wlan.local	Microsoft-Workstation	802.3	GigabitEthernet1/0/40
10.50.1.100	Jane		Intel	5508	Microsoft-Workstation	802.11n(5GHz)	data-contractor

General

User Name	**Jack**
IP Address	**10.20.1.101**
MAC Address	**00:21:6a:5a:85:3a**
Vendor	**Intel**
Endpoint Type	**Microsoft-Workstation**
Client Type	**Regular**
Media Type	**Lightweight**
Mobility Role	**Local**
Hostname	**Data Not Available**
CCX	**V4**
E2E	**V1**
Power Save	**OFF**

Device Identity or Profile from ISE Integration

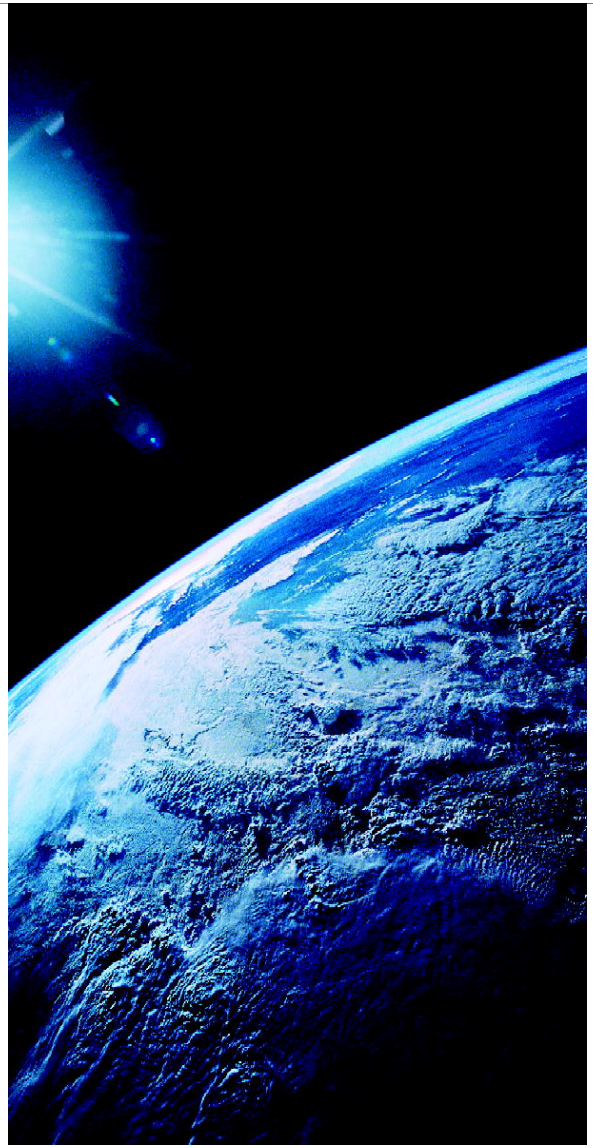
AAA Override Parameters Applied to Client

Policy Information Including Posture

Security

Security Policy Type	**WPA2**
EAP Type	**PEAP**
On Network	**Yes**
802.11 Authentication	**Open System**
Encryption Cipher	**CCMP (AES)**
SNMP NAC State	**Access**
Radius NAC State	**RUN**
AAA Override ACL Name	**none**
AAA Override ACL Applied Status	**N/A**
Redirect URL	**none**
ACL Name	**none**
ACL Applied Status	**N/A**
H-REAP Local Authentication	**No**
Policy Manager State	**RUN**
Authenticating ISE	**ISE**
Authorization Profile Name	**AuthEmp**
Posture Status	**Not Applicable**
TrustSec Security Group	**Data Not Available**
Windows AD Domain	**wlan.local**

One Network



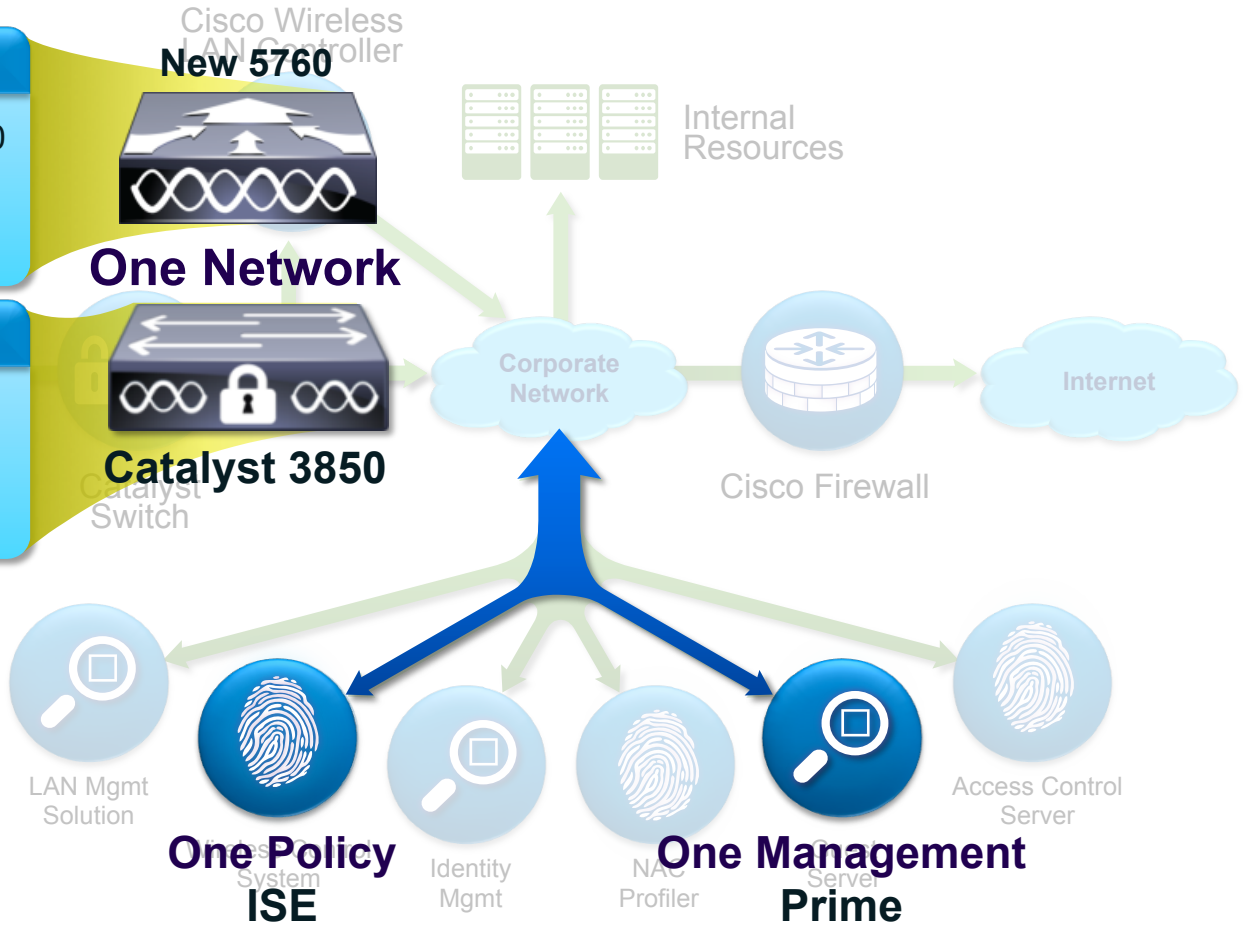
Delivering Converged Access

IOS Based WLAN Controller

- Consistent IOS and ASIC as Catalyst 3850
- Required to scale beyond 250 AP or 16K client domains

Converged Access Mode

- Integrated wireless controller
- Distributed wired/wireless data plane (CAPWAP termination on switch)



Single Platform for Wired and Wireless

20+ Years of IOS Richness – Now on Wireless

WIRELESS

Features:

- 802.11n
- Clean Air
- Video Stream
- Radio Resource Management (RRM)
- Wireless Intrusion Prevention System (WiPS)
- 802.11ac Ready

Benefits

- Built on **Doppler** – Cisco's Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

WIRED

Features:

- Stacking, Stackpower
- Trustsec/Identity
- AVC/Medianet
- Flexible Netflow
- Granular QoS
- Smart Operations
- EnergyWise
- Virtualization

Note: All features may not be available on new platforms at introduction but are expected to be added within 12-18 months

UA Converged Wired/Wireless Access
Components

One Policy

- BYOD policy management
- Device profiling and posture
- Guest access portal

One Management

- Full wired and wireless management
- User/device centric view
- Intuitive troubleshooting workflows

Catalyst 3850

- Industry's first fully integrated wired and wireless switch
- Wireless: 480G stack, 50 APs, 2K clients, 40G
- Flexible Netflow, Granular QoS
- First IOS Release: 15.0(1)EZ

Sup 8E on Catalyst 4500E

- 888 Gbps. Sup 7-E equiv TCAM
- Wireless: 40G Capacity, 50 APs, 2K clients
- 8 x 10G SFP+
- FNF, VSS*

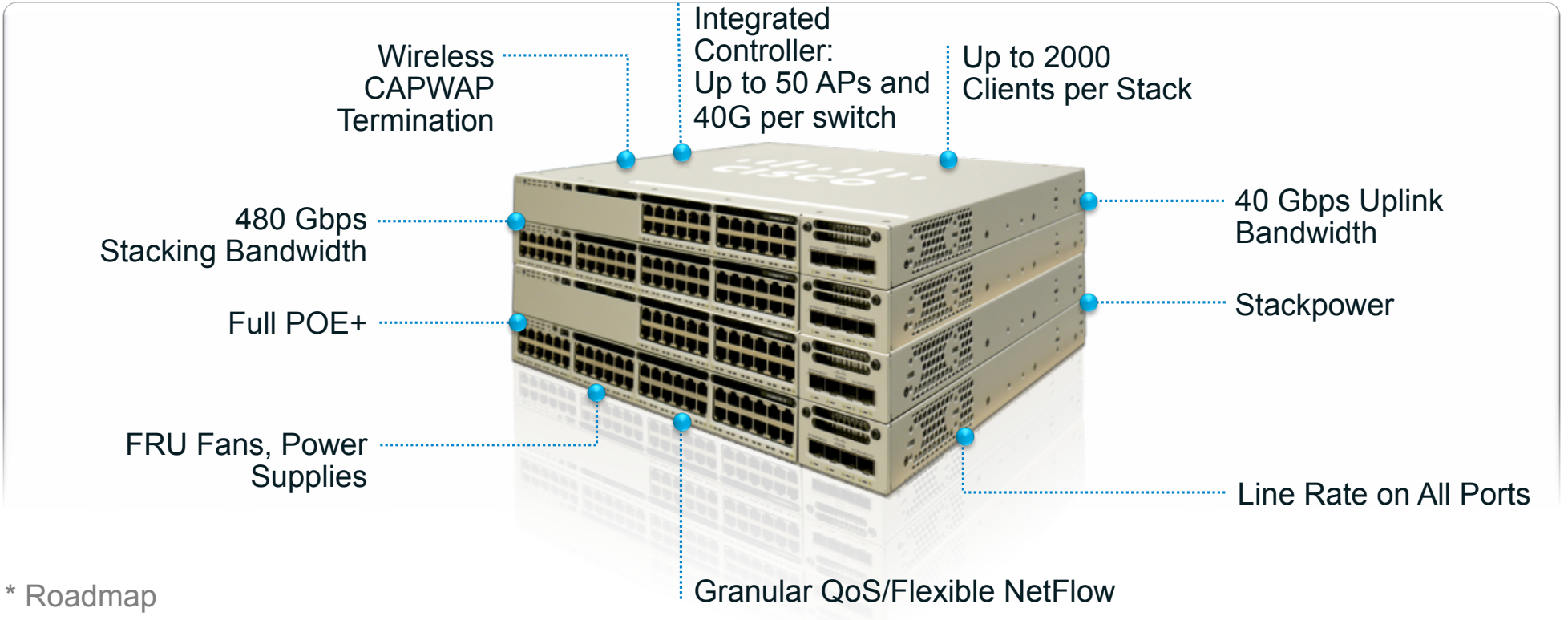
5760 Wireless Controller

- Consistent IOS with Catalyst UA 3850
- 60G, 1K APs, N+1 Redundancy
- FNF, Granular QOS
- First IOS Release: 15.0(1)EZ

Best-in-Class Performance, Security, and Resiliency

* - Software Roadmap . Expected to be added within 12-18 months

NEW Catalyst 3850 Switch



* Roadmap

Built on Cisco's Innovative "Doppler" ASIC

Converged Wired/Wireless Access – Benefits

Single platform for wired and wireless

Common IOS, same administration point, one release

Network wide **visibility** for faster troubleshooting

Wired and wireless traffic visible at every hop

Consistent security and quality of service **control**

Hierarchical bandwidth management and distributed policy enforcement

Maximum **resiliency** with fast stateful recovery

Layered network high availability design with stateful switchover

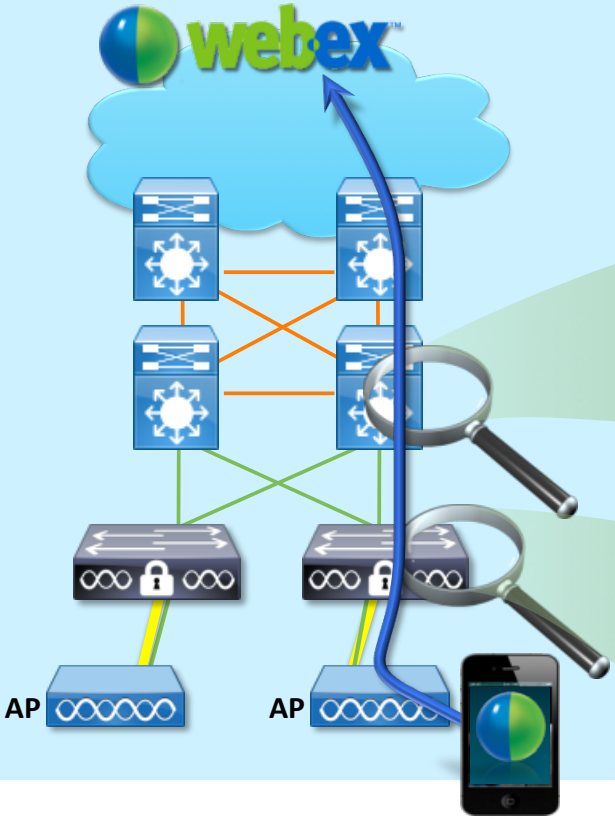
Scale with distributed wired and wireless data plane

480G stack bandwidth; 40G wireless/switch; 16K clients without separate WLC – future proof

Unified Access - One Policy | One Management | One Network

Network Wide Visibility for Faster Troubleshooting

Converged Access Deployment



Employee joins webex call on iPhone

Employee iPhone connected

Benefits

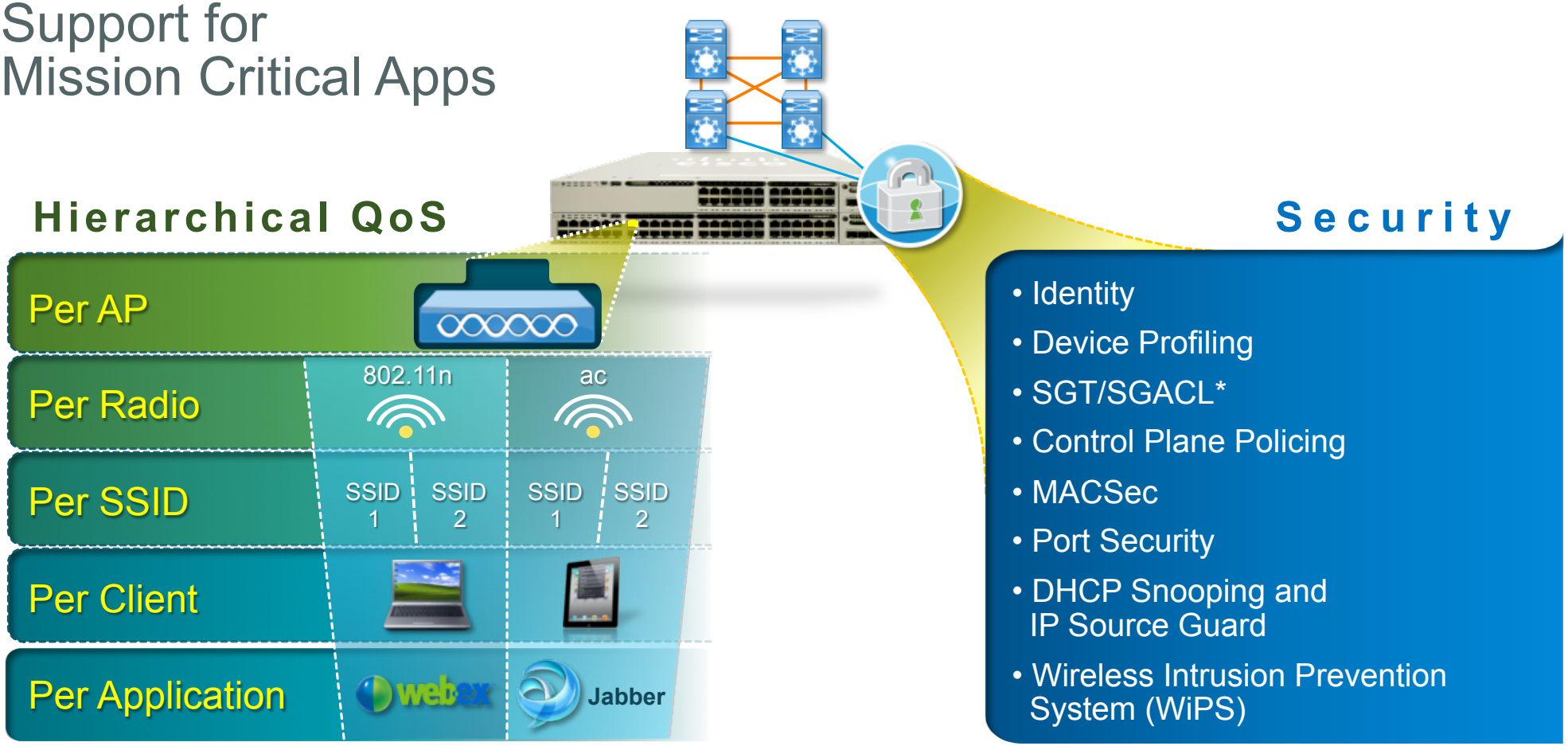
- **Track applications at every hop**
- **Root cause issues quickly**

- **App level visibility –** Flexible Netflow, Wireshark
- **Media Troubleshooting** – Medianet

Device Identification
- Device Profiling

Consistent Security and Quality of Service Control

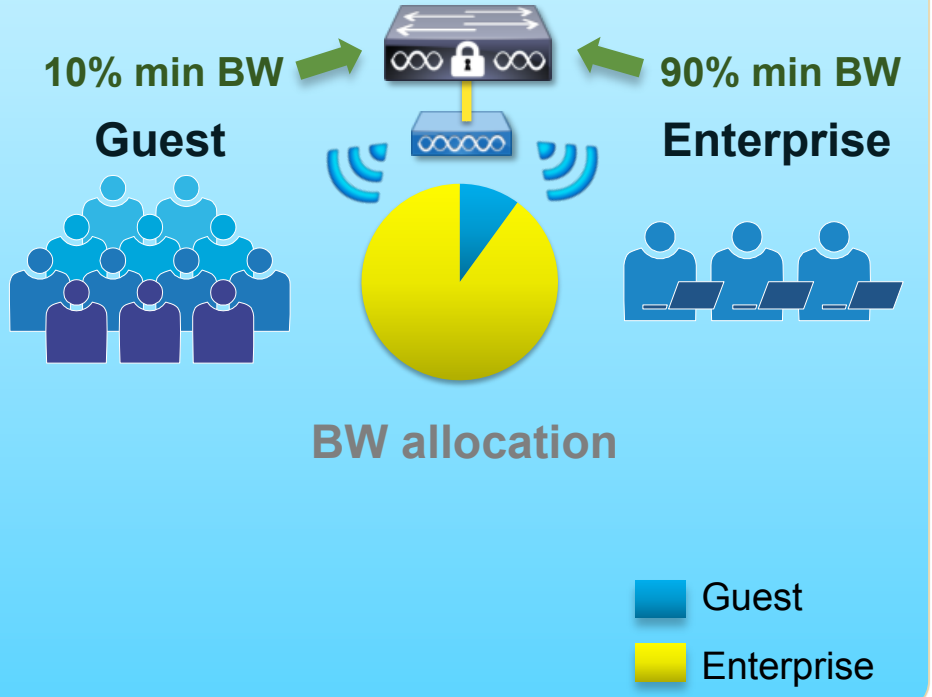
Support for Mission Critical Apps



Hierarchical Bandwidth Management

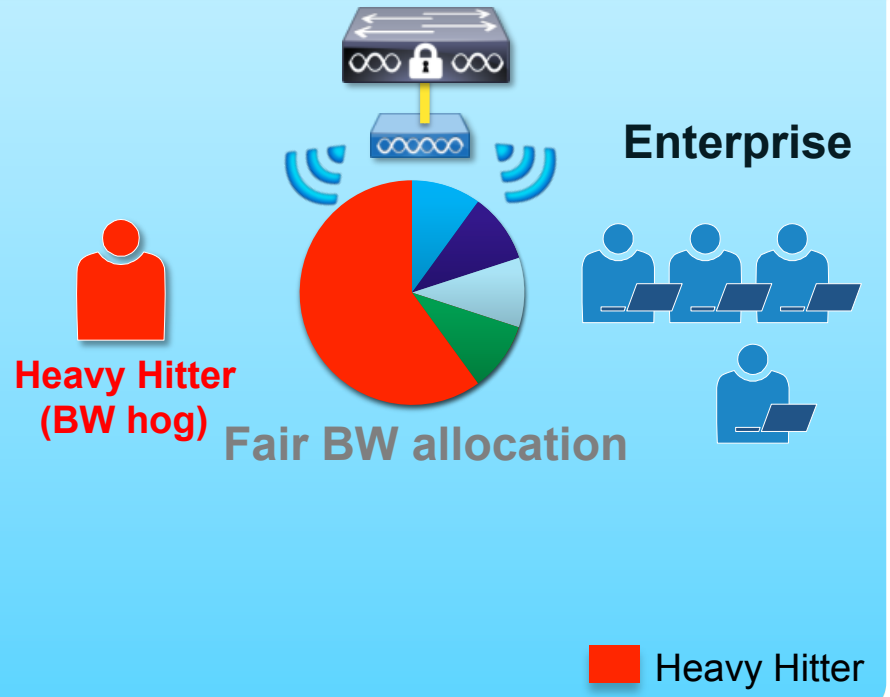
per SSID Bandwidth

Converged Access
Deterministic SSID bandwidth

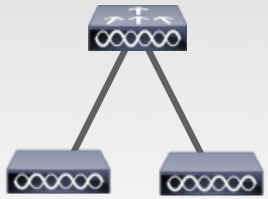
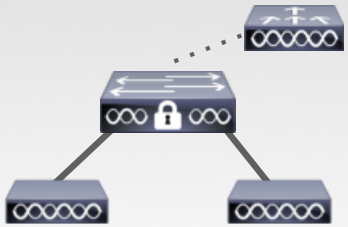


Fair Sharing

Usage based fair bandwidth allocation



Unified Access—Wireless Deployment Modes

	Autonomous	FlexConnect	Centralized	Converged Access
				
	Standalone APs	Traffic Distributed at AP	Traffic Centralized at Controller	Traffic Distributed at Switch
Target Positioning	**Small Wireless Network**	**Branch**	**Campus**	**Branch and Campus**
Sales Motion	Wireless only	Wireless only	Wireless only	Wired and Wireless
Benefits	• Simple and cost-effective for small networks	• Highly scalable for large number of remote branches • Simple wireless operations with DC hosted controller	• Simplified operations with centralized control for Wireless • Wireless Traffic visibility at the controller	• Wired and Wireless common operations • One Enforcement Point • One OS (IOS) • Traffic visibility at every network layer • Performance optimized for 11ac
Key Considerations	• Limited RRM, no Rogue detection	• L2 roaming only • WAN BW and latency requirements	• System throughput	• Catalyst 3850 in the access layer

Unified Infrastructure: Wireless Innovation

Cisco Mobility Technology for High-Performance Wireless Network

Best-in-Class Mobility Technology

Cisco Aironet® 600,1600, 2600, 3600 Access Point

Access Point Innovation

Tablet access point, with enhanced throughput and coverage for advanced applications for tablets and smart devices

Cisco CleanAir™ Technology

Improved Performance

Proactive and automatic interference mitigation

Cisco® ClientLink 2.0

Improved Performance

Proactive and automatic beam forming for IEEE 802.11n and traditional clients

Cisco VideoStream Technology

Improved Performance

Wired multicast over a wireless network

Summary

Cisco's Unified Access Strategy

One Policy
One Management
One Network

IT Top of Mind

- Manage complexity and reduce costs?
- Offer secure, mission critical services?
- Future proofed for scale?

Converged Access

- Distributed wired/wireless data plane with new Cisco Catalyst 3850
- Benefits of single platform, visibility, control, resiliency, and scale

Thank you.