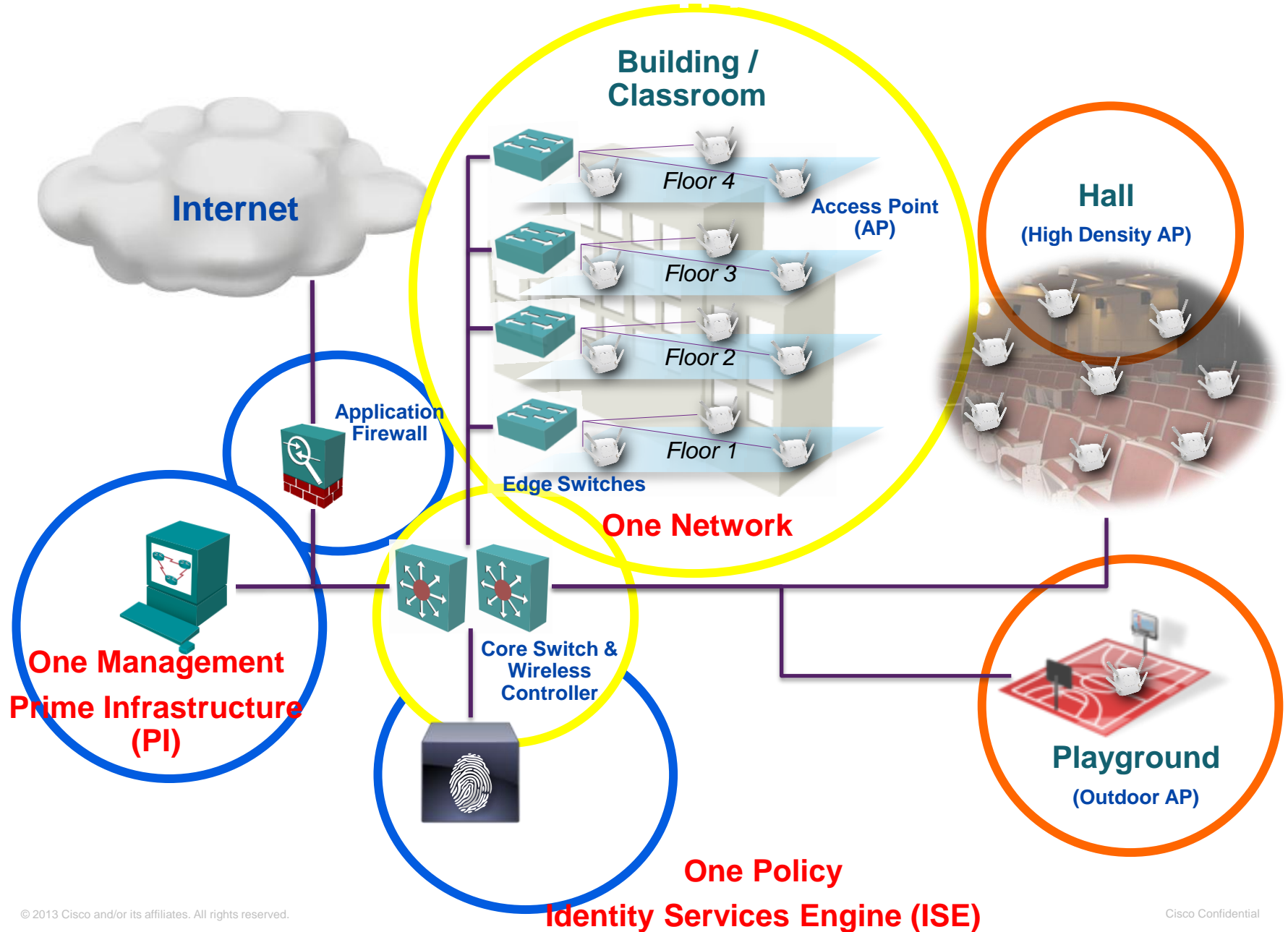# Cisco BYOD Solution

Unified Access -

One Policy,

One Management,

One Network

Clement Tam

Perfect Campus Infrastructure - Unified Access

Internet

Building / Classroom

Hall
(High Density AP)

Application Firewall

Floor 4

Access Point (AP)

Floor 3

Floor 2

Floor 1

Edge Switches

One Network

One Management

Prime Infrastructure (PI)

Core Switch & Wireless Controller

Playground

(Outdoor AP)

One Policy

Identity Services Engine (ISE)

One Policy – Network Control

Wish List **By Cisco ISE, Dream Comes True**

Identity Services Engine

Simplified Policy Management

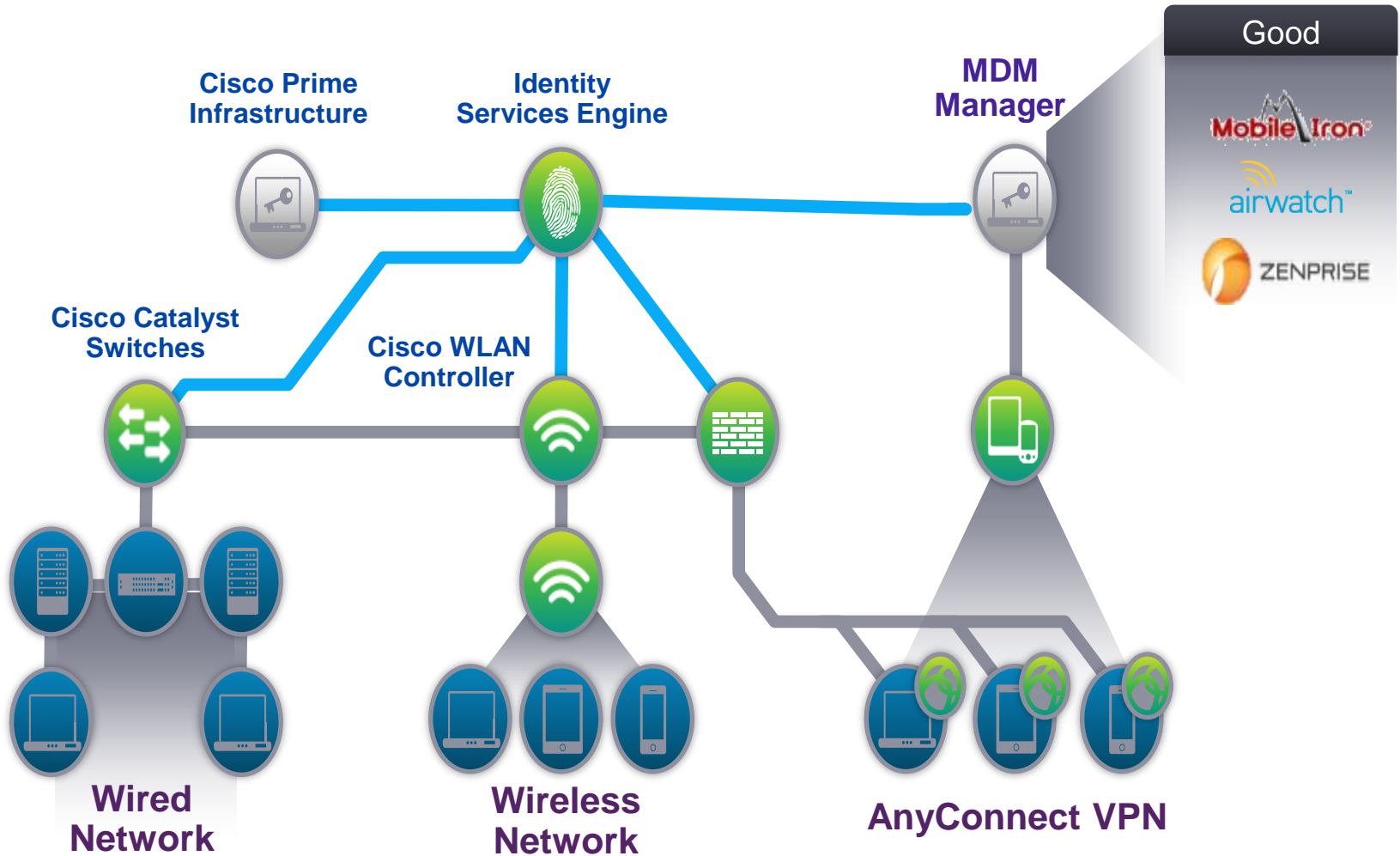| Wish	Service
I only want to allow the "right" users and devices on my network	Authentication Services
I want user and devices to receive appropriate network services	Authorization Services
I want to allow guests into the network and control their behavior	Guest Lifecycle Management
I need to allow/deny iPads in my network (BYOD)	Profiling Services
I want to ensure that devices on my network are clean	Posture Services
I need a scalable way of enforcing access policy across the network	Secure Groups Access

Network Policy vs MDM

Cisco Prime Infrastructure

Identity Services Engine

MDM Manager

Good

MobileIron

airwatch™

ZENPRISE

Cisco Catalyst Switches

Cisco WLAN Controller

Wired Network

Wireless Network

AnyConnect VPN

Cisco One Policy Solution - ISE (Identity Service Engine)

Many Dimensions of Policy and Provisioning

Posture (MDM)	Custom

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	Classrooms	8 am – 4 pm	Student VLAN
	School Device	Wireless	Anywhere	Anytime	Student ACL
Teacher	iOS	Wired	Anywhere	Anytime	Faculty VLAN
	Android	Wireless	Anywhere	Anytime	Faculty ACL
	Windows	VPN		Anytime	

IF $Identity AND $Device AND $Access AND $Location AND $Time AND $Posture (MDM) THEN $Policy

One Management

Wish List By Cisco Prime Infrastructure, Dream Comes True

Prime Infrastructure

Simplified Network Management

I want to monitor the LAN, WLAN and WAN with a single application	Monitoring Services
I want to discover who in the network accessing to unwanted applications	Discovery Services (with ISE)
I want to control the bandwidth and QoS for the students	Control Services (with ISE)
I want to have clear visibility to the RF environment	Planning Services
I want to troubleshoot the LAN, WLAN, and WAN from a single application	Troubleshooting Services
I need to monitor and audit system-wide configurations for compliance purposes	Compliance Services

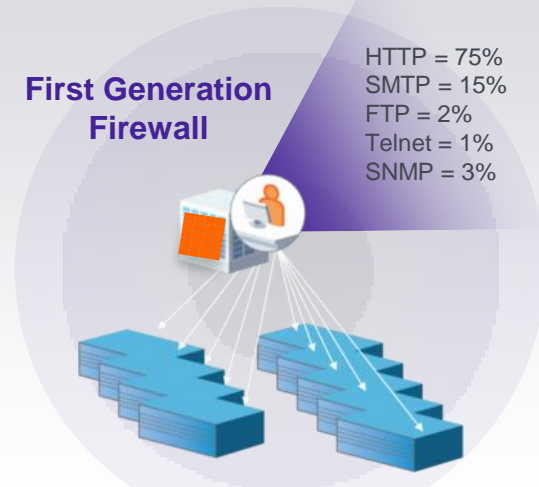# Application Visibility and Control
Identify, Analyze, and Optimize Application Traffic

BEFORE
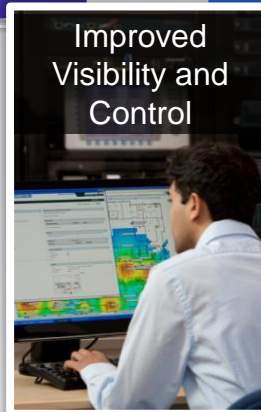Application View and ControL Based
On L4 Firewall Sessions

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

**First Generation
Firewall**

HTTP = 75%
SMTP = 15%
FTP = 2%
Telnet = 1%
SNMP = 3%

FW L4 Session Visibility and Control

Improved
Visibility and
Control

AFTER
Network Based Application Recognition –
NBAR2 Deep Packet Inspection and App ID

Wireless LAN Controller

Traffic

Real Time
Interactive
Non-Real Time
Background

NBAR2 LIBRARY
Deep Packet Inspection

POLICY
Packet Mark
and Drop

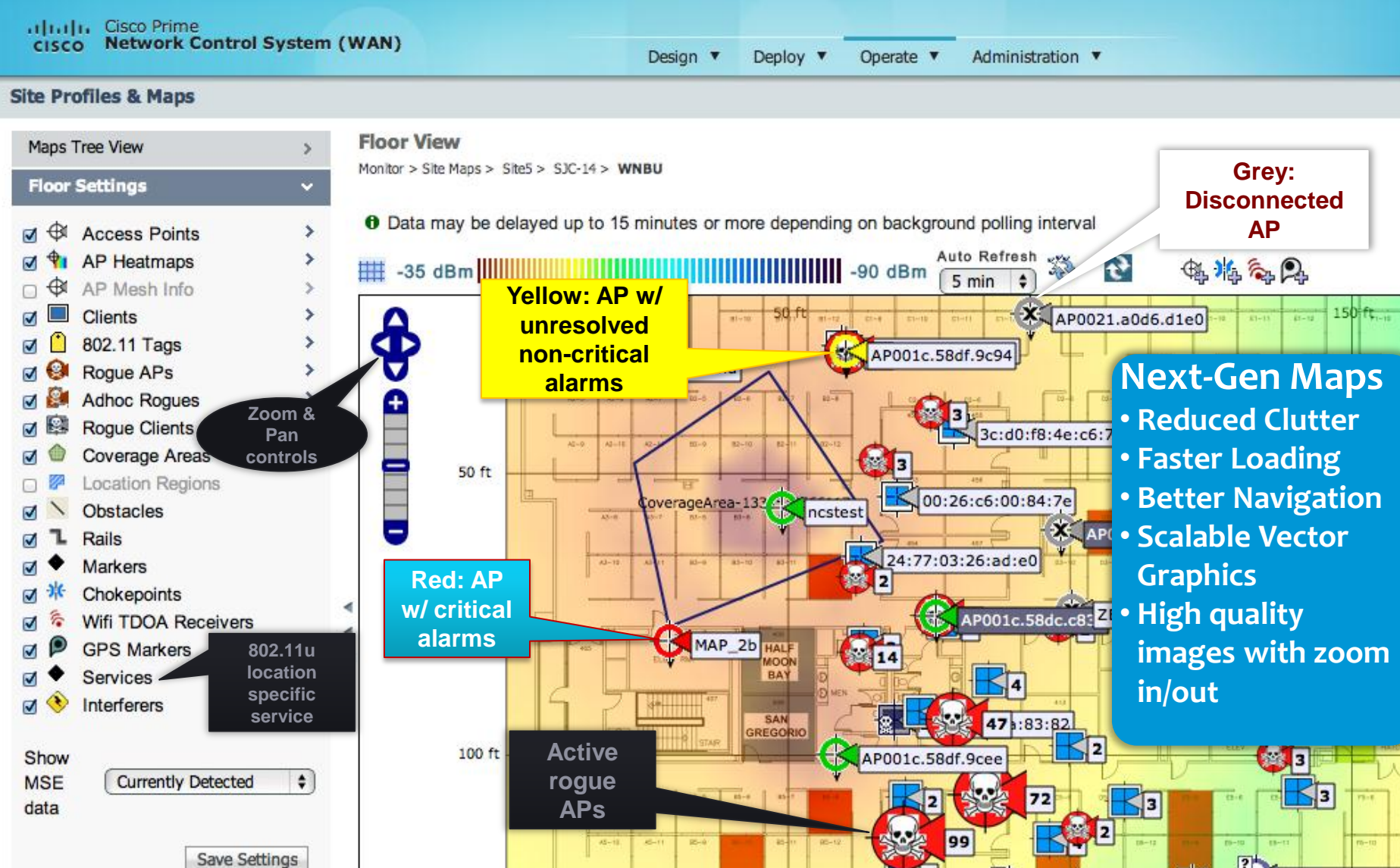| Inspect Packet	NetFlow Cache		
• Source IP address	Flow Information	Packets	Bytes/pack
• Destination IP address			
• Source port	Address, ports...	11000	1528
• Destination port	...		
• Layer 3 protocol			
• TOS byte (DSCP)			
• Input Interface			

NetFlow
Key Fields

2

Create a Flow from the Packet Attributes
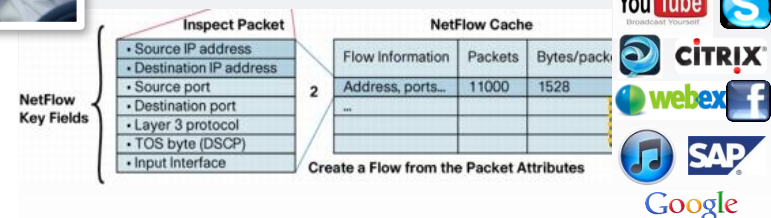
View, Control and
Troubleshoot – End User Application Experience

Cisco WLAN AVC and Prime Assurance Provides
Unparalleled Visibility and Control
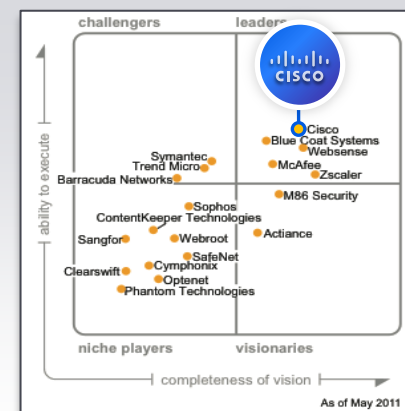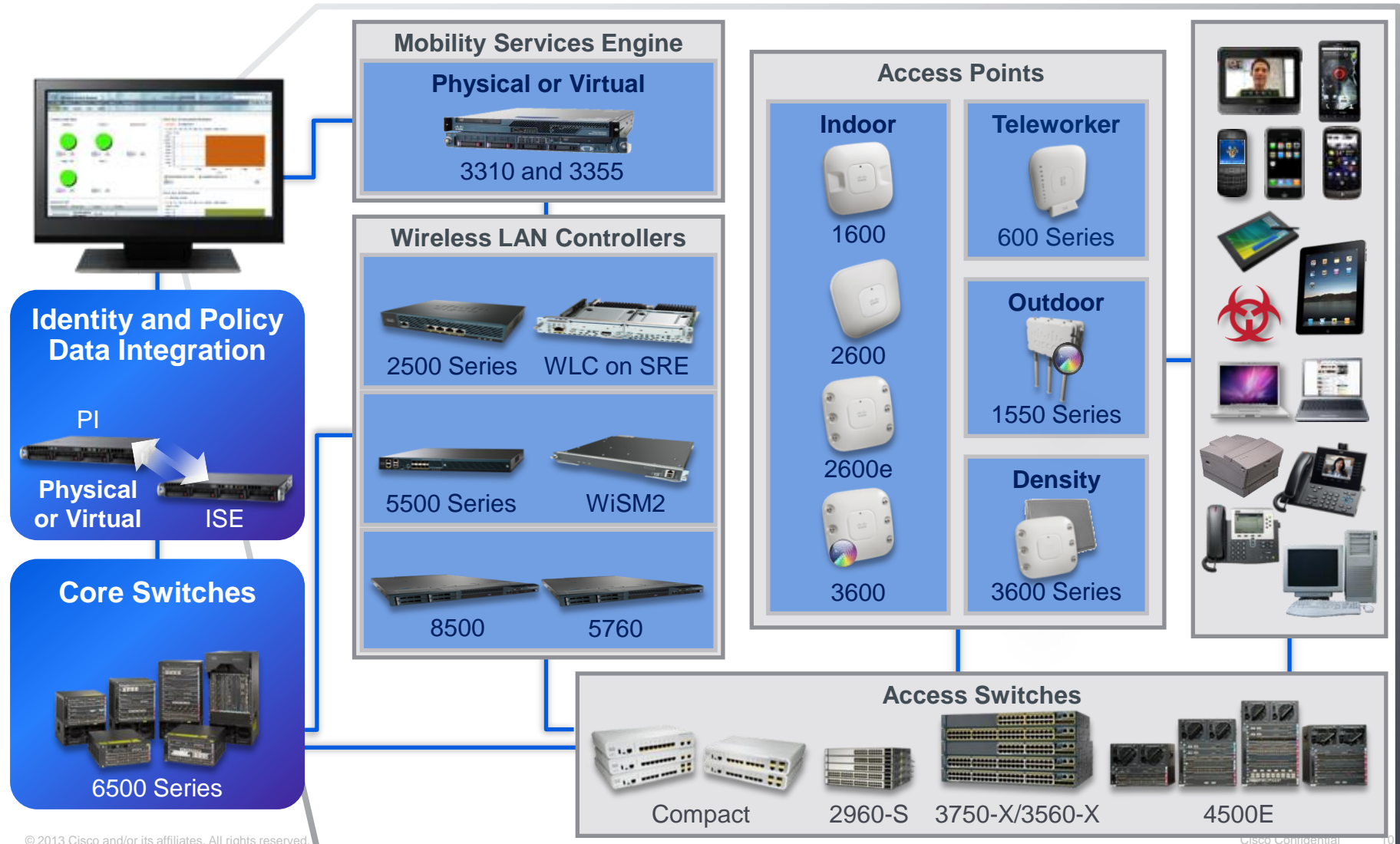
Automatically Generated Heat Maps

Gartner Leadership

Unified Access

Source: Gartner (June 2012)

Web Security

Key Takeaway –
One Policy, One Management, One Network

Identity and Policy Data Integration

PI

Physical or Virtual   ISE

Core Switches

6500 Series

Mobility Services Engine

Physical or Virtual

3310 and 3355

Wireless LAN Controllers

2500 Series   WLC on SRE

5500 Series   WiSM2

8500   5760

Access Points

Indoor

1600

2600

2600e

3600

Teleworker

600 Series

Outdoor

1550 Series

Density

3600 Series

Access Switches

Compact   2960-S   3750-X/3560-X   4500E

Thank you.

Cisco Networking Academy
Mind Wide Open