

TOMORROW starts here.



Cisco *live!*

Inside Cisco IT: Deploying Enterprise Network Technologies

BRKRST-2640

Ling Yang

Network Engineer

Enterprise Network



Bring Life to Work



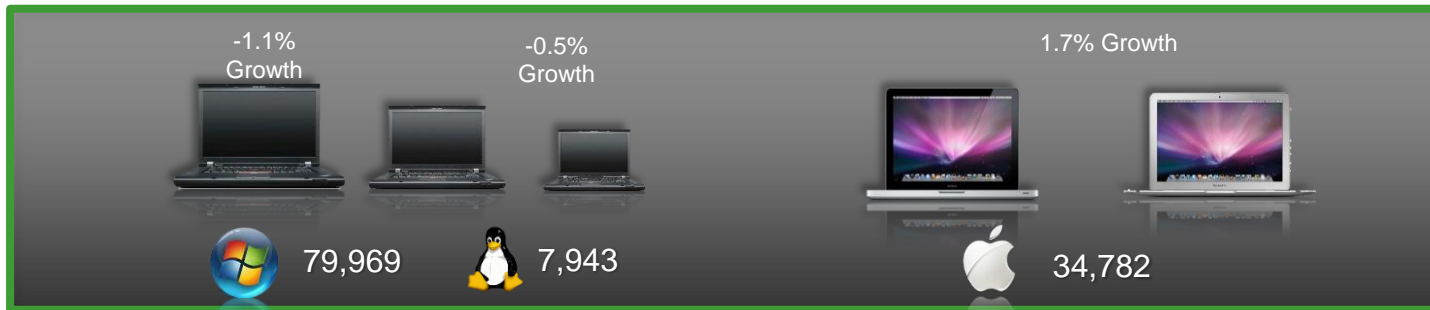
Agenda

- Enterprise Network Challenges & Opportunities
- Cisco IT Network Overview
- Cisco IT Unified Access Design
- Cisco IT Identity Service Engine (ISE) Design
- Cisco IT Cisco Prime Infrastructure Design



Enterprise Network Challenges & Capabilities

Cisco's Any Device Landscape (Dec 31, 2013)

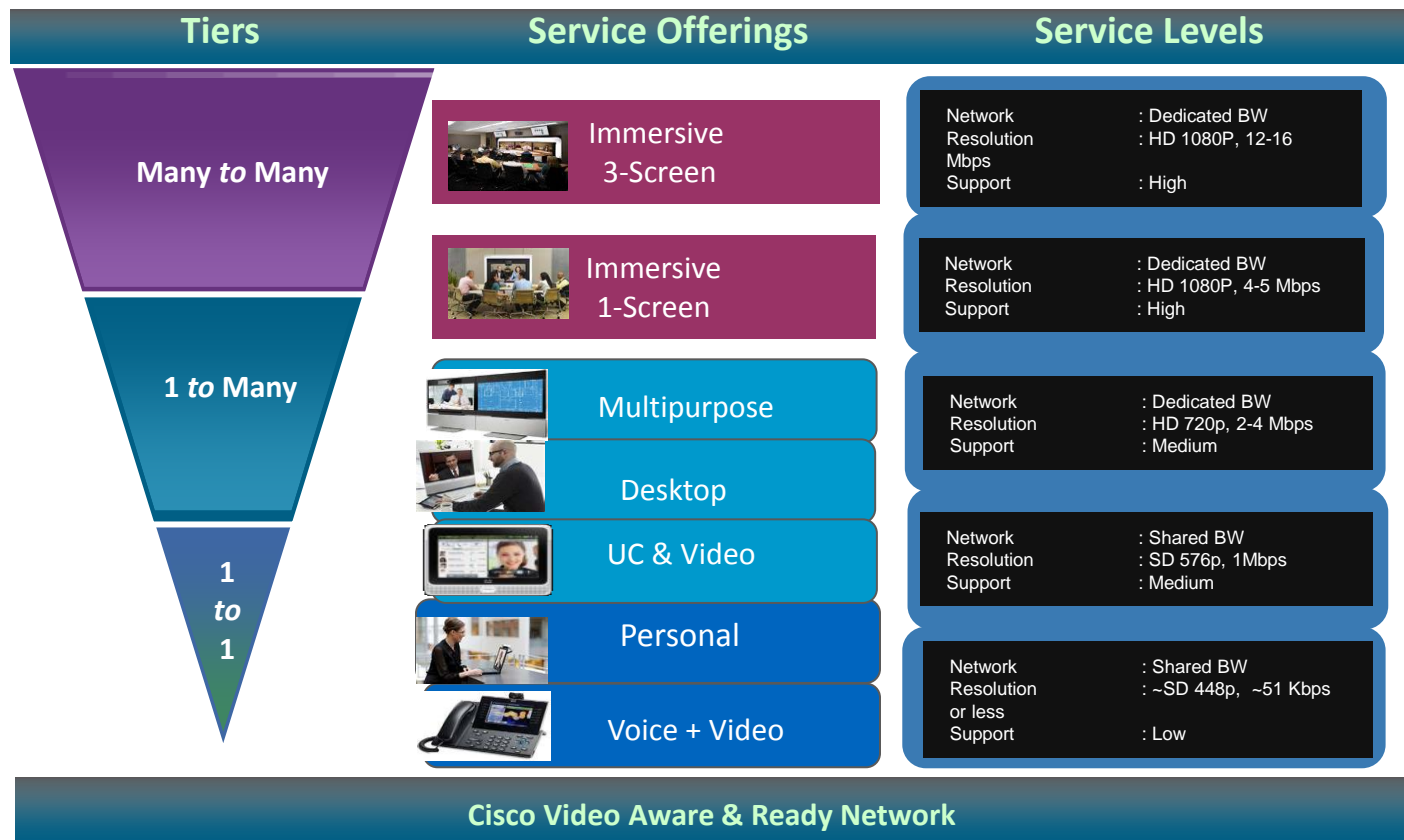


122,694
Corporate
Provided
Laptops
(CYOD)

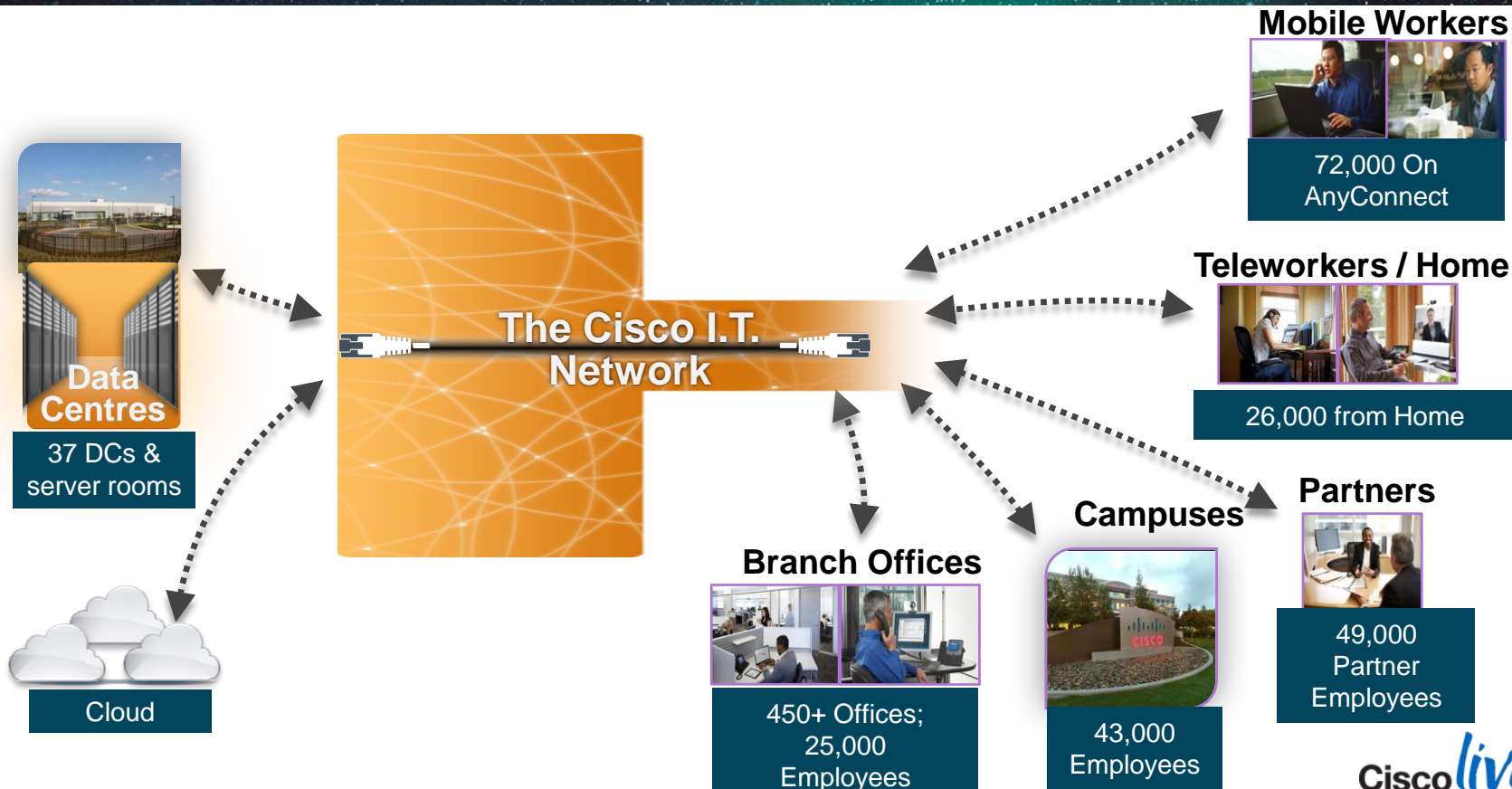


70,631
Personally
Owned
Mobile
Devices
(BYOD)

Explosive Use Of Video



Enable Seamless and Consistent User Experiences



Network Capabilities



Mobility/BYOD

Over 50,000 mobile devices access Cisco's wireless network today, an increase of 52% over the past 12 months.



Security

Understanding context to set policy that will mitigate future security risks.



Video

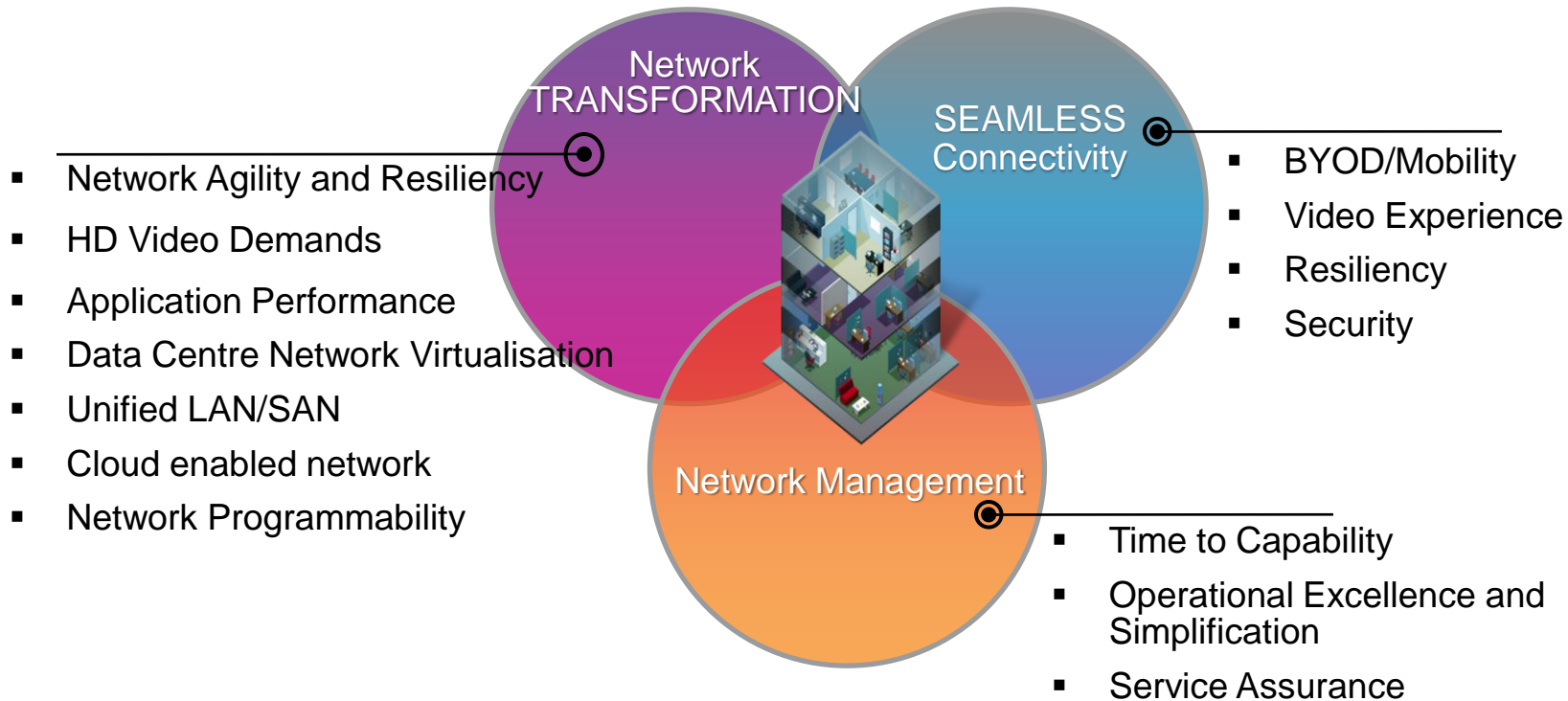
Personal HD video via Jabber, Tablets and Mobility will dramatically grow network traffic.



Network Mgmt

Simplified Network Management, opportunities for automation to lower TCO and improve user experience through Cisco ONE.

Core Competencies For Future Network



Extended Enterprise Network



Architecture for Agile Delivery of the Extended Enterprise Experience



Cisco IT Network Overview

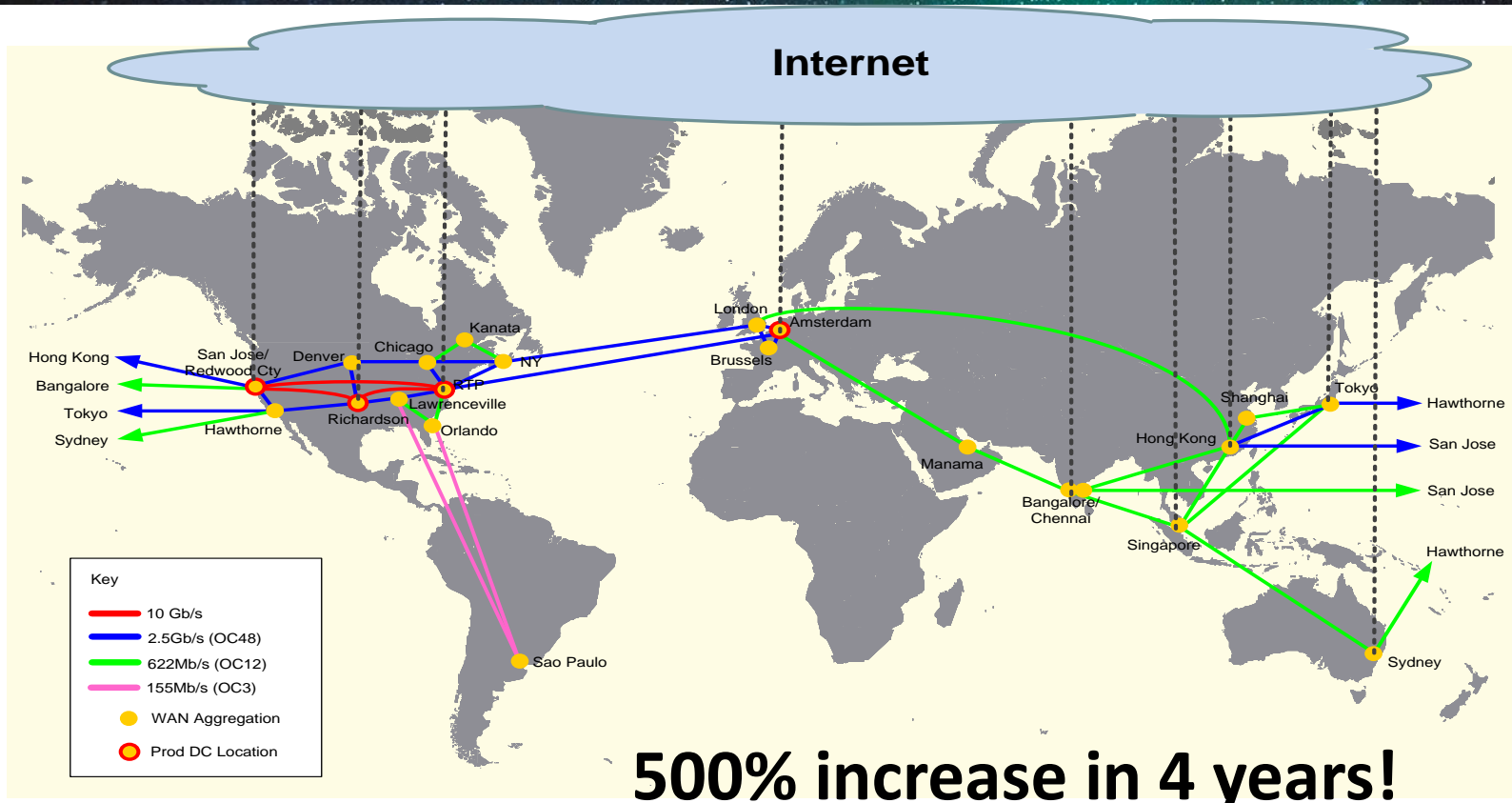
Cisco IT Network - Technology and People



More Than 180,000
People Worldwide in the
Extended Cisco Family

- 312 locations in 90 countries
- 450+ buildings
- 51 data centres and server rooms
- 1500+ labs worldwide (500+ in San Jose)
- 66,000+ employees
- 30,000 contractors
- 20,000 channel partners
- 110+ application service providers
- 210+ business and support development partners

Cisco IT Network - Backbone



Cisco Enterprise Router Portfolio

Core/Distribution Router

Catalyst 6500 Series - 1,700
Catalyst 4500-X Series – 50

Core/Distribution Router

Nexus 7000 Series - 20

5,345 + 27,000

Integrated Services Routers

2800 Series - 348
2900 Series - 524
3800 Series - 890
3900 Series - 1,265

Aggregation Services Routers

7200 Series – 111
ASR 1000 Series – 342

Integrated Services Routers (Home Office)

800 Series – 27,000

Cisco Enterprise Switching Portfolio

Fixed-Configuration Switches

Catalyst 4900 Series - 429
Catalyst 3850 Series - 4
Catalyst 3750-X Series - 1,303
Catalyst 3750 Series - 1,194
Catalyst IE3010 Series - 4

Modular Switches

Nexus 7000 Series
Catalyst 6500 Series - 1,650
Catalyst 4500 Series - 291

5,297

Fabric Extender

Nexus 2000 Series

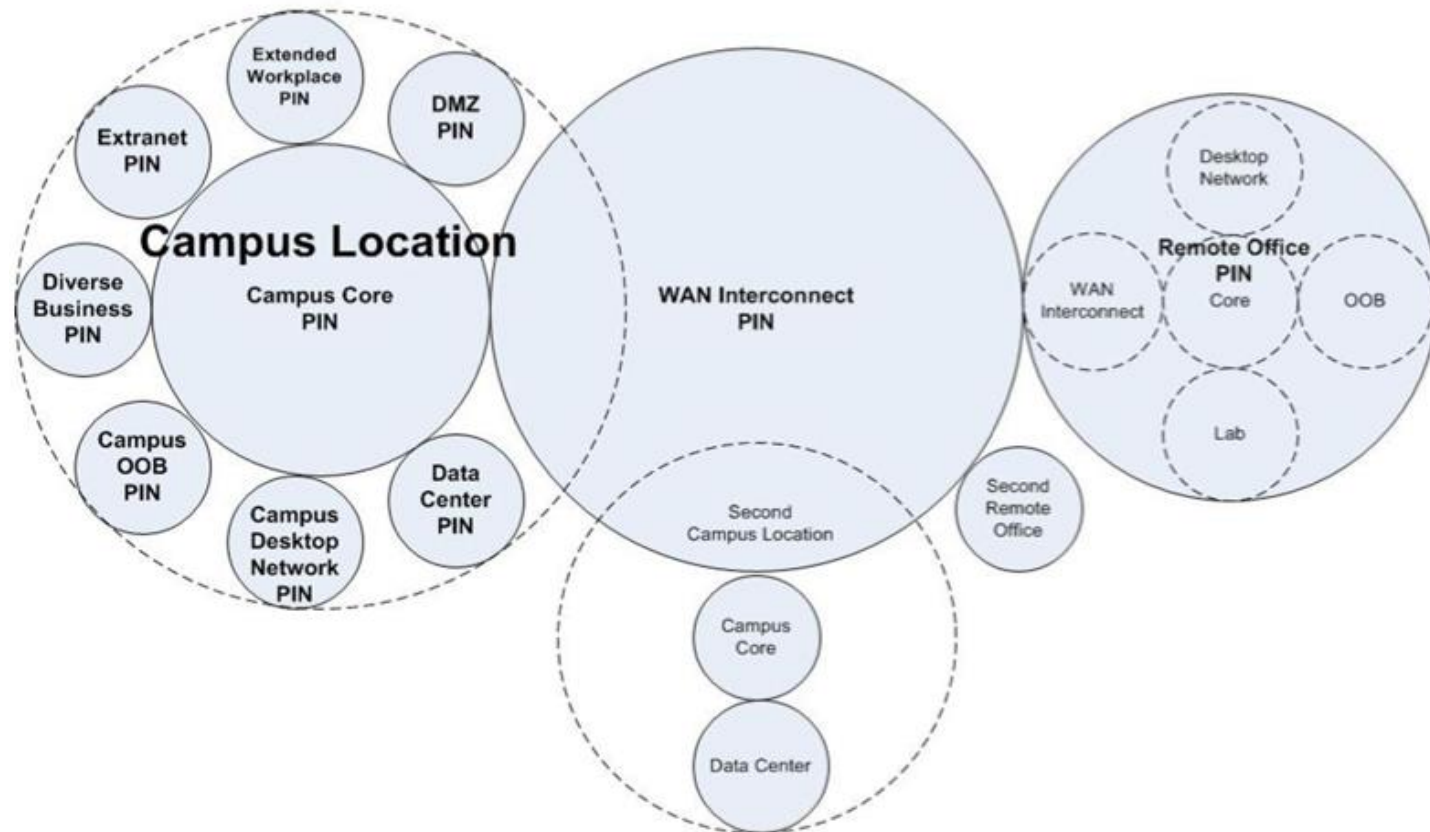
Blade Switches

Nexus 4000 Series

Virtual Switches

Nexus 1000V Series

Places in the Network (PINs)



Roadmaps, Certifications, Designs, Cookbooks

- **Roadmaps**

Track new hardware, software, and technologies and they generate HW, certifications, SW certifications and designs

- **Certifications**

Internal QA process to make sure that HW/SW and technologies work as advertised before adding to our global hardware and software standards

- **Designs**

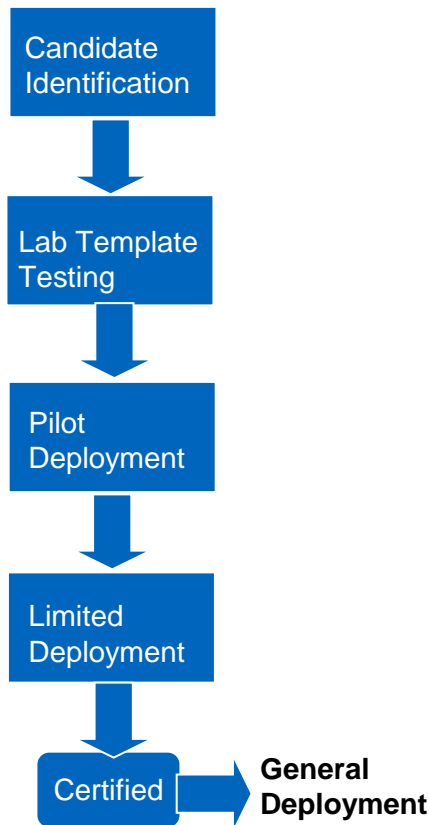
Technology specific designs such as EIGRP, QoS, and Multicast that are solution tested before global deployment

- **Cookbooks**

Culmination of the various technology designs, Global HW/SW standards, and implementation documentation necessary to deploy a solution in a PIN

HW/SW Certification Process

- **HW/SW Candidate Identification**
 - Roadmap Owners evaluate IOS business drivers
 - Request IOS Risk Analysis from AS
- **Lab Template Testing (1-2 weeks)**
 - SME test existing IOS features using templates
 - SME investigate and test “new” IOS features
- **SVL Pilot Deployment (2-4 weeks)**
 - Deploy new HW/SW in the SVL PIN topologies
 - Test impact on up/down stream devices, mgmt
- **Prod Limited Deployment (4-6 weeks)**
 - Identify low impact production sites or devices
 - Establish scope, success criteria, and SLA
- **General Deployment**
 - Deploy code to all production devices



Fleet Management

- Fleet Management is an ongoing Cisco IT program that manages a technology asset lifecycle to support operational health and infrastructure readiness
- Fleet is a technology enabler for applications and services
 - Visibility into network health and readiness
 - Drives the optimum infrastructure solution to enable the business
 - Indirect productivity enhancer
- Cisco Advanced Services for inventory tracking and compliance
- Cisco Remote Management Services for monitoring and software upgrades
- Cisco IT GIS Implementation resources for hardware upgrades



Cisco IT Unified Access Design

Unified Access

Supporting BYOD, Mobility, and HD video over wireless requires a new distributed architecture of switching the wireless traffic at the edge utilising a converged wired and wireless infrastructure providing uncompromised user experience on any workspace.



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

WIRED



Features:

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

Benefits

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

Converged Wired/Wireless – Components

One Policy - Identity Services Engine



ISE

One Management - Cisco Prime Infrastructure



Cisco Prime

Catalyst 3850



Catalyst 4500-E Sup 8E



5760 Wireless Controller



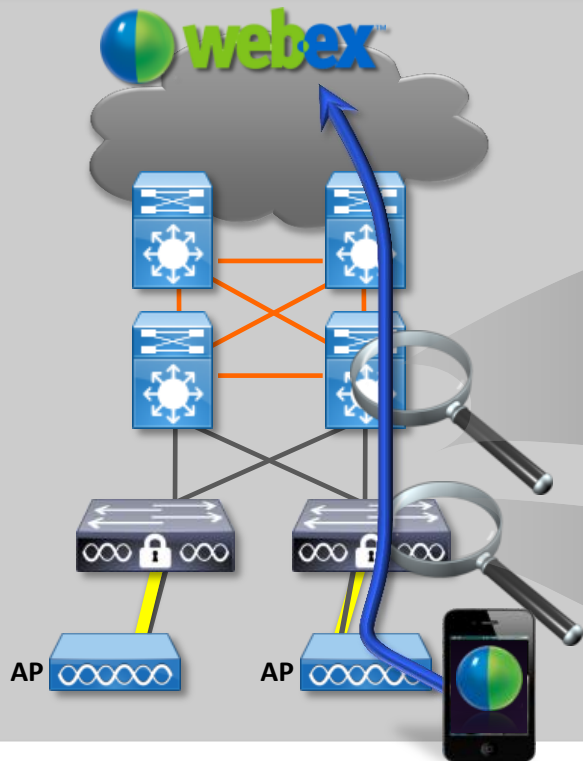
3850 (FCS Jan 2013)

Sup 8E (FCS July 2013)

5760 (FCS Jan 2013)

UA Benefit - Network Wide Visibility

Converged Access Deployment



Employee joins
webex call on
iPhone

Employee
iPhone
connected

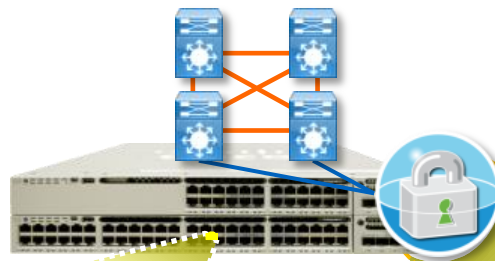
Benefits

- Track applications at every hop
- Root cause issues quickly

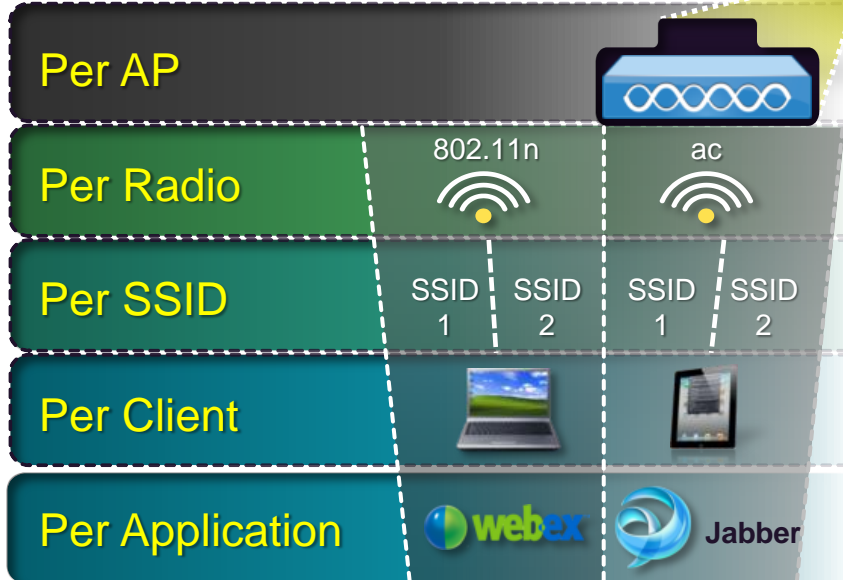
- **App level visibility**
 - Flexible Netflow
- **Media Troubleshooting**
 - Medianet

- **Device Identification**
 - Device Profiling

UA Benefit - Consistent Security and QoS Control



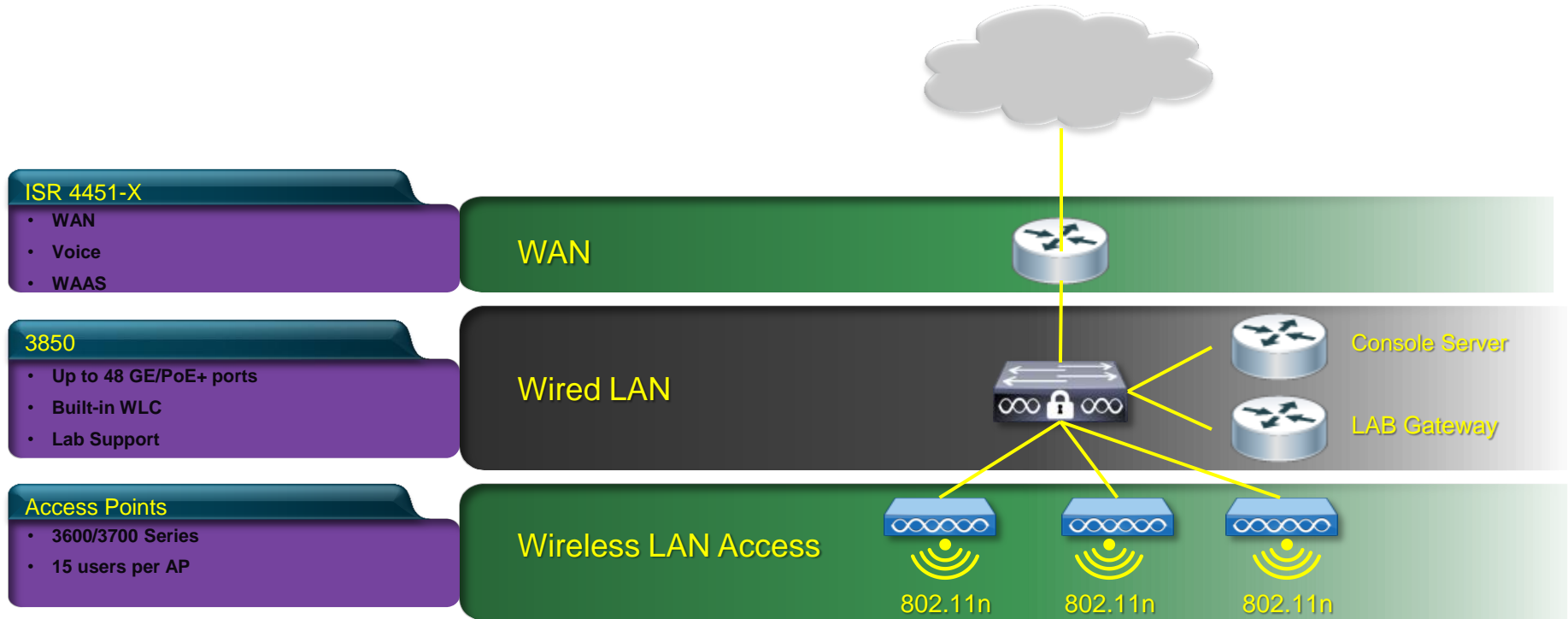
Hierarchical QoS



- Identity
- Device Profiling
- SGT/SGACL *SW Roadmap
- Control Plane Policing
- MACSec
- Port Security
- DHCP Snooping and IP Source Guard
- Wireless Intrusion Prevention System (WiPS)

Cisco IT UA Design

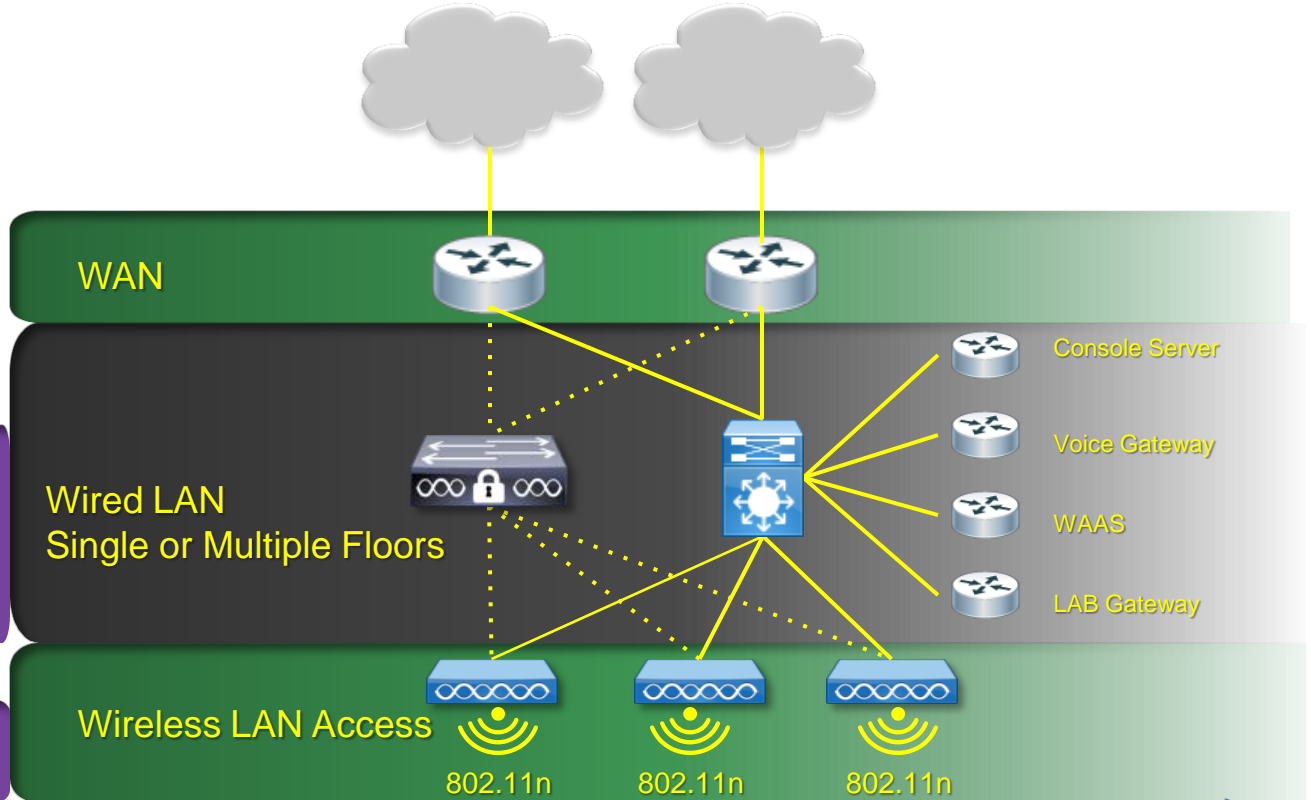
Small Office



Cisco IT UA Design

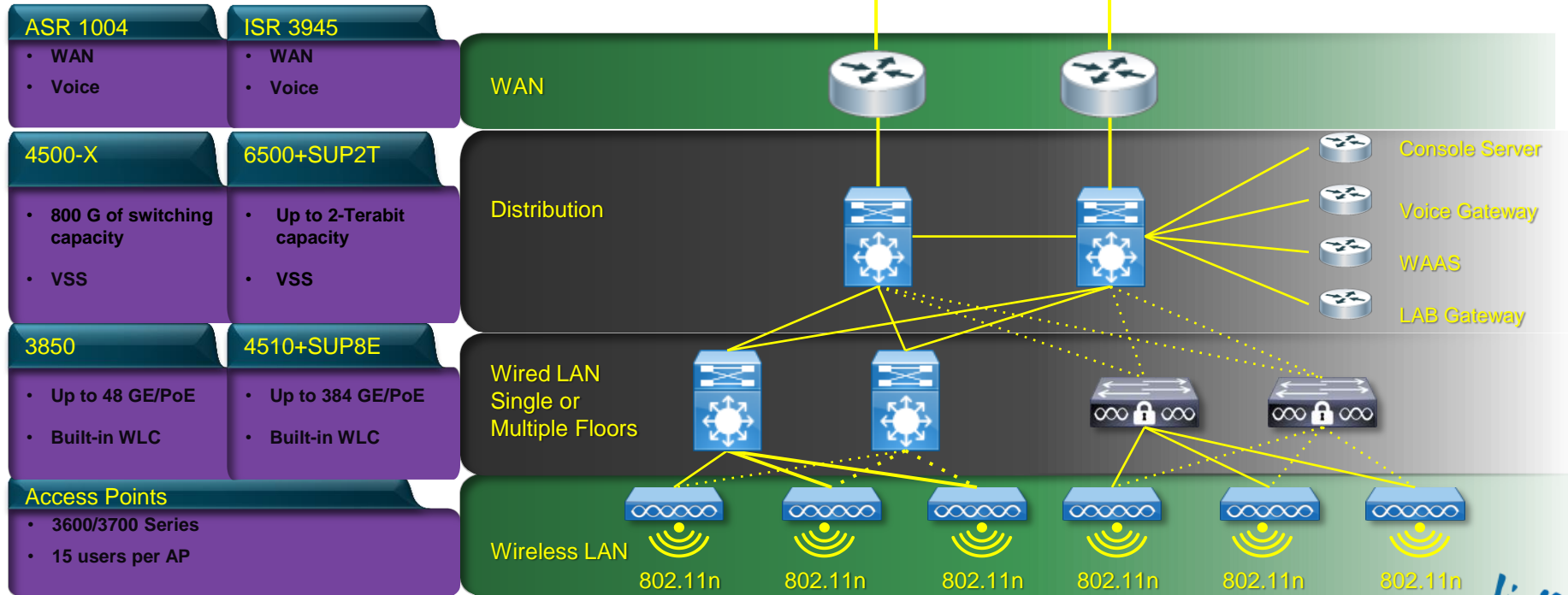
Medium Office

ASR1004 <ul style="list-style-type: none"> • WAN • Voice 	ISR3945 <ul style="list-style-type: none"> • WAN • Voice
3850 <ul style="list-style-type: none"> • Up to 48 GE/PoE • Built-in WLC 	4510+SUP8E <ul style="list-style-type: none"> • Up to 384 GE/PoE • Built-in WLC
Access Points <ul style="list-style-type: none"> • 3600/3700 Series • 15 users per AP 	



Cisco IT UA Design

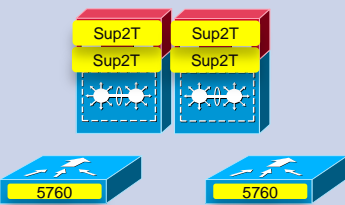
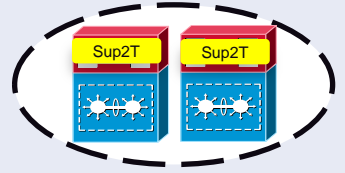

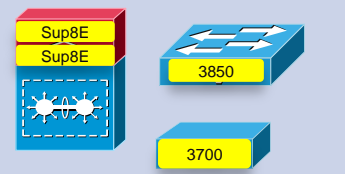
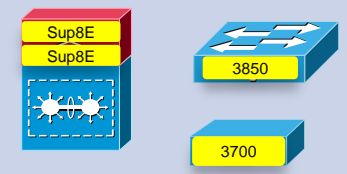
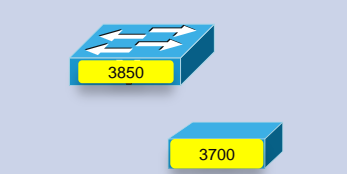
Large Office





Cisco IT UA Hardware Deployment Plan

Unified Access Hardware Deployment Plan

PIN	Platform	Campus	Branch Office	Small Branch Office
Core	Catalyst 6500/Sup2T (Quad VSS) CT5760 WLC			
Distribution	Catalyst 6500/Sup2T (Dual VSS) Catalyst 4500-X VSS			
Access	Catalyst 4500/Sup8E (Dual Sup) Catalyst 3850 3700 Series APs			

Unified Access Hardware Deployment Status

- 3850 - deployed 10 locations
- 5760 - deployed in 1 location
- Sup8E - first deployment scheduled for January 2014

Unified Access – Challenges and Lessons Learned

Challenges

- HW/SW Feature parity - UPOE, Energywise, Medianet
- Max stack of 4 3850s at FCS

Lessons

- Cisco Prime Infrastructure - wired and wireless management issues
- TrustSec – Device Sensor for device profiling, Secure Group Tagging, MACSec



Cisco IT Identity Service Engine (ISE) Deployment

Cisco TrustSec Architecture Overview

Overlay/Appliance Mode

or

Infrastructure Integrated Mode



802.1X, Web Authentication, MAC Authentication Bypass, Guestnet, Device Profiling



VLAN, dACL, Security Group Access, Identity Firewall



MACSec (802.1AE)

Cisco IT will Deliver Multiple Capabilities with ISE



ION

Restrict
unauthorised
devices & users
to Internet
access only



Profiling
Ability to
identify **users**
and **devices** on
our network



**Endpoint
Protection**
Protect the
network from
infected
devices



**Access Control
Authentication**
on wired &
wireless
networks



BYOD
Support *Trusted
Device*
Standard and
enable BYOD

Trusted Device Standard

Architectural Principles

Device security posture assurance

User authentication and authorisation

Secure storage of corporate data at rest



Execution Elements

Core Requirements

PIN or Password

10 Minute Auto Lock

Remote and Local Wipe

Encryption

Anti-Malware

Minimum OS Version

Device Registration

Hardware/Software Inventory

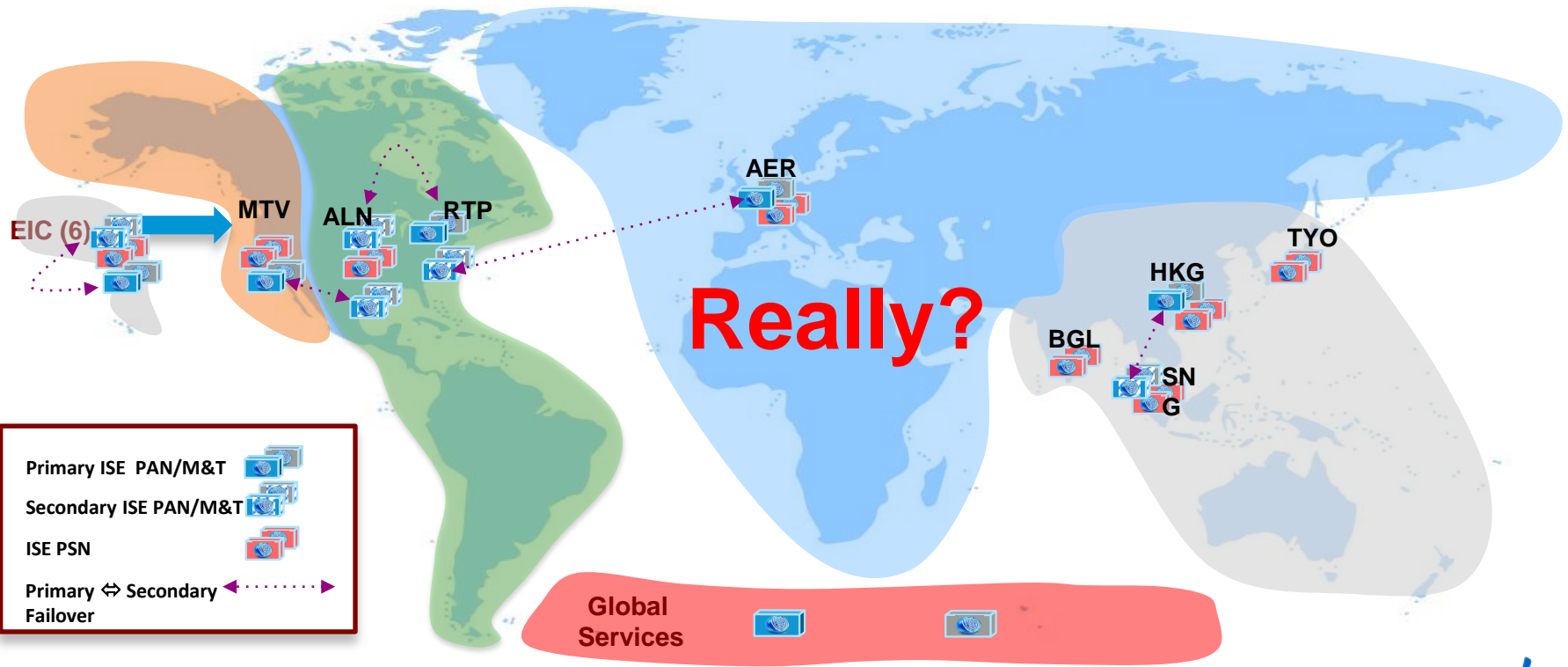
Cisco IT Trustsec Deployment Strategy

- **Avoid the “Big Bang”**
 - Too many new capabilities to enable in a single deployment.
- **“ISE Deployment Bundle” model**
 - Capabilities have been grouped into bundles to enable targeted & manageable deployments
- **Single Global ISE Cluster (“ISE Cubes”)**
- **Global Infrastructure Foundation**
 - Deploy global VM infrastructure and ISE servers first
 - Enable features (based on “ISE Deployment Bundles”)
 - ION enabled and deployed globally

What Services are IT Delivering with ISE?

What	Why	Where	When
Internet Only Networking (ION)	<ul style="list-style-type: none"> Policy based differentiated network access Basis for future network security 	All sites globally.	December 2013
Profiling	<ul style="list-style-type: none"> Device profiling Visibility into endpoint demographics 	All sites globally.	Q3FY14 Q3FY14
802.1X Monitor Mode	<ul style="list-style-type: none"> User attribution Reduce user impact of future Auth Mode 	All sites globally.	Q3FY14 Q3FY14
802.1X Auth Mode	<ul style="list-style-type: none"> Access layer security Improve security in Extranet, labs, ICZ's etc 	50% of ICZ (China) Publicly accessible ports TAC locations (lab access) CVO (29,000 routers)	Q3FY14 Q3FY14 Q3FY14 Q4FY14
CVO	<ul style="list-style-type: none"> Secure tunnel authentication 	All 29,000 CVO routers	Q4FY14
Endpoint Protection Services	<ul style="list-style-type: none"> Quarantine infected/compromised devices 	Limited deployment in ICZ	Q4FY14

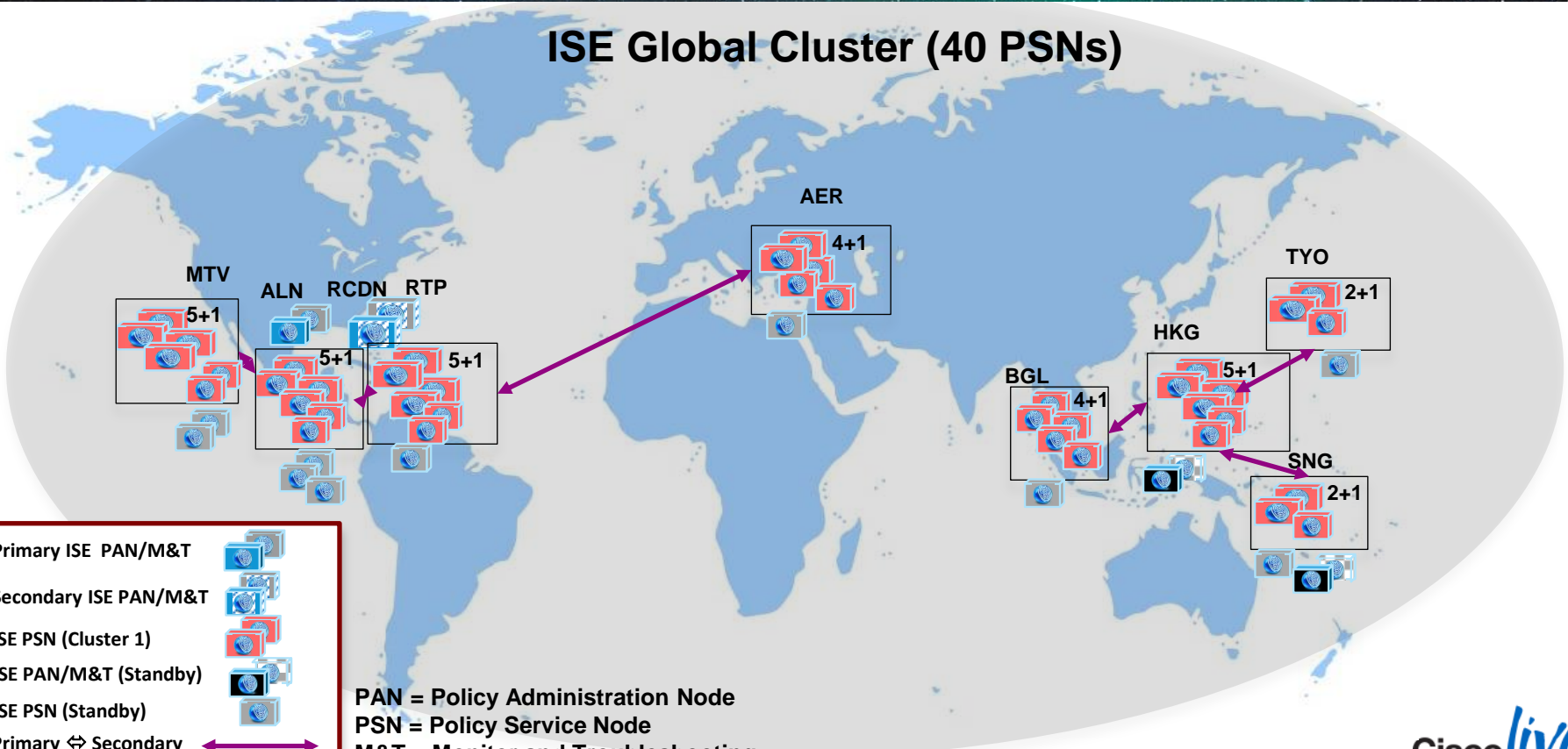
Original Multiple ISE Cubes



Really?

Single Global ISE Cluster

ISE Global Cluster (40 PSNs)



Primary ISE PAN/M&T

Secondary ISE PAN/M&T

ISE PSN (Cluster 1)

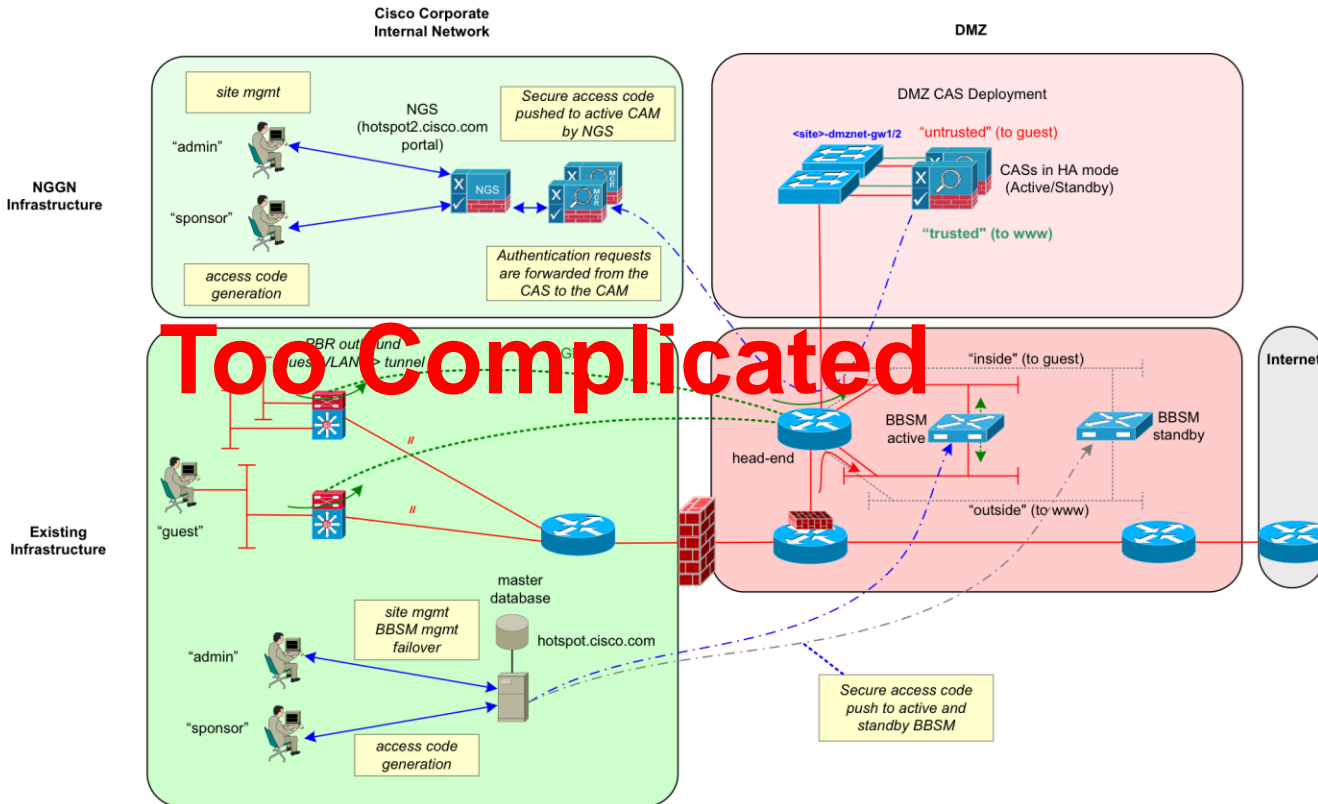
ISE PAN/M&T (Standby)

ISE PSN (Standby)

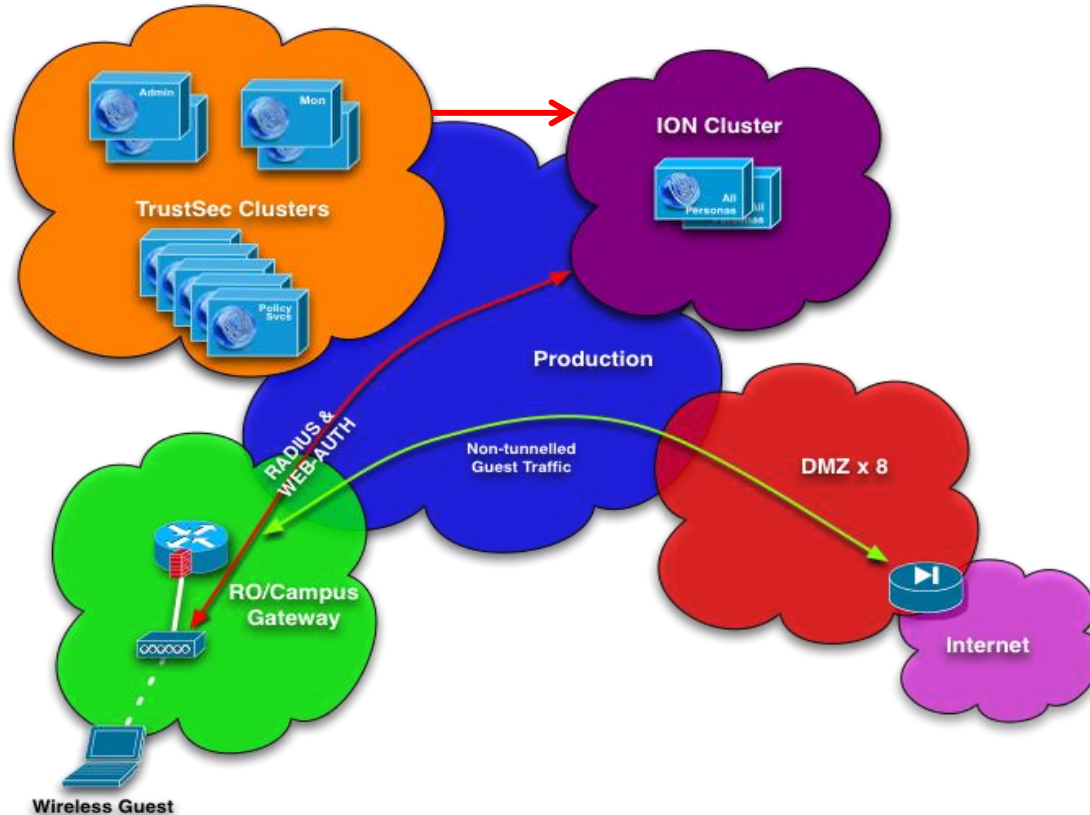
Primary ↔ Secondary Failover

PAN = Policy Administration Node
 PSN = Policy Service Node
 M&T = Monitor and Troubleshooting

ION (Internet Only Networking)



ION (Internet Only Networking) Current



ISE 1.2 Deployment Status

- Deployed in all four regions (US West, US East, EMEAR, and APJC)
 - ION (Internet Only Networking) active globally
 - Profiling active in 43 sites
 - 802.1x Monitor Mode active in 15 sites.
 - 53 live ISE servers.
 - Migrated wireless authentication from ACS to ISE

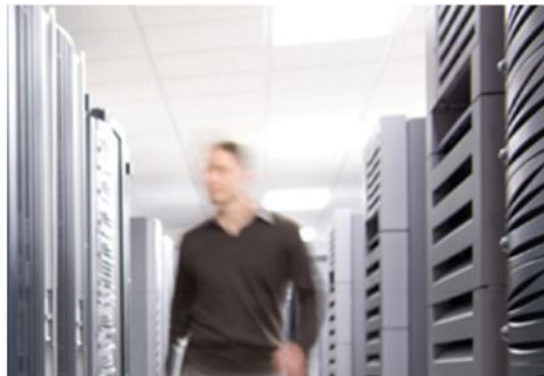
ISE – Challenges and Lessons Learned

Challenges

- Infrastructure readiness
- ISE scalability

Lessons

- Virtualisation
- Profiling policies
- Logs analysis

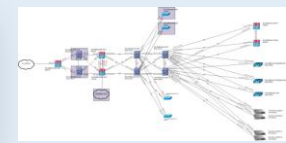
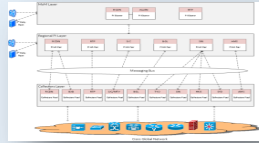


Cisco IT Cisco Prime Infrastructure Deployment

Cisco Prime Infrastructure

The foundation of network management of IT

Network Devices: 450,000+
Applications: 4000+
End Points: 300,000+
Wireless Clients: 120,000+



Managed Elements

NGWC, ACEM, ASA, AXG, AiroNet_AP, CSS, CacheEngine, CVO, GSS, GateKeeper, IOSD, Switch (Cat 2k, 3k, 4k, 6k series), Nexus, MDS, ONS, PIX, Gateway, Router (ISR, ASR, ESR), VSG, WAAS, WLC etc

Management Tools in Use

- Cisco Prime Infra (CPI), to manage global wireless network.
- Cisco IT internal + 3rd party tools, to manage global wired network.

NM Target Capabilities

- Network config & change Management
- WAN Traffic Analysis (Netflow, NBAR)
- Network Performance Mgmt (AVC, PFR)
- Software Image Management
- Compliance Management
- End User Experience (IPSLA)
- Unified Access Wired and Wireless
- Event Correlation & Runbook Automation
- Device Lifecycle Mgmt
- Configuration Optimisation
- Capacity Management (usage trending)
- Network Security Management
- Access Control Management
- Zero Touch deployment

Cisco IT Transition to Prime Infra...

- One tool to manage wired and wireless devices
- Configuration management
- Device 360 provides a unified view for device troubleshooting
- Multi-NAM management and device fault & performance management
- Application visibility, capacity planning, simulation and service assurance
- Unified Collector & MoM on highly available & distributed Cluster Architecture

Cisco Prime Infrastructure - Value Propositions

Prime Infrastructure is one of the major building blocks of the Domain management of Cisco IT Service management.

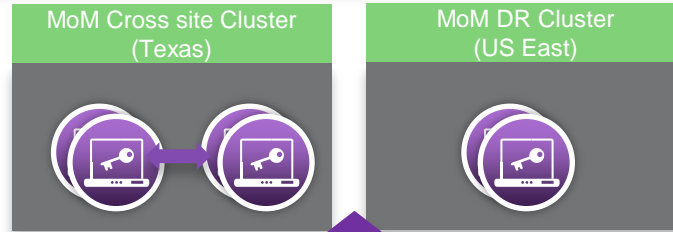
- ✓ Cisco IT is **reducing** and redirecting the in-house development to customer repeatable model.
- ✓ Reduce the **implementation**, service activation and operational cost.
- ✓ **Single-pane of glass** enhancing the user experience with standard user interface.
- ✓ **Reduce mean time to recovery** with network analytics.
- ✓ Simplify the Network Management and reduce the **TCO**.

Cisco Prime Infrastructure:

Tiered cluster architecture and collector

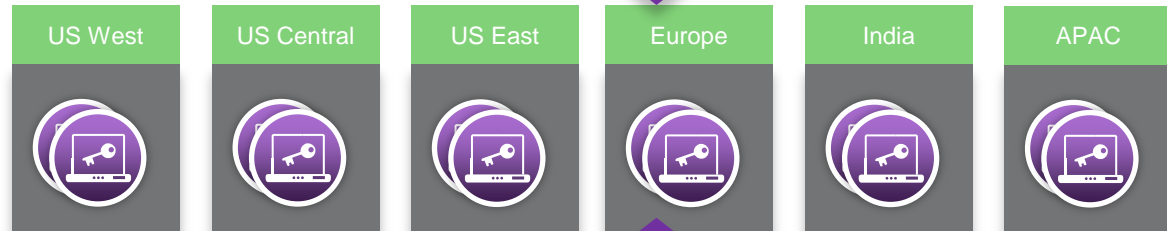
MoM Layer

- Single Pane of glass
- Configuration/Policy repository
- Built for HA (Cross site cluster + DR site)

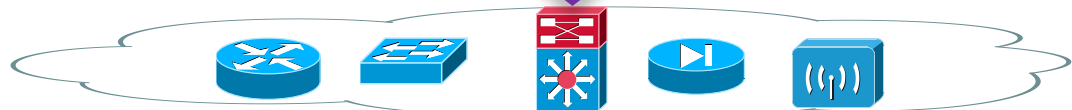


Regional CPI Deployment

- Configuration Change Mgmt
- Service Assurance



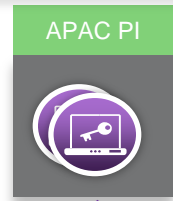
Network Infrastructure



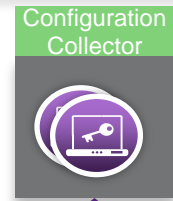
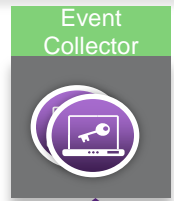
Cisco Prime Infrastructure

The collector layer

Regional Deployment



ANZ Collectors



Traps, Syslog, Netflow

SNMP Poll, ICMP
Discovery Agent

Configure/Image
Polling Pushing

Network Infrastructure

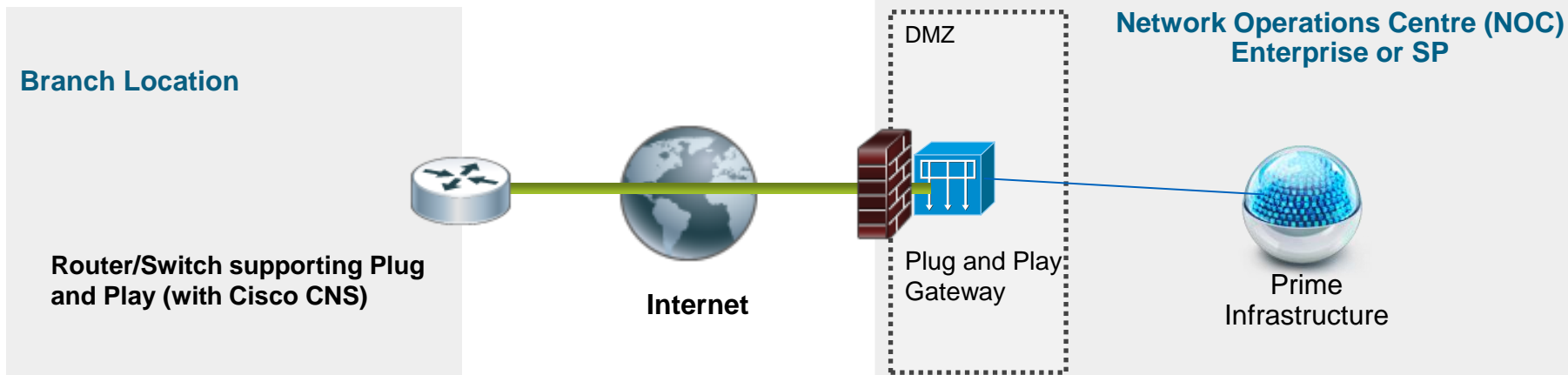


The Core of Cisco IT as a Service Organisation

This architecture not only allows the transition from the old state to the new one, but introduces new capabilities to our NM, essential for Cisco IT as a service organisation:

- ✓ Network Assurance
- ✓ ZTD
- ✓ Compatibility management
- ✓ Resiliency management
- ✓ Event correlation

Zero Touch Deployment (ZTD)



- 1) Plug and Play Gateway in a DMZ (w/ PI 1.3): devices connect to over the Internet without exposing Prime Infrastructure
- 2) Plug and Play Gateway integrated into Prime Infrastructure (w/ release PI 2.0)

PI 2.0 Deployment Status

- Upgraded Six PI 2.0 Network Management Stations
 - Regionally divided – US West/Central/East,
 - APAC and Europe
 - Deployed on UCS Virtual Machines with SAN storage
 - MSE's backup to NCS
- 6 PnP Gateway Servers
- Zero-Touch Deployment (Initial Pilot)
 - Day0 (bootstrap config)
 - Day1 (basic features)
 - Day2 (complete configuration)

Cisco Prime Infrastructure

Challenges and Lessons Learned

Challenges

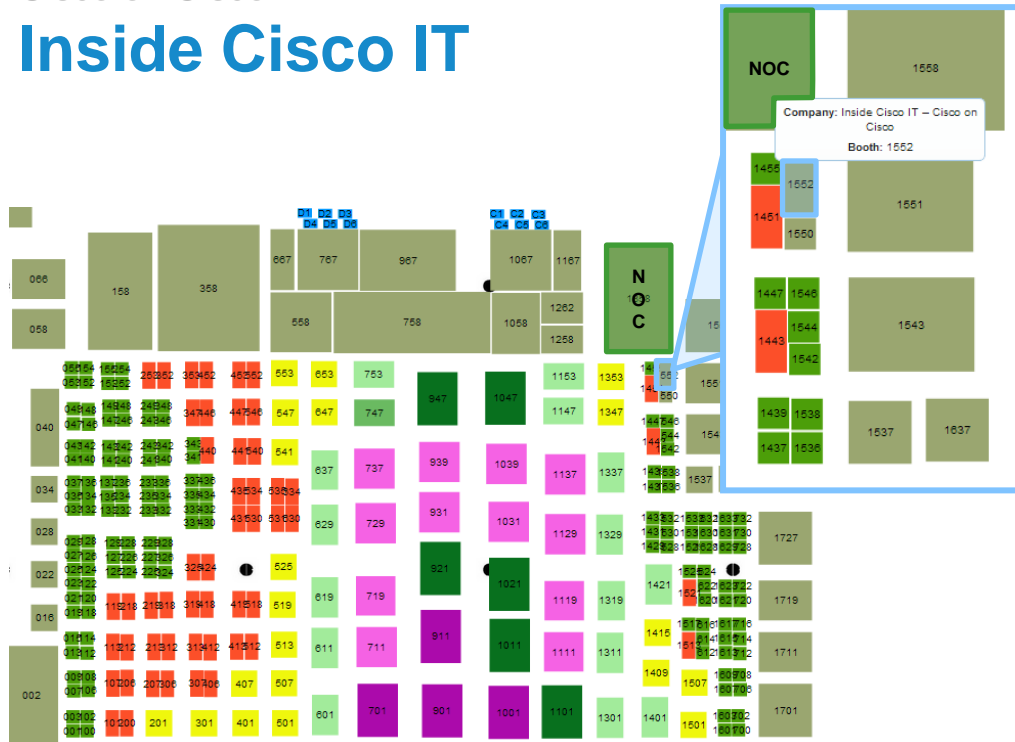
- Scalability

Lessons

- In-place Upgrade
- ZTD Templates Development

Cisco on Cisco

Inside Cisco IT



Visit our booth to speak to Cisco's own IT team, opposite the Networks Operation Centre.

Experts will be available to talk about the following:

- Bring Your Own Device (BYOD)
- Collaboration
- Unified Communications
- Video
- Network Ops & Management
- Cloud, SDN & DC Solutions
- IPv6
- Security

 <http://www.twitter.com/ciscoit>

 <http://www.facebook.com/ciscoit>

 <http://www.youtube.com/cisco>

 <http://www.cisco.com/go/ciscoit>

 <http://blogs.cisco.com/ciscoit>

Cisco *live!*



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO™