Follow us on Twitter at *#CiscoConnect_TO*
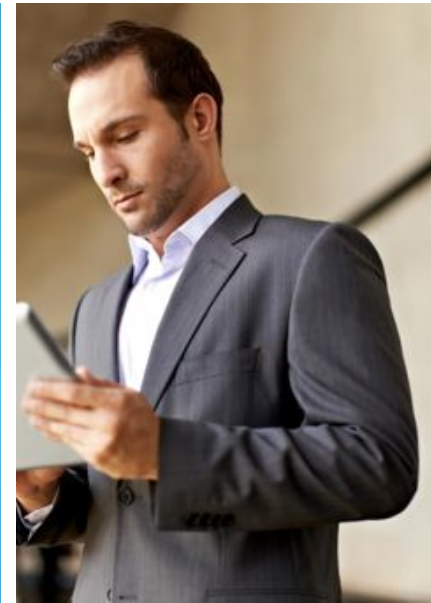
Cisco Connect

Toronto, Canada
May 30, 2013

Innovations In Switching

Borderless Networks – Intermediate Level

David Jirku – Technical Solutions Architect
djirku@cisco.com

PEARSON

CISCO

CISCO CERTIFIED CCIE 10 YEARS

intel

"Come to this session to learn about Cisco's latest innovations in Ethernet switching. Covering Cisco's major Catalyst switching platforms, this session will provide you with an overview of Cisco's latest advancements in switching, and how these capabilities can be applied to solve problems in your network environments. Attendees at this session will learn how they can move their networks, and organizations, forward by leveraging the newest advancements in Cisco's switching portfolio. This session is targeted to Network Managers, Architects, and Administrators.

Session Abstract

Cisco Innovation Strategy

From Pioneering Pre-Standard Innovations to Driving Industry Standards

Cisco Innovations

On Average, Cisco innovations are 3-5 *YEARS* ahead of standards

Integration into ASIC and Hardware/ Software takes an additional 18 – 24 months

Resulting Standards

Cisco is committed to Innovation and bringing Cutting-Edge Standards-based Technologies to Market

Investing in Innovation & Canada

- 3rd in total revenue for all Cisco global sales operations; 21th in global GDP
- Approximately 1,400 employees nationwide
- Approximately half of Cisco Canadian staff committed to R&D

- Canada's primary R&D centre located in Kanata, ON
  - ➢ 400 employees develop some of Cisco's most innovative technologies
  - ➢ Cisco R&D investment in Kanata facility is approximately $100M annually
  - ➢ $25 Million committed by the Ontario Government over three to create 300 jobs in R&D
  - ➢ Total Cisco investment : $455 million over 5 years

- Scientific Atlanta R&D operations in Vancouver and Toronto – 200 employees

you + networks = impact^{x}

ENTERPRISE THE NETWORK MEGATRENDS

IMMERSIVE COLLABORATION

Pervasive Video

MOBILITY BYOD

CLOUD
SaaS | DC/V

Google

Linked **in**

facebook

Cisco webex

salesforce.com
Success On Demand™

Security
Accelerating Cyber Threats

Cost Control
TCO, Operational Efficiency
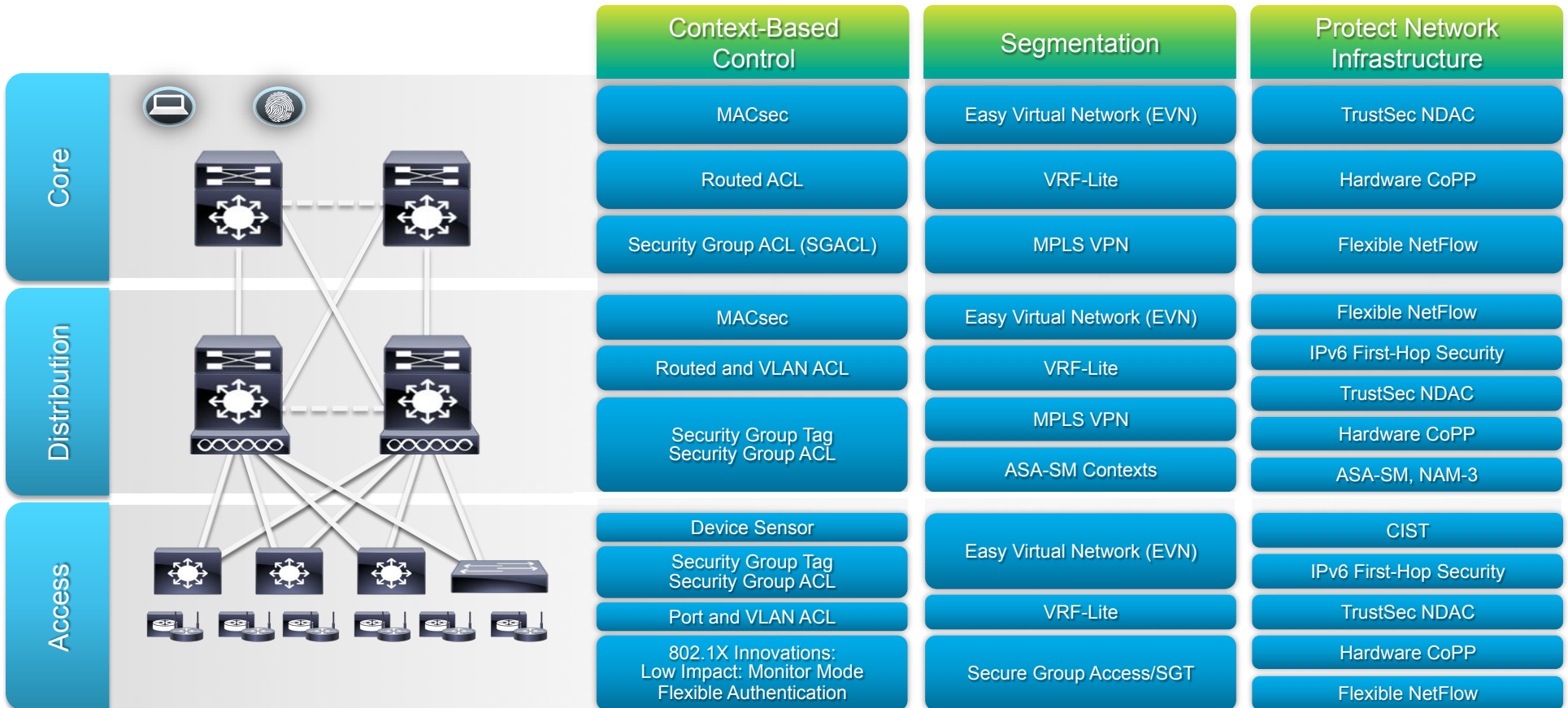
IT Effectiveness
Service and Network Management

Securing the Campus Infrastructure
Where to Apply Security Policies

	Context-Based Control	Segmentation	Protect Network Infrastructure
Core	MACsec	Easy Virtual Network (EVN)	TrustSec NDAC
	Routed ACL	VRF-Lite	Hardware CoPP
	Security Group ACL (SGACL)	MPLS VPN	Flexible NetFlow
Distribution	MACsec	Easy Virtual Network (EVN)	Flexible NetFlow
	Routed and VLAN ACL	VRF-Lite	IPv6 First-Hop Security
	Security Group Tag Security Group ACL	MPLS VPN	TrustSec NDAC
		ASA-SM Contexts	Hardware CoPP
			ASA-SM, NAM-3
Access	Device Sensor	Easy Virtual Network (EVN)	CIST
	Security Group Tag Security Group ACL		IPv6 First-Hop Security
	Port and VLAN ACL	VRF-Lite	TrustSec NDAC
	802.1X Innovations: Low Impact: Monitor Mode Flexible Authentication	Secure Group Access/SGT	Hardware CoPP
			Flexible NetFlow

Cost Control: Operational Efficiency
Where to Application Visibility and Control Features

	Assessment	App Visibility and Control	Monitoring / Troubleshooting
Core	Enhanced Object Tracking	Flexible NetFlow	Performance Monitor
	IP SLA	Microflow Policing	Mediatrace
		QoS	Mini-Protocol Analyzer
Distribution	Enhanced Object Tracking	Flexible NetFlow	Performance Monitor
	IP SLA	Microflow Policing	Mediatrace
		AVC in WiSM-2	Mini-Protocol Analyzer
		QoS	NAM-3
			SPAN / RSPAN / ERSPAN
Access	Clean Air	Flexible NetFlow	Performance Monitor
	Built-in Traffic Simulator	Media Service Proxy	Mediatrace
		Device Sensor	Wireshark
		Wireless Controller AVC	Device Sensor
			SPAN / RSPAN / ERSPAN

IT Effectiveness: Service & Network Management
Where to Deploy Smart Operations Features

	Deploying	Monitoring	Troubleshooting
Core	Smart Install	Performance Monitor	Mediatrace
	AutoQoS	Flexible NetFlow	Mini-Protocol Analyzer
	EEM	IP SLA	GOLD
	Medianet 2.2	EEM	EEM
			TDR
Distribution	Smart Install	Performance Monitor	Mediatrace
	AutoQoS	Flexible NetFlow	Mini-Protocol Analyzer
	EEM	IP SLA	GOLD
	Medianet 2.2	EEM	EEM
			TDR
Access	Smart Install	Performance Monitor	Mediatrace
	Auto Smart Ports	Flexible NetFlow	Wireshark
	AutoQoS	Clean Air	Smart Call Home
	EEM	EEM	EEM
	Client Link		On-Board Failure Logging

But… We Only Have 90 Minutes!

Focusing on 3 areas during this session to address all 3 of the networking drivers discussed previously.

Innovation comes in multiple forms:

- Features
- Technologies
- Architectures

Operational Efficiency to Address TCO

IT Effectiveness

Converged Access

Agenda

Operational Efficiency: EnergyWise

IT Effectiveness: Network Automation

Converged Access

Regulatory Pressures

Canada Energy Efficiency Act – external power supplies, battery chargers, TV set top boxes, and digital TV adapters

EU EuP Directive – energy using products, including set top boxes; Data Center Code of Coduct

Japan –networking equipment

China –TV receivers, set top boxes, and DVD players

US Energy Policy Act of 2005 – battery chargers and external power supplies; EnergyStar for Servers, Storage, UPS, and Data Centers

Australia – DVD players and recorders, hard disk recorders, AV receivers, other audio / video equipment

Mexico evaluating efficiency standards for electronic products

US HR 3221 – external power supplies, promote energy efficient data centers.
HR 6 – energy efficiency labeling for set top boxes and DVR products.

Energy Usage

Transportation 25%

Buildings 25%

Total Energy Consumption

Manufacturing 50%

Lighting 11%

IT Equipment 25%

Enterprise Buildings

Other 6%

Heating, Cooling, and Ventilation 58%

Consumer Communications 6.1%

Handheld Devices 0.5%

Wireless Infrastructure 7.3%

PCs, Laptops & Monitors 31.5%

Wired Telecom 11.1%

Enterprise/ SMB Comm. 13.3%

IT Equipment

Printers 14.5%

Servers 16.2%
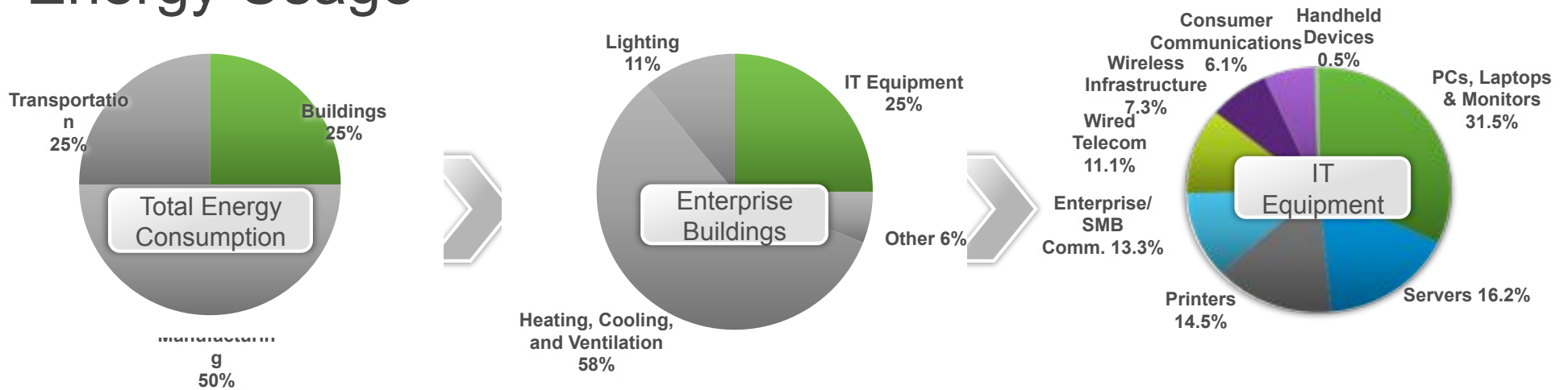
Cost Savings

- Rising energy costs
- IT device proliferation
- Video applications

Sustainability Mandates

- Regulatory compliance
- Government mandates
- Company requirements

Source: BOMA 2006, EIA 2006, AIA 2006
Source: UK Energy Efficiency Best Practice Program; Energy Consumption Guide 19: Energy Use in Offices
Source: Gartner Dataquest, Forecast of IT Hardware Energy Consumption, Worldwide, 2005-2012.

Cisco EnergyWise Goals

- Use the network to measure, monitor and manage energy.

- Allow the network to be the command and control plane for power management

- Cisco Switch or Router is an arbiter or timer for energy management

- Use the network to aggregate power usage reporting

- Allow the network to provide secure, reliable energy management

- Develop a partner eco-system to manage anything connecting to the network.

- Realize the network effect to provide services like location, presence for energy management.

- No Technology Religion – Everything that draws power using lowest common denominator

Cisco EnergyWise Architecture

MANAGEMENT APPLICATIONS

Energy Management Applications	Network Management Applications	Building Management Systems

EnergyWise Management API

Catalyst Switching Network

API

SDK

Gateways

EnergyWise SDK / APIs   **POE / POE+ / UPOE**   **Building Protocols**

Cisco and Partner Devices	POE Powered Devices	Building Devices

IT DEVICES   BUILDING FACILITIES
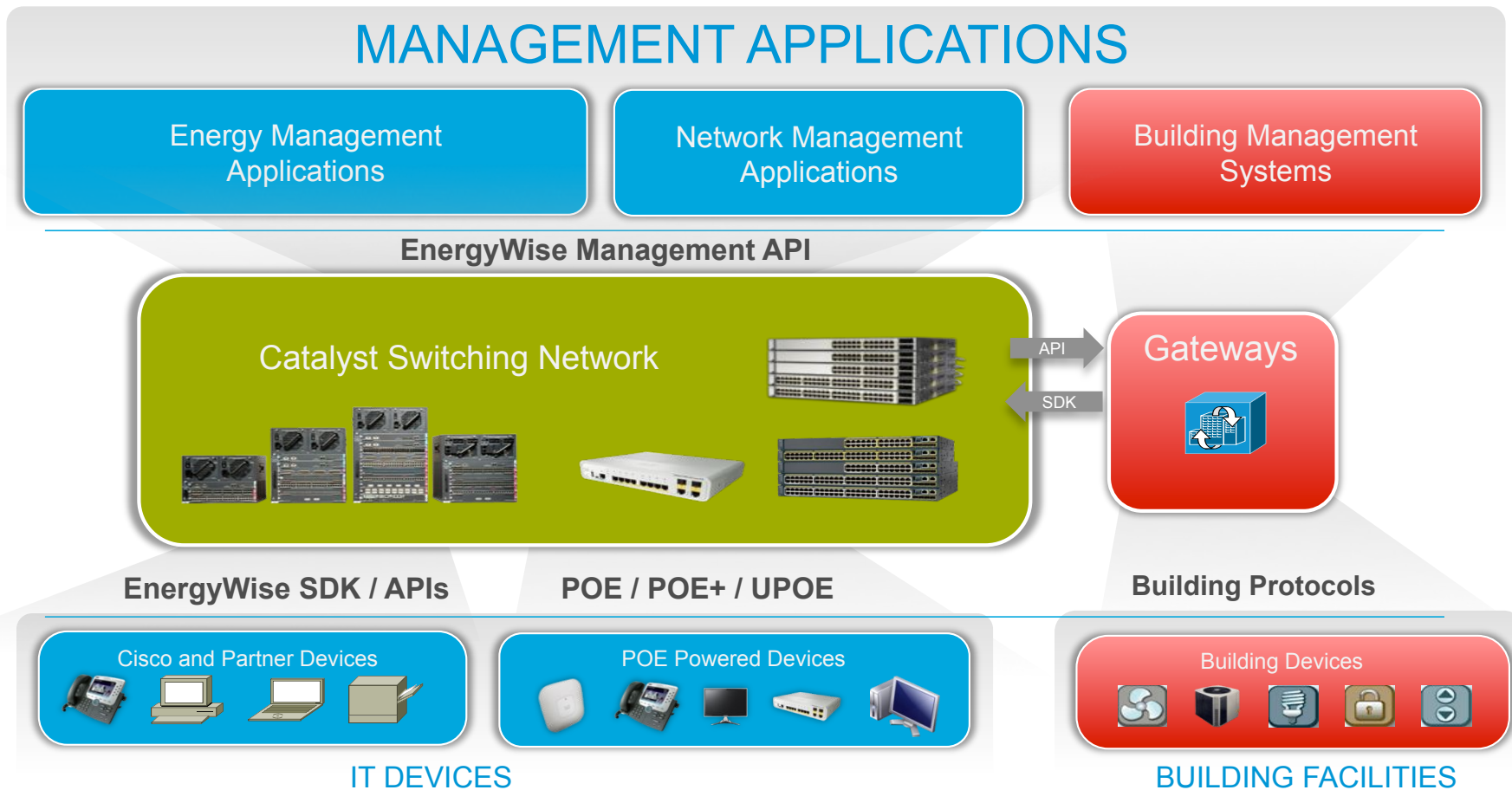
EnergyWise Lowers IT Operational Costs

Across 5,000 Employees Working 9 Hours a Day, 5 Days a Week…

	Annual Energy Cost by Device	EW Annual Savings	EW Annual Savings
PCs: Desktop	$95	10–35%	$50,000 – 175,000
Laptop	$35	10–15%	$20,000 – 30,000
PC Monitors	$30	10–15%	$15,000 – 25,000
APs using POE	$10	40–65%	$20,000 – 35,000
IP Phones	$5	30–50%	$10,000 – 15,000

Saves up to $65 per Switch Port**

Up to 30% Savings in IT!

*Estimates 65% desktops, 35% laptops, 1 AP for every 20 employees, everyone has an IP Phone
Results vary based on what, if any, energy management solution is previously in place; Assumes $0.12 per kWh (kilowatt-hour).
** Assumes ROI across 5 years; modeled on a 250 employee campus

Cisco EnergyWise Product Portfolio

Catalyst 2960-S	Catalyst 2960 and 2975	Catalyst 4500, 4500-X 4900	Catalyst 6500/6500E
Catalyst 3560-E and 3560	Catalyst 3750-E, 3750, 3850*	Catalyst 3750-X / 3560-X	Catalyst 2960-C / 3560-C Compact
Cisco Prime LMS	Cisco IP Phones	VDI Phone Backpack and Tower	Integrated Services Routers (ISR i.e. 1900/2900/3900) G2

Management Applications

What are they useful for?

Global visibility for all devices, not just EnergyWise domains

Graphical reporting: far beyond just numeric values

Policy management: set scheduled on/off

Savings accounting: know when you save and when you don't

Energy baselining and trending: how am I doing versus last month?

Access Control: distribute responsibilities, protect assets

Programmable Actions: turn on a user's equipment when badging

Policy management

Most devices don't need to stay on 24/7 and most are easy to shut down.

PoE Phones, access-points, camera can be shut down easily.

Servers can be spin down (power capped and/ or use conservative frequency governor)

New generation of devices coming up (UPoE lights)

New devices easier to power manage with EnergyWise integration (Xerox for example)
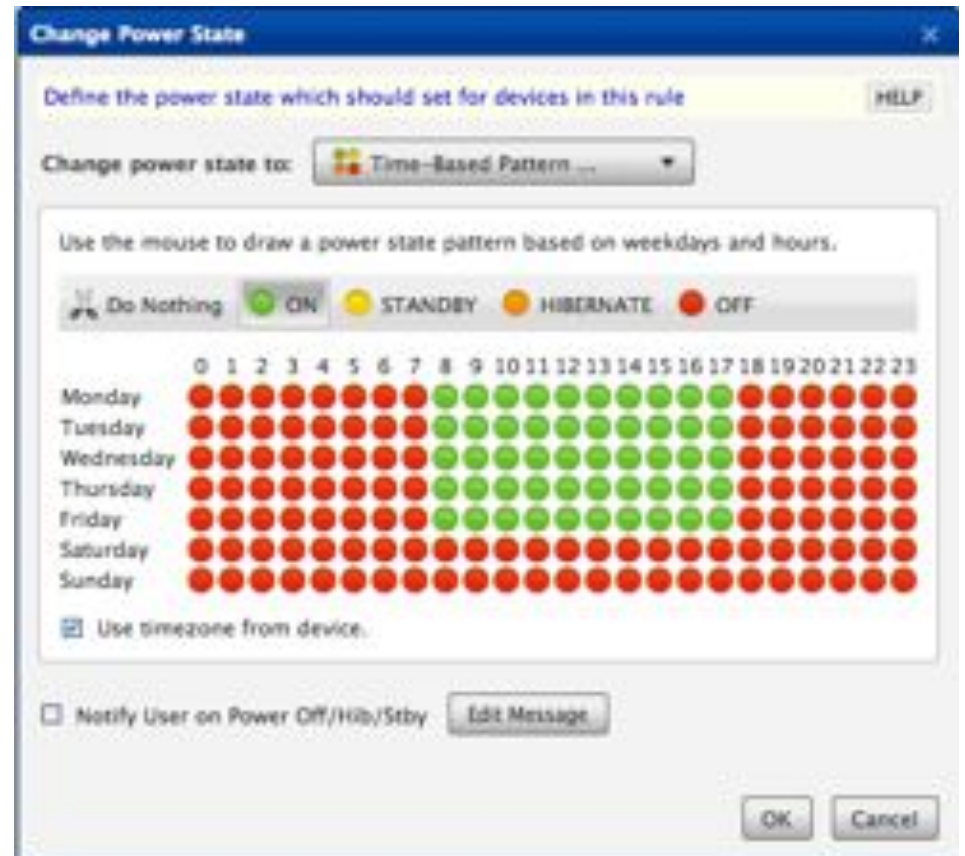
Savings accounting

Savings are no fun when no one's counting.

Mapping between policies and savings

Reporting by type of device, location, business unit and no on.

Perfect for incentivizing teams, as well as cross charging when needed.

Programmable Actions

Policies are great, but programmable actions are more powerful.

Trigger based on external event (energy price, user inactivity, badge access, and so on).

Enables location-based energy services (using phone for location).

Example: when a UPS kicks in, start shutting down non essential equipment after a few minutes.

iPhone Application

EnergyWise Concepts Review

Network/Power Management Application
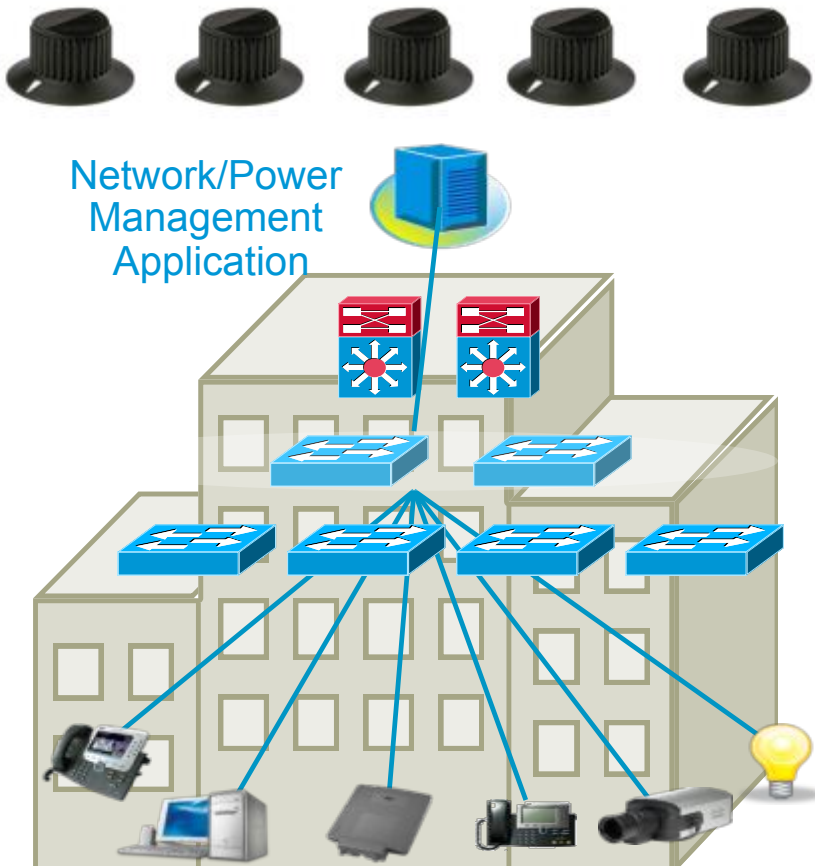
- **Domain**
  Grouping of devices (domain members & endpoints)

- **Name, Role, and Keywords**
  Tag devices with labels to filter the search (via query)

- **Power Levels**
  Indicates the power state of an endpoint (0-10)

- **Importance**
  A mechanism to assign how critical devices are within the domain (1-100)

- **Query**
  The search, command, and control mechanism (collect, sum, set)

- **Recurrence**
  A Time of Day scheduling mechanism to change PoE power states

Configuring a Domain

Begin by Creating an EnergyWise Domain. This Activates EnergyWise on the Switch:

```
EWbackbone# config t

EWbackbone(config)# energywise domain EWdomain1 secret 0 mySecret protocol udp port
43440 ip 10.16.194.200

Switch(config)# exit
EWbackbone#show energy
Module/
Interface    Role             Name              Usage       Category   Lvl   Imp   Type
---------    ----             ----              -----       --------   ---   ---   ----
             backbone-switch  EWbackbone        151.0 (W)   consumer   10    100   module

EWbackbone#show energy domain
Name        : EWbackbone
Domain      : EWdomain1
Protocol    : udp
IP          : 10.16.194.200
Port        : 43440

EWbackbone#
```

Verify that EnergyWise Is Active, and Report Total Available Power

Cisco Confidential   22

EnergyWise Versions and Compatibility

As EnergyWise specifications change over time,

please be aware that some incompatibilities may arise

ensure that the EnergyWise specifications are compatible before deploying a new device

Refer to EnergyWise IOS release notes for versions and compatibility notes
http://www.cisco.com/en/US/docs/switches/lan/energywise/version2_8/ios/release/notes/ol23554.html

Upgrading IOS versions:

CLI that was changed is automatically updated in the running-config

Are generally backward compatible

How to know what EnergyWise version your switch is running:

```
EWbackbone#show energy version
EnergyWise is Enabled
IOS Version:  12.2(58)SE2
EnergyWise Specification:   (rel2_7)4.0.28
```

Endpoint Initiation Process

This is the console output of a proper endpoint discovery

```
sw16#term mon
sw16#debug energywise endpoint
Endpoint debug debugging is on

sw16#show energywise children
Module/
Interface    Role              Name              Usage        Category  Lvl  Imp  Type
---------    ----              ----              -----        --------  ---  ---  ----
             access-switch     sw16-1            55.0  (W)    consumer  10   100  module
Gi1/0/22     FSB3510           FST_Cisco         5.0   (W)    consumer  10   1    endpoint

Total Displayed: 2         Usage: 60.0
sw16#
Apr 27 04:01:27.018: NRGYZ:ENDPOINT:New nanny vector 0x0 for endpoint VMR3
Apr 27 04:01:27.018: NRGYZ:ENDPOINT:New discovery packet from endpoint VMR3(10.16.194.197)
Apr 27 04:01:27.029: NRGYZ:ENDPOINT:Endpoint socket opened, fd 1
Apr 27 04:01:27.034: NRGYZ:ENDPOINT:Successfully sent 32 bytes of endpoint data fd=1
Apr 27 04:01:27.034: NRGYZ:ENDPOINT:Successfully sent 216 bytes of endpoint data fd=1
Apr 27 04:01:27.034: NRGYZ:ENDPOINT:Closing socket, fd 1
Apr 27 04:01:27.102: NRGYZ:ENDPOINT:New discovery packet from endpoint VMR3(10.16.194.197)
Apr 27 04:01:27.102: NRGYZ:ENDPOINT:Endpoint socket opened, fd 1
Apr 27 04:01:27.107: NRGYZ:ENDPOINT:Successfully sent 32 bytes of endpoint data fd=1
Apr 27 04:01:27.107: NRGYZ:ENDPOINT:Successfully sent 216 bytes of endpoint data fd=1
Apr 27 04:01:27.107: NRGYZ:ENDPOINT:Closing socket, fd 1
```

Endpoint Initiation Process (Cont.)

Endpoint discovery continues every 3 minutes thereafter

```
sw16#show energywise children
Module/
Interface    Role                Name                    Usage         Category   Lvl   Imp
  Type
---------    ----                ----                    -----         --------   ---   ---
  ----
             access-switch       sw16-1                  55.0  (W)     consumer   10    100
  module
Gi1/0/22     FSB3510             FST_Cisco               5.0   (W)     consumer   10    1
  endpoint
Gi1/0/23     endpoint            VMR3                    6.0   (W)     consumer   *     *
  endpoint

Total Displayed: 3      Usage: 66.0
sw16#

Apr 27 04:04:27.405: NRGYZ:ENDPOINT:New discovery packet from endpoint
  VMR3(10.16.194.197)
Apr 27 04:04:27.405: NRGYZ:ENDPOINT:Endpoint socket opened, fd 1
Apr 27 04:04:27.405: NRGYZ:ENDPOINT:Successfully sent 32 bytes of endpoint data fd=1
Apr 27 04:04:27.405: NRGYZ:ENDPOINT:Successfully sent 216 bytes of endpoint data fd=1
Apr 27 04:04:27.411: NRGYZ:ENDPOINT:Closing socket, fd 1
Apr 27 04:07:27.698: NRGYZ:ENDPOINT:New discovery packet from endpoint
```

25

Empowering Search

Names, Roles, and Keywords empower search

- Use unique endpoint names to avoid duplicates
- Roles group devices by function
- Keywords allow multiple logical finds

Partner SDK Implementation Philosophies vary:

- Provide minimal EW configuration, use Management Application to push out EW Names, Roles, Keywords (and Importance)
- Provide full GUI(or CLI) EW configuration, use Management Application to push out updates

Empowering Search (Cont.)

Example: PDU

- PDU Names are kept unique: VMR1, VMR2, epower1, etc
- Outlet Names have a convention: Outlet_epower1_1, Outlet_epower1_2, etc
- Role groups device by function: PDU (at the PDU level), Outlet (at the Outlet level)
- Keywords: server,payroll,primary

Empowering Search (Cont.)

PDU's are given unique names

```
EWstack1#energy query imp 100 name VMR* collect usage all

EnergyWise query, timeout is 6 seconds:

Host                Name                          Usage          Level      Imp
----                ----                          -----          -----      ---
10.16.194.189       VMR5                          6.0    (W)     10         50
10.16.194.207       VMR1                          6.0    (W)     10         5
10.16.194.190       VMR4                          6.0    (W)     10         50

Queried:  3    Responded:  3    Time:  4.48 seconds
```

Wildcard searches group similar devices

Empowering Search (Cont.)

Unique outlet names allow the collecting outlet data of a particular PDU

```
EWstack1#energy query imp 100 name Outlet_VMR1* collect usage all

EnergyWise query, timeout is 6 seconds:

Host                Name                            Usage        Level    Imp
----                ----                            -----        -----    ---
10.16.194.207       Outlet_VMR1_1                   0.0   (W)    10       50
10.16.194.207       Outlet_VMR1_2                   104.0 (W)    10       50
10.16.194.207       Outlet_VMR1_3                   0.0   (W)    10       50
10.16.194.207       Outlet_VMR1_4                   0.0   (W)    10       50
10.16.194.207       Outlet_VMR1_5                   69.0  (W)    10       50
10.16.194.207       Outlet_VMR1_6                   116.0 (W)    10       50
10.16.194.207       Outlet_VMR1_7                   0.0   (W)    10       50
10.16.194.207       Outlet_VMR1_8                   104.0 (W)    10       50

Queried:  8     Responded:  8      Time:   4.854 seconds

EWstack1#
```

Empowering Search (Cont.)

Keywords group the outlets of multiple PDU's by vertical function

```
EWstack1#energy query imp 100 keyword finance collect usage all

EnergyWise query, timeout is 6 seconds:

Host                Name                            Usage        Level    Imp
----                ----                            -----        -----    ---
10.16.194.207       Outlet_VMR1_8                   104.0  (W)   10       100
10.16.194.189       Outlet_VMR5_2                   99.0   (W)   10       100

Queried:  2     Responded:  2      Time:  4.47 seconds

EWstack1#
```

Know Your Colors

EnergyWise colors are different than IT colors

Know which colors Partner Products use

Common IT Application Colors

Category	Color	Code	Color
Operational		00FF00	Green
Warning		FFFF00	Yellow
Failed		FF0000	Red

Same Color Has Different Context

EnergyWise Application Colors

Category	Color	Code	Color	Level	Label
Operational (1)		FF0000	Red	10	Full
				9	High
		FFFF00	Yellow	8	Reduced
				7	Medium
		00FF00	Green	6	Frugal
				5	Low
Standby (0)		0000FF	Blue	4	Ready
				3	Standby
		A52A2A	Brown	2	Sleep
				1	Hibernate
Non-Operational (-1)		000000	Black	0	Shut

EnergyWise SNMP Translator

An Agentless mechanism for control of SNMP devices

Many ITC devices are not EnergyWise enabled or PoE Powered.

Problem : Incomplete coverage of IT assets.

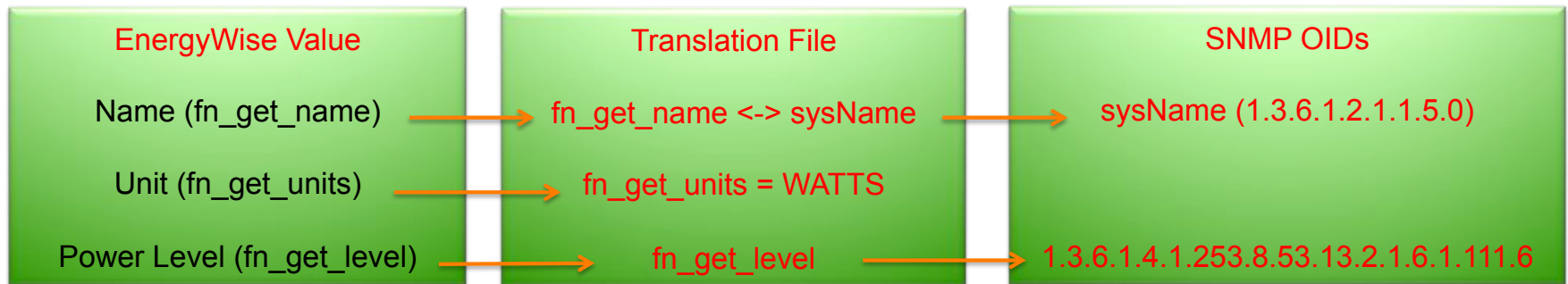**Solution : Translate other protocols to EnergyWise**

Cisco IOS® Software Release 15.0(2)SE

EnergyWise SNMP Translator Behavior

Map EnergyWise and SNMP Data Models – Translation file – load in flash.

SNMP endpoints become transparently managed as if they were native EW endpoints.

Sample translation files available at Cisco.com

EnergyWise Value	Translation File	SNMP OIDs
Name (fn_get_name)	fn_get_name <-> sysName	sysName (1.3.6.1.2.1.1.5.0)
Unit (fn_get_units)	fn_get_units = WATTS	
Power Level (fn_get_level)	fn_get_level	1.3.6.1.4.1.253.8.53.13.2.1.6.1.111.6

Verification

If everything has been configured properly, you should see:

```
switch#show energywise children
Module/
Interface     Role                Name                 Usage         Category   Lvl   Imp   Type
---------     ----                ----                 -----         --------   ---   ---   ----
              WS-C3560G-48PS      NRGYZ-TB-11          130.0  (W)    consumer   10    1     parent
Gi0/1         Endpoint            saturn-lnx1          100.0  (W)    consumer   10    1     endpoint
Gi0/5         IP Phone 7960       SEP0003E3864795      6.3    (W)    consumer   10    1     PoE
Gi0/11        IP Phone 7970       SEP00192FB9CAA5      6.3    (W)    consumer   10    1     PoE
Gi0/12        Xerox WorkCentre    Printer_Floor1_Lobby 300.0  (W)    consumer   10    1     proxy

Subtotals: (Consumer: 542.6 (W), Meter: 0.0 (W), Producer: 0.0 (W))
Total: 542.6 (W), Count: 5
```

New command introduced to check what SNMP proxies are currently running:

```
NRGYZ-TB-11#show energywise proxies
Interface    Host              Role             Name                 Protocol    Mapping
---------    -----             ----             ----                 --------    ------
Gi0/12       2.2.2.11:161      Xerox Workcentre Printer_Floor1_Lobby snmp v2c    Xerox
Gi0/13       2.2.2.12:161      Xerox Workcentre Printer_Floor2_Lobby snmp v2c    Xerox
Gi0/14       2.2.2.20:161      Ricoh            Printer_Floor3_Lobby snmp v2c    Ricoh
```

Currently Shipping EnergyWise-enabled endpoints

Cisco IP Phones*

PDUs

PDUs

Lenovo Laptops

Fieldserver gateway

PDUs

Torana Gateway

Windows with Verdiem Agent

Shipping EnergyWise management solutions

Prime LMS 4.1

Joulex JEM 2.6

Verdiem Surveyor 6

CA EcoMeter

*Requires Call Manager 8.5 and above

0$ Limited Functionality Partner Management Application SKU's allow hands-on use of EnergyWise

New Bundle with every 3K / 4K PoE Switch

- ❑ SKU appears in GPL
- ❑ Features vary with partner
- ❑ Announcement at CiscoLive US 2012

PRESS RELEASE

Cisco Announces Intent to Acquire JouleX

Acquisition Enhances Cisco's Software-as-a-Service Offerings with Energy Management for Enterprise Networks and Data Center Infrastructures

SAN JOSE, Calif. – May 29, 2013 – Cisco today announced its intent to acquire privately held JouleX, a leader in enterprise IT energy management for network-attached and data center assets. JouleX, with headquarters in Atlanta, GA, complements Cisco's existing services portfolio by using the capabilities of the network to gain visibility into and control energy usage across global IT environments.

❑ Upgrade path available

0$ SKU Comparison

joulex.

Device Types	Visibility (Monitoring)	Basic Control (Time Based)	Advanced Control and Reporting*
Cisco Switches and Routers	√	√	Upgrade
Wireless access points	√	√	Upgrade
VoIP phones	√	√	Upgrade
EnergyWise-enabled devices	√	√	Upgrade
Windows PCs/Laptops	√	Upgrade	Upgrade
Monitors, Printers	√	Upgrade	Upgrade
All other campus and data center devices	Upgrade	Upgrade	Upgrade

Verdiem.

Device Types	Visibility (Monitoring)	Basic Control (Time Based)	Advanced Control*
PoE	Unlimited devices forever	Unlimited devices 1 Year	Unlimited devices 1 Year
Cisco Switches	Unlimited devices forever	Unlimited devices 1 Year	Unlimited devices 1 Year
PC/Laptops	Unlimited devices 1 Year	1000 devices 1 Year	1000 devices 1 Year

ca technologies

Note: entire Nimsoft functionality that will support EnergyWise as well as other Nimsoft functionality will be provided for 90 days free of charge.

Call To Action:
Management-friendly Video & Savings Calculator

http://youtube.googleapis.com/v/hGf6DADO468&hl=en_US&fs=1&

Agenda

Operational Efficiency: EnergyWise

IT Effectiveness: Network Automation

Converged Access

An Analogy

Highly motivated individuals

Full control over every single detail

Highly skilled and trained crew

Human brain in every control loop

Specialized distributed crew

Reasonable control within boundaries

From: Detailed control by a single central authority

Towards: Collaborative operations of a partially autonomic system

Device Manageability Instrumentation

Cisco IOS® Device Manageability Instrumentation (DMI)

Fault	Configuration	Performance	Accounting
▪ **IP OAM**—Ping, Trace, BFD, ISG per session ▪ **802.3ah**—Link monitoring and remote fault indication ▪ **802.1 ag**—Continuity check, L2 ping, trace, AIS ▪ **MPLS OAM**—LSP ping, LSP trace, VCCV ▪ **EEM**—Embedded Event Manager ▪ **EVENT-MIB**—OID-based triggers, events, or SNMP Set, IETF DISMON ▪ **EXPRESSION-MIB**—OID expression-based triggers, IETF DISMON ▪ …	▪ **Config CLI**—diff, logging, lock, replace, rollback ▪ **E-LMI**—parameter and status signaling ▪ **E-DI**—Enhanced Device Interface, CLI, Perl, IETF Netconf ▪ **EMM —** Embedded Menu Manager ▪ **NETCONF**—IETF NETCONF XML PI ▪ **CNS** and **WSMA** ▪ **TR-069** ▪ **KRON**—command scheduler ▪ **AutoInstall**—bootstrapping ▪ **IOS.sh** —IOS Shell ▪ **SmartInstall** ▪ **Auto SmartPorts** ▪ …	▪ **Auto IP SLA**—delay, jitter, loss probability ▪ **CBQoS MIB**—class-based QoS ▪ **NBAR** ▪ **RMON** ▪ **EPC** – Embedded Packet Capture ▪ **ERM**—Embedded Resource Manager ▪ **GOLD**—Generic Online Diagnosis ▪ **Smart Call Home**—preventive maintenance ▪ **VidMon**—Video Monitoring ▪ …	▪ **Flexible NetFlow**—IETF IPFIX ▪ **BGP policy accounting** – includes AS information ▪ **Periodic MIB bulk data collection and transfer** ▪ …

Security
▪ **Auto Secure**—one-touch device hardening ▪ **LDP Auth**—message authentication ▪ **Routing Auth**—MD5 authentication, BGP, OSPF ▪ …

**Device Manageability Instrumentation Has Evolved Significantly**

Smart Operations Feature Support – Switching Portfolio

January 2013

Feature	Catalyst 6500	Catalyst 4500	Catalyst 3xx0	Catalyst 2xx0
Smart Install (Director)	●	●	●	○
Auto Smartports	○	●	●	●
AutoQoS	●	●	● *	●
Flexible NetFlow	●	●	●	○
IP SLAs	●	●	●	◐ Responder only
EEM	●	●	●	○
Smart Call Home	●	●	●	●
GOLD	●	●	●	○
SPAN/RSPAN	●	●	●	●
ERSPAN	●	○	○	○
Protocol Analyzer / Wireshark	●	●	○	○
TDR	●	●	●	●

* Specific hardware required C3KX-SM-10G

Embedded Event Manager (EEM)
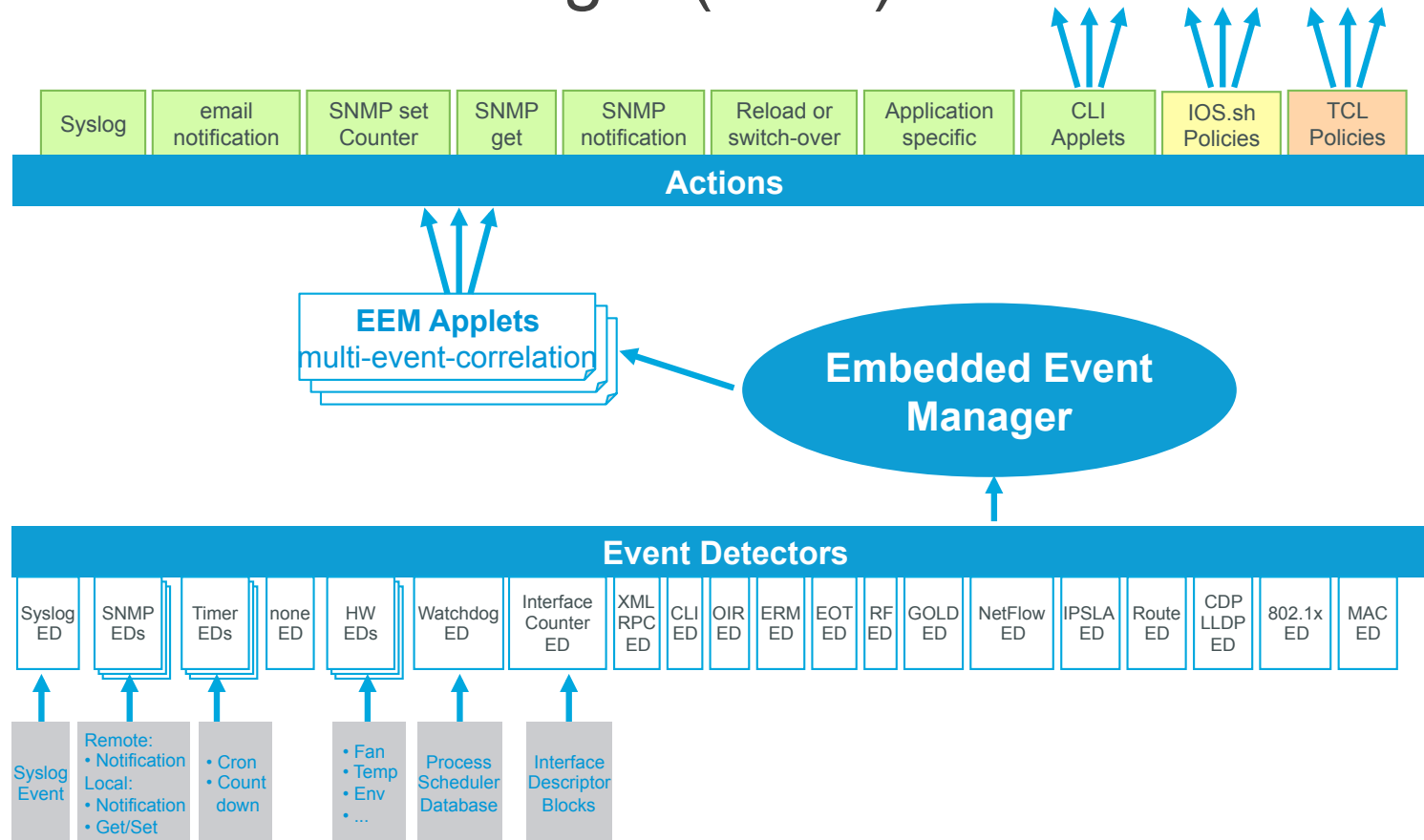
Embedded Event Manager – Applet Evolutions

EEM Version	Release	Applet Modifications	Peanut Gallery Comments
1.0	12.0(26)S 12.3(4)T	2 Events: Syslog, SNMP Actions: Log, CNS event, Reload, Switchover	Initial Version Limited benefits
2.0 2.1 2.2	12.3(14)T1 12.2(18)SXF5 12.4M	No structure changes Various New event detectors New actions: cli, info, mail, policy, SNMP trap, Modify counters, Publish application events, Read/set tracked objects	Many new actions Popular CLI / mail Actions run linear
2.3	12.4(11)T	maxrun support pattern parameter for CLI actions	Maxrun support == security Can handle CLI prompts
2.4	12.4(20)T	multi-event support	Boolean correlation of events within applet.
3.0	12.4(22)T 12.2(33)SE	Redesign of action mechanism Program counter added Loops, conditionals, regexps, context save, error handling	Applets now rock! Programming language feel.
3.1/3.2	-	No changes	-
4.0	15.2(2)T	Applet file actions TLS/SSL support for SMTP actions Custom port for SMTP actions	File manipulation handy!

Example: EEM Applets – Loops, Variables

Problem: None in Particular

Solution: Have fun exploring EEM Applet capabilities

```
event manager applet 99-bob
    description written by bklauser inspired by http://www.99-bottles-of-
beer.net
    event none
    action 100 set b 99
    action 110 while $b gt 1
    action 120  puts "$b bottles of beer on the wall, $b bottles of beer."
    action 130  decrement b
    action 140  puts "Take one down, pass it around, "
    action 150  puts "$b bottles of beer on the wall.\n"
    action 160 end
    action 170 puts "$b bottle of beer on the wall, $b bottle of beer."
    action 180 puts "Take one down, pass it around, "
    action 190 puts "no more bottles of beer on the wall.\n"
    action 200 puts "No more bottles of beer on the wall, "
    action 210 puts "no more bottles of beer."
    action 220 puts "Go to the store and buy some more, "
    action 230 puts "99 bottles of beer on the wall.\n"
!
alias exec sing event manager run 99-bob
```

Setting a Variable

While Loop – {

Decrementing a Variable

While Loop – }

Referencing a Variable

Using an Alias to run our Applet

See also: http://www.99-bottles-of-beer.net/language-cisco-ios-embedded-event-manager-applet-2909.html

Network Automation Adoption

OPEN NETWORK ENVIRONMENT

Value to Business

Type III – Automation as Integral Part of Solution Design

Benefits:
- Revenue *enabler*
- OPEX ↓
- CAPEX ↓
- Quality ↑
- Reactive → Proactive
- Corporate Learning enabler

Type II Automate New Task

Benefits:
- OPEX ↓
- CAPEX ↓
- Quality ↑
- Reactive → Proactive

Type I Automate Existing Task

Benefits:
- OPEX ↓
- Quality ↑

Maturity and Innovation

Cisco ONE Platform Kit (onePK)

YOUR Applications

onePK

Any Cisco Router or Switch

Network Programming Environment to:

- Innovate
- Extend
- Automate
- Customize
- Enhance
- Modify

C, JAVA Program

API Presentation

onePK IPC Channel

API Infrastructure

Catalyst

Nexus

ASR ISR
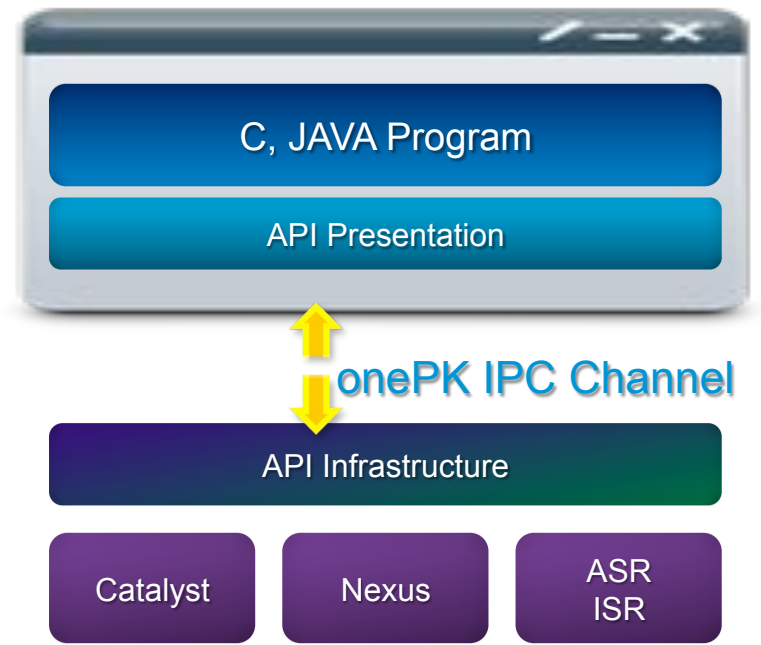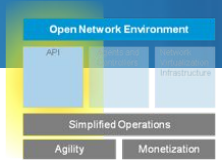
Cisco ONE Platform Kit (onePK)

onePK Provides

Abstractions (Service Sets)

Programmatic Interfaces (C, Java, (REST) …)

Software Development Kit (SDK)

Anatomy of a onePK Application

Software Application (currently C and Java)

Interfaces and Abstractions (Service Sets)

Communication Bus (Thrift IDL)

Connected-Apps Agent in Network OS
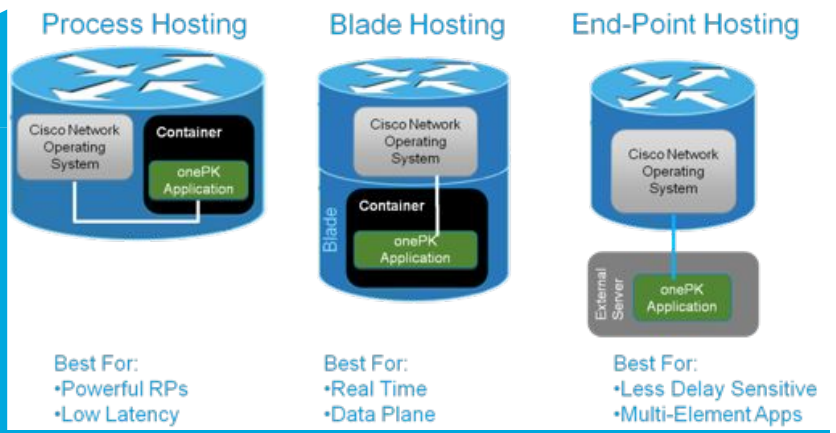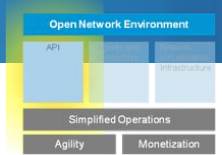
Network OS Features and Embedded Automations

Service Set	Description
Data Path	Provides packet delivery service to application: Copy, Punt, Inject
Policy	Provides filtering (NBAR, ACL), classification (Class-maps, Policy-maps), actions (Marking, Policing, Queuing, Copy, Punt) and applying policies to interfaces on network elements
Routing	Read RIB routes, add/remove routes, receive RIB notifications
Element	Get element properties, CPU/memory statistics, network interfaces, element and interface events
Discovery	L3 topology and local service discovery
Utility	Syslog events notification, Path tracing capabilities (ingress/egress and interface stats, next-hop info, etc.)
Developer	Debug capability, CLI extension which allows application to extend/integrate application's CLIs with network element

Process Hosting

Cisco Network Operating System — Container — onePK Application

Best For:
• Powerful RPs
• Low Latency

Blade Hosting

Cisco Network Operating System — Container — onePK Application

Best For:
• Real Time
• Data Plane

End-Point Hosting

Cisco Network Operating System — External Server — onePK Application

Best For:
• Less Delay Sensitive
• Multi-Element Apps

Write once run anywhere

Portfolio of API, Languages and Abstractions

Network Programming with onePK and Embedded Network Automation

Native Network OS Embedded Automation	Advanced Network OS Embedded Scripting	Structured API	Object Oriented API	Higher-Level Abstractions / Interfaces
Event-/Expression-MIB, PfR, IPSLA Thresholds, Embedded Event Manager Applets, …	Tcl, Python, Embedded Event Manager, EASy, …	onePK C	onePK Java	onePK Libraries REST, XMPP, Design Patterns, OMNI Controllers, …

Network Programming – SDN

Network Automation – Embedded Automations

Choice and Flexibility of Implementation

Monitoring Resources

Problem: During the planning cycle, we would like to understand if total CPU usage reaches critical levels

Solution: Define an ERM policy to notify upon resource depletion

```
resource policy
 policy my-erm-policy-1 type iosprocess
  system
    cpu total
      critical rising 90 interval 15 falling 20 interval 10 global
      major rising 70 interval 15 falling 15 interval 10 global
      minor rising 60 interval 15 falling 10 interval 10 global
!
```

➜ If **Total** CPU usage count rises above 90% at an interval of 15s, a Critical Up notification is sent

```
Feb 17 13:32:18.283: %SYS-4-CPURESRISING: System is seeing global
cpu util 62% at total level more than the configured minor limit 60%
```

Monitoring Multiple Processes

Problem: In order to detect resource consumption caused by brute force login attempts, we want to keep an eye on CPU utilization by the login processes

Solution: Define an ERM policy to notify upon critical / suspicious levels
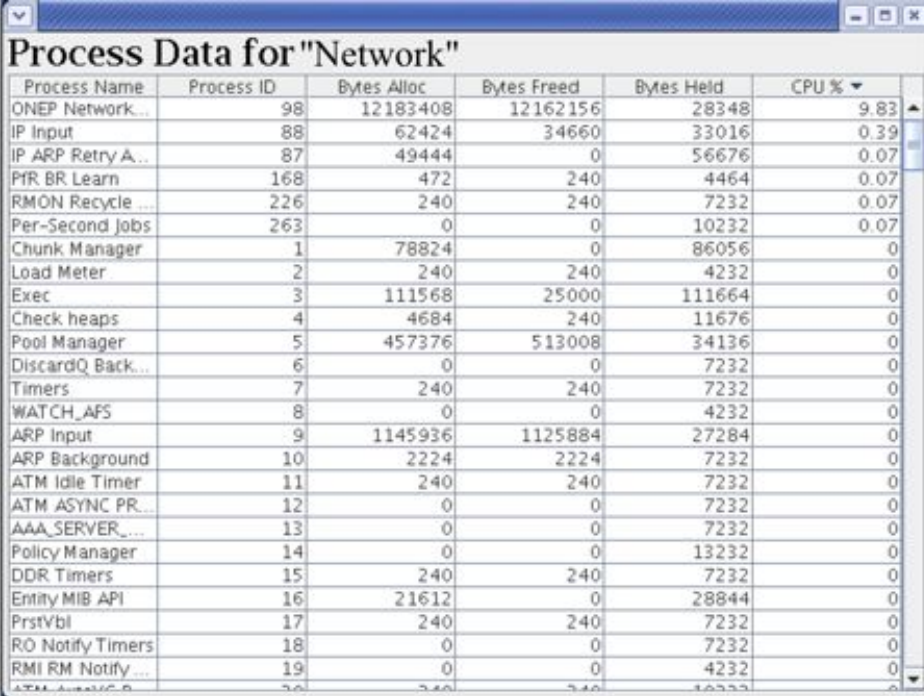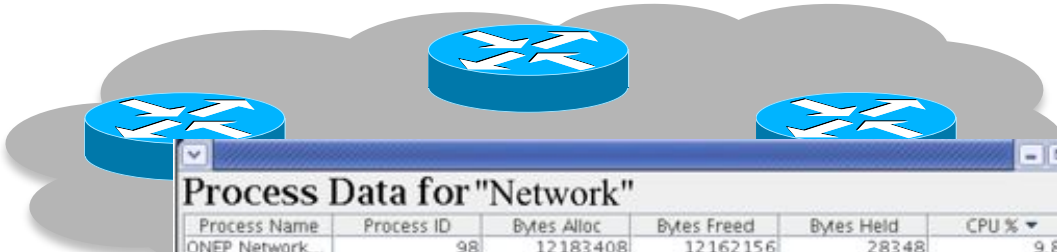
```
resource policy
  policy my-login-policy type iosprocess
    system
      cpu process
        critical rising 30 interval 10 falling 20 interval 10
        major rising 20 interval 10 falling 10 interval 10
        minor rising 10 interval 10 falling 5 interval 10
  user group my-login-group type iosprocess
    instance "SSH Process"
    instance "SSH Event handler"
    :
    policy my-login-policy
```

→ Syslog if **Group** CPU Usage Count Rises Above 10% at an Interval of 10s

```
*Aug 25 12:56:26.089: %SYS-4-CPURESRISING: Resource group my-login-group is seeing local cpu
util 16% at process level more than the configured minor limit 10%

*Aug 25 12:56:41.089: %SYS-6-CPURESFALLING: Resource group my-login-group is no longer seeing
local high cpu at process level for the configured minor limit 10%, current value 0%
```

51

A Network "Top"

Process Data for "Network"

Process Name	Process ID	Bytes Alloc	Bytes Freed	Bytes Held	CPU % ▼
ONEP Network...	98	12183408	12162156	28348	9.83
IP Input	88	62424	34660	33016	0.39
IP ARP Retry A...	87	49444	0	56676	0.07
PfR BR Learn	168	472	240	4464	0.07
RMON Recycle ...	226	240	240	7232	0.07
Per-Second Jobs	263	0	0	10232	0.07
Chunk Manager	1	78824	0	86056	0
Load Meter	2	240	240	4232	0
Exec	3	111568	25000	111664	0
Check heaps	4	4684	240	11676	0
Pool Manager	5	457376	513008	34136	0
DiscardQ Back...	6	0	0	7232	0
Timers	7	240	240	7232	0
WATCH_AFS	8	0	0	4232	0
ARP Input	9	1145936	1125884	27284	0
ARP Background	10	2224	2224	7232	0
ATM Idle Timer	11	240	240	7232	0
ATM ASYNC PR...	12	0	0	7232	0
AAA_SERVER_...	13	0	0	7232	0
Policy Manager	14	0	0	13232	0
DDR Timers	15	240	240	7232	0
Entity MIB API	16	21612	0	28844	0
PrstVbl	17	240	240	7232	0
RO Notify Timers	18	0	0	7232	0
RMI RM Notify ...	19	0	0	4232	0

Use onePK to build a live process monitor similar to UNIX *top*

The same app can connect to multiple devices to display the top processes across the entire network

Quickly export SNMP Statistics?

Problem: Sometimes we need data from one or multiple MIBs, but

- we may not want to (re-)configure an NMS
- don't want to constantly poll
- need to gather data during temporary loss of connectivity

Solution: Use Bulk File MIB to define the data we need and periodically transfer it to a convenient location

- group data from multiple MIBs
- single, common polling interval
- buffer data
- transfer using RCP, FTP, TFTP
- format ASCII or Binary

Feature Name: Periodic MIB Data Collection and Transfer Mechanism

Available from: IOS 12.0(24)S, 12.2(25)S, 12.3(2)T, IOS XE 2.1, IOS XR 3.2
Platforms: ASR1k, x8xx ISR, x900x ISR, 72xx, 73xx, 76xx, 10xxx, ME3400, C4k, C6k, …
See: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.2.1.2

Configuration – Example

1. Define Lists of relevant OIDs (Names for IF-MIB, ASN.1 for all others)

```
Router(config)# snmp mib bulkstat object-list my-if-data
Router(config-bulk-objects)# add ifIndex
Router(config-bulk-objects)# add ifDescr
Router(config-bulk-objects)# add ifAdminStatus
Router(config-bulk-objects)# add ifOperStatus
Router(config-bulk-objects)# exit
```

2. Specify Polling Schema

```
Router(config)# snmp mib bulkstat schema my-if-schema
Router(config-bulk-sc)# object-list my-if-data
Router(config-bulk-sc)# poll-interval 1
Router(config-bulk-sc)# instance exact interface FastEthernet0
Router(config-bulk-sc)# exit
```

3. Configure the Transfer Mechanism – and enable it !

```
Router(config)# snmp mib bulkstat transfer my-fa0-transfer
Router(config-bulk-tr)# schema my-if-schema
Router(config-bulk-tr)# transfer-interval 5
Router(config-bulk-tr)# url primary tftp://10.10.10.10/folder/
Router(config-bulk-tr)# retain 30
Router(config-bulk-tr)# buffer-size 4096
Router(config-bulk-tr)# enable
```

Flexible NetFlow (FNF) – Recap

Traffic

Flow Monitor 1

Flow Monitor 2

Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non-Key Fields
Packets
Bytes
Timestamps
Next Hop Address

Key Fields	Packet 1
Source IP	3.3.3.3
Dest IP	2.2.2.2
Input Interface	Ethernet 0
SYN Flag	0

Non-Key Fields
Packets
Timestamps

Traffic Analysis Cache

Source IP	Dest. IP	Source Port	Dest. Port	Protocol	TOS	Input I/F	…	Pkts
3.3.3.3	2.2.2.2	23	22078	6	0	E0	…	1100

Security Analysis Cache

Source IP	Dest. IP	Input I/F	Flag	…	Pkts
3.3.3.3	2.2.2.2	E0	0	…	11000

Flexible NetFlow (FNF) – Key Fields – 1/2

Flow
Sampler ID
Direction

Interface
Input
Output

Layer 2
Source VLAN
Dest VLAN
Dot1q VLAN
Dot1q priority
Source MAC address
Destination MAC address

IPv4	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	TTL
Protocol	Options bitmap
Fragmentation Flags	Version
Fragmentation Offset	Precedence
Identification	DSCP
Header Length	TOS
Total Length	

IPv6	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	DSCP
Protocol	Extension Headers
Traffic Class	Hop-Limit
Flow Label	Length
Option Header	Next-header
Header Length	Version
Payload Length	

Flexible NetFlow (FNF) – Key Fields – 2/2

Routing
src or dest AS
Peer AS
Traffic Index
Forwarding Status
IGP Next Hop
BGP Next Hop
Input VRF Name

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type*	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

Application
Application ID*

Multicast
Replication Factor*
RPF Check Drop*
Is-Multicast

*: IPv4 Flow only

57

Flexible NetFlow (FNF) – Configuration

1. Configure the Exporter

```
Router(config)# flow exporter my-exporter

Router(config-flow-exporter)# destination 1.1.1.1
```

2. Configure the Flow Record

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

3. Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor

Router(config-flow-monitor)# exporter my-exporter

Router(config-flow-monitor)# record my-record
```

4. Apply to an Interface

```
Router(config)# interface s3/0

Router(config-if)# ip flow monitor my-monitor input
```

Flexible NetFlow (FNF) – Top Talkers

- Top ten IP addresses that are sending the most packets

```
Router# show flow monitor <monitor> cache
        aggregate ipv4 source address
        sort highest counter bytes top 10
```

- Top five destination addresses to which we're routing most traffic from the 10.10.10.0/24 prefix

```
Router# show flow monitor <monitor> cache
        filter ipv4 destination address 10.10.10.0/24
        aggregate ipv4 destination address
        sort highest counter bytes top 5
```

- 5 VLAN's that we're sending the least bytes to:

```
Router# show flow monitor <monitor> cache
        aggregate datalink dot1q vlan output
        sort lowest counter bytes top 5
```

- Top 20 sources of 1-packet flows:

```
Router# show flow monitor <monitor> cache
        filter counter packet 1
        aggregate ipv4 source address
        sort highest flow packet top 20
```

Flexible NetFlow and EEM – Low TTL

Problem: We want to know about low-TTL traffic

Solution: Use Flexible Netflow and Embedded Event Manager 3.0 to detect traffic flows with TTL < 5

1. Configure flexible Netflow to match on TTL, Source- and Destination Address

```
flow record <my-record>
        match ipv4 ttl
        match ipv4 source address
        match ipv4 destination address
:
flow monitor <my-monitor>
        record <my-record>
:
```

- Top (unexpected) Talkers with low-TTL traffic ?
- Deviation from Normal ?
- Senders with many low-TTL flows ?
- Take Actions (block suspicious senders) ?

2. Configure the Netflow Event Detector in EEM to notify upon a new flow record

```
event manager applet my-ttl-applet
        event nf monitor-name "my-ttl-monitor" event-type create event1
                entry-value "5" field ipv4 ttl entry-op lt
        action 1.0 syslog msg "Low-TTL flow from $_nf_source_address"
```

3. Syslog message and/or use `show flow monitor <my-monitor> cache` command

```
*Dec  2 17:39:31.221: %HA_EM-6-LOG: my-ttl-applet: Low-TTL flow from 192.168.2.248
```

60

Son: Dad, why are there always 2 Pilots?

Dad: One has to prevent the other from doing **stupid things**

Son: Which one is doing the stupid things?

CLI 'Safety' and Quality Features

- **Contextual configuration diff utility**   (from 12.3(4)T, 12.2(25)S)

    Easily show differences between running and startup configuration

    Compare any two configuration files

- **Config change logging and notification**   (from 12.3(4)T, 12.2(25)S)

    Tracks config commands entered per user, per session

    Notification sent indicating config change has taken place—changes can be retrieved via SNMP

- **Configuration replace and rollback**   (from 12.3(7)T, 12.2(25)S)

    Replace running config with any saved configuration (only the diffs are applied) to return to previous state

    Automatically save configs locally or off box

    Config Rollback Confirmed Change   (from 12.4(23)T, 12.2(33)S)

- **Configuration locking**   (from 12.3(14)T, 12.2(25)S)

    Ensures exclusive configuration change access

Example: Config Revert

Problem: critical config change to a remote router may result in loss of connectivity, requiring a reload

Solution: revert the running configuration after two minutes – unless the change made is confirmed

```
router# config terminal revert time 2
Rollback Confirmed Change: Backing up current running config to flash:bk-2

Enter configuration commands, one per line.  End with CNTL/Z.
  :
  ... your Config Change work here ...
  :
router# hostname oops
oops(config)# end
oops# Rollback Confirmed Change: Rollback will begin in one minute. Enter
"configure confirm" if you wish to keep what you've configured
```

```
oops# Rollback Confirmed Change: rolling
to:flash:bk-2
Total number of passes: 1
Rollback Done
router#
```

or

```
oops# config confirm
oops#
```

Available from: IOS 12.4(23)T, 12.2(33)S

63

Event-Based Configurations – Beyond ASP

Problem: How to trigger custom event-based port configurations

Solutions: Use Embedded Event Manager (EEM)

Auto Smart Ports are powered by EEM

Pre-built port configuration templates for simplify user experience and minimize configuration error

Automatic event detection (CDP/LLDP/MAC) triggers auto configuration

Authentication (802.1x, MAB) and authorization can be conducted before port configuration applied

Automatic notification can be sent to NMS system to help with asset tracking

Plug-n-play device deployment ~ over all management cost
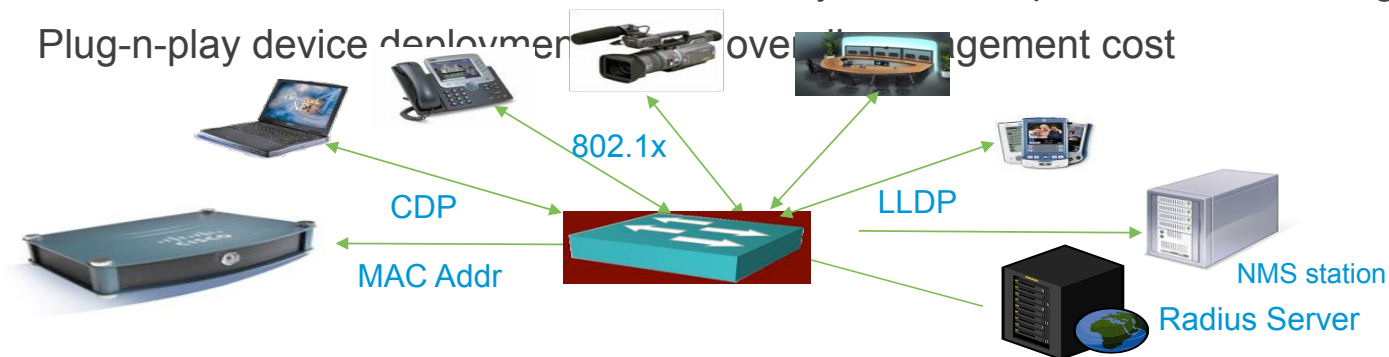
Event-Based Configurations – Beyond ASP

Example: When a printer is added to the network, use an EEM applet to create a new ASP event

```
event manager applet dectect-printer
event neighbor-discovery interface regexp FastEthernet.* cdp add
action 001 regexp ".*LasterJet.*" "$_nd_cdp_platform"
action 002 if $_regexp_result eq 1
action 003  cli command "enable"
action 004  cli command "config t"
action 005  cli command "interface $_nd_local_intf_name"
action 006  cli command "switchport access vlan $printer_vlan"
action 007  cli command "switchport mode access"
action 008  cli command "switchport port-security"
action 009  cli command "switchport port-security violation restrict"
action 010  cli command "switchport port-security aging time 2"
action 011  cli command "switchport port-security aging type inactivity"
action 012  cli command "spanning-tree portfast"
action 013  cli command "spanning-tree bpduguard enable"
action 014  cli command "end"
action 015  syslog msg "New printer added: $_nd_cdp_entry_name , type:
   $_nd_cdp_platform"
action 016 end
```

```
*** STOP: 0x0000007B (0xF201B84C,0xC0000034,0x00000000,0x00000000)
INACCESSIBLE_BOOT_DEVICE

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check for viruses on your computer. Remove any newly installed
hard drives or hard drive controllers. Check your hard drive
to make sure it is properly configured and terminated.
Run CHKDSK /F to check for hard drive corruption, and then
restart your computer.

Refer to your Getting Started manual for more information on
troubleshooting Stop errors.
```

POST (Power-On Self-Test) is great ...

... but some errors you prefer to know while the system is up and running ...

... and: can you afford to power-cycle after OIR just for POST to run ?

Generic Online Diagnostics (GOLD)

Problem: How to detect wear and tear issues before they cause an outage? Hardware aging as well as repeated insertion and removal of modules can lead to wear and tear damage on connectors. This can cause failures – how do you find out during operation, without power-cycling the box ?

**Solution:** Use GOLD to verify functionality of a mis-behaving module

- Bootup Diagnostics (upon bootup and OIR)

- Periodic Health Monitoring (during operation)

- OnDemand (from CLI)

- Scheduled Testing (from CLI)

- Test Types include:
  - Packet switching tests
  - Memory Tests
  - Error Correlation Tests

- Complementary to POST

Available from: CatOS 8.5(1), IOS 12.2(14)SX
Platforms: CBS 3xxx, Cat 3560, 3750, 6500, ME6524, 72xx, 10k, CRS

Good Practice: schedule all non-disruptive tests periodically
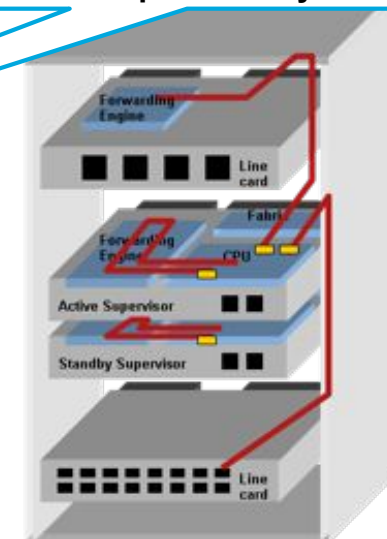
References – Instrumentation and Automation

Device Manageability Instrumentation (DMI) www.cisco.com/go/instrumentation

- Embedded Event Manager (EEM): www.cisco.com/go/eem

- Cisco Beyond – EEM Community: www.cisco.com/go/ciscobeyond

- Embedded Menu Manager (EMM): http://tinyurl.com/emm-in-124t

- Embedded Packet Capture (EPC): www.cisco.com/go/epc

- Flexible NetFlow: www.cisco.com/go/netflow and www.cisco.com/go/fnf

- GOLD: http://www.cisco.com/en/US/products/ps7081/products_ios_protocol_group_home.html

- IPSLA (formerly SAA, formerly RTR): www.cisco.com/go/ipsla

- Network Analysis Module: http://www.cisco.com/go/nam

- Network Based Application Recognition (NBAR): www.cisco.com/go/nbar

- Security Device Manager (SDM): http://www.cisco.com/go/sdm

- Smart Call Home: www.cisco.com/go/smartcall

- Web Services Management Agents (WSMA): http://tinyurl.com/wsma-in-150M

- Cisco Configuration Engine (CCE): www.cisco.com/go/ciscoce

- **Feature Navigator: www.cisco.com/go/fn**
- **MIB Locator: www.cisco.com/go/mibs**

Key Takeaways

Network Automation and Programming with
Cisco Open Networking Environment …

… provides Choice and Flexibility of
- APIs and Abstractions
- Architectures
- Deployment Models

… closes the gap between Applications and Networks

… enables Operational Savings and New Opportunities
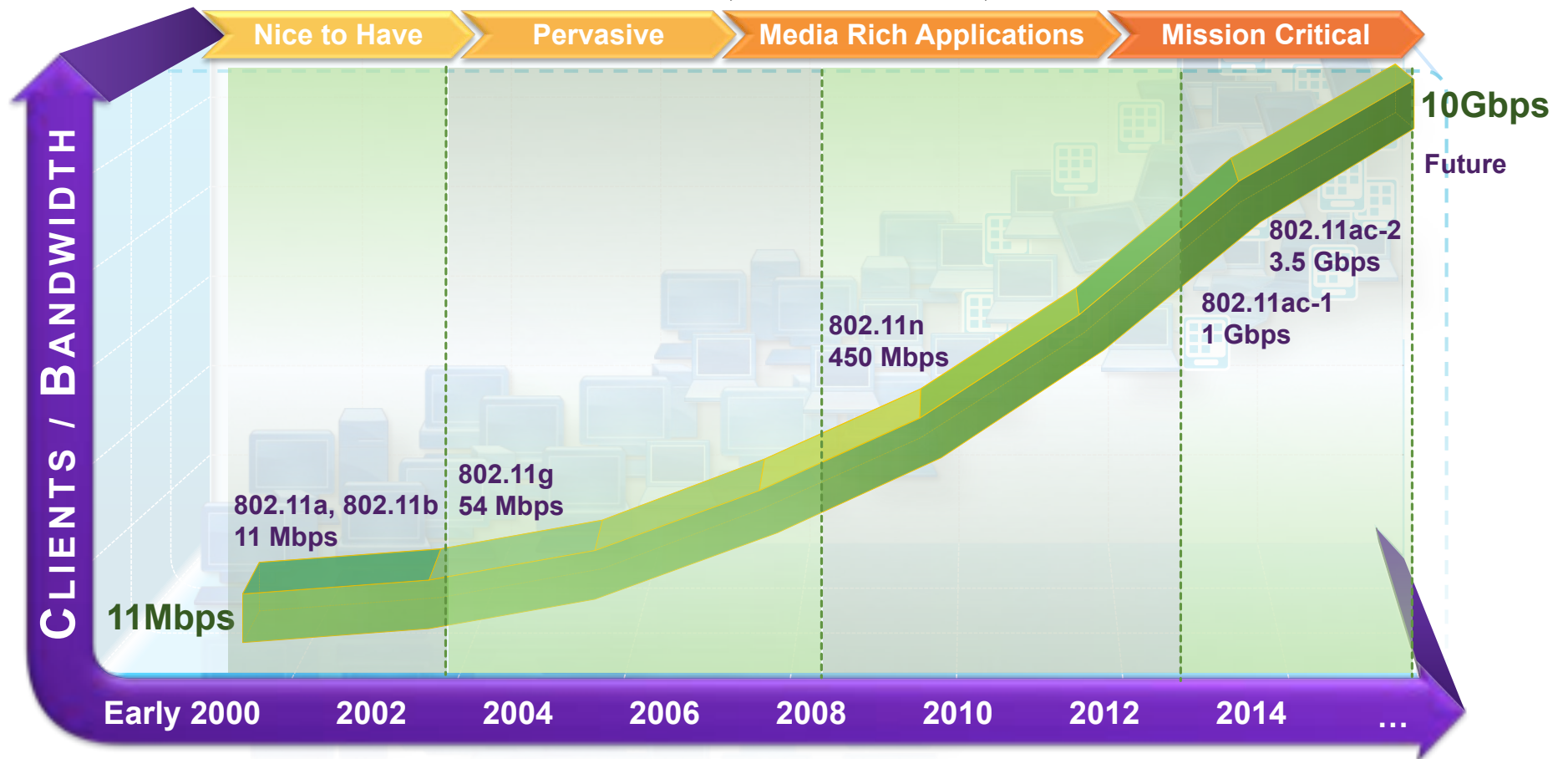
… puts YOU in control

What will YOU program ?

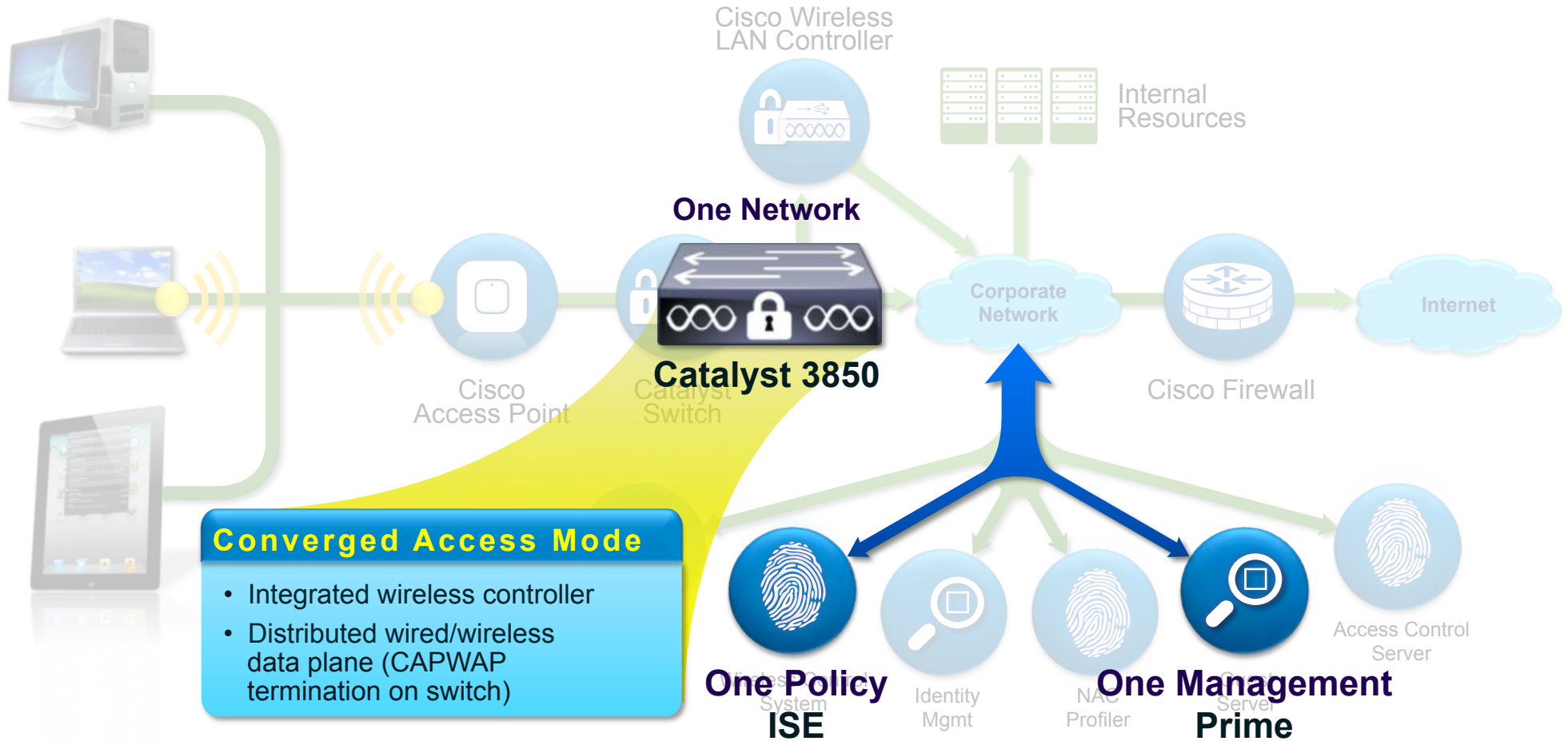# Agenda

Operational Efficiency: EnergyWise

IT Effectiveness: Network Automation

Converged Access

Wireless Standards – Past, Present, and Future

One Network with Converged Access

Cisco Wireless
LAN Controller

Internal
Resources

One Network

Corporate
Network

Catalyst 3850

Cisco
Access Point

Catalyst
Switch

Cisco Firewall

Internet

Converged Access Mode

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

**One Policy
ISE**

Wireless Control
System

Identity
Mgmt

NAC
Profiler

**One Management
Prime**

Guest
Server

Access Control
Server

Change in Catalyst Access Switching Portfolio

Unified Workspace

Data Voice

BYOD Video Mobility

Traditional Workspace

Catalyst 3750-X

Catalyst 3k Series

Catalyst 3850

Catalyst 4500E

Scale & Performance

TrustSec

Application Visibility

Energy Management and Green

Lower TCO

Catalyst 2960-S

- Scale & Performance
- Security
- Lower TCO

CONVERGED ACCESS*

Distributed Intelligent Access Services

* - Shipping on Catalyst 3850, Roadmap on Catalyst 4500E

Converged Wired/Wireless Access – Benefits

Single platform for wired and wireless	Network wide **visibility** for faster troubleshooting	Consistent security and quality of service **control**	Maximum **resiliency** with fast stateful recovery	**Scale** with distributed wired and wireless data plane
Common IOS, same administration point, one release	Wired and wireless traffic visible at every hop	Hierarchical bandwidth management and distributed policy enforcement	Layered network high availability design with stateful switchover	480G stack bandwidth; 40G wireless/switch; efficient multicast

Unified Access - One Policy | One Management | One Network

Catalyst 3850 - Platform Overview

Wireless CAPWAP Termination

Up to 50 APs/2000 clients per stack, and 40G per switch

480 Gbps Stacking Bandwidth

Up to 2000 Clients per Stack

FRU Fans, Power Supplies - HA

Full POE+

Stackpower

Granular QoS/Flexible NetFlow

Multi-Core CPU

Line Rate on All Ports

40 Gbps Uplink Bandwidth (Modular)
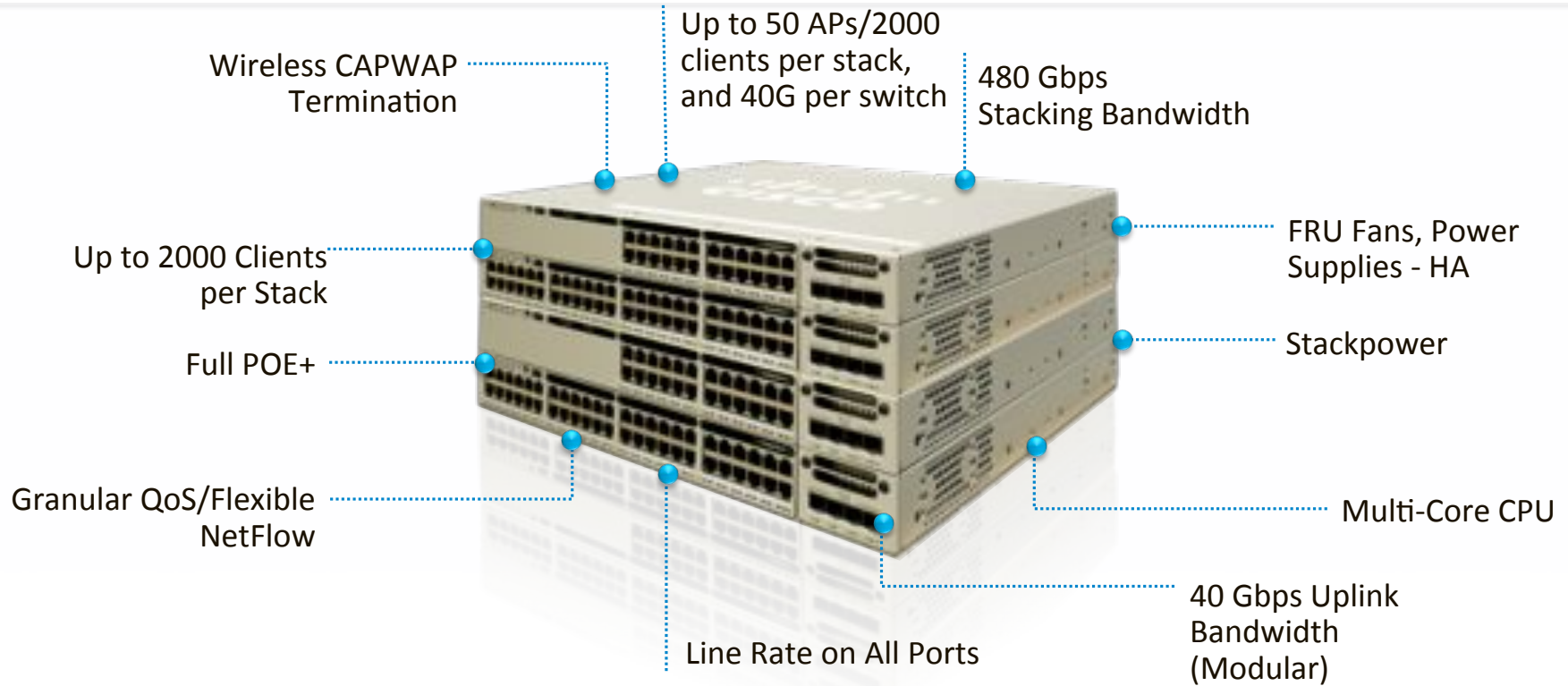
Built on Cisco's Innovative "UADP" ASIC

Scalable and Programmable ASIC – Foundation for Cisco ONE

Unified Access Data Plane (UADP) ASIC

$100M+ R&D Investment

300+ Person-Years

First Access ASIC for Wired and Wireless Traffic Processing

Future integration with Cisco ONE (Open Network Environment)

Programmable: Fast Feature Rollout with Investment Protection

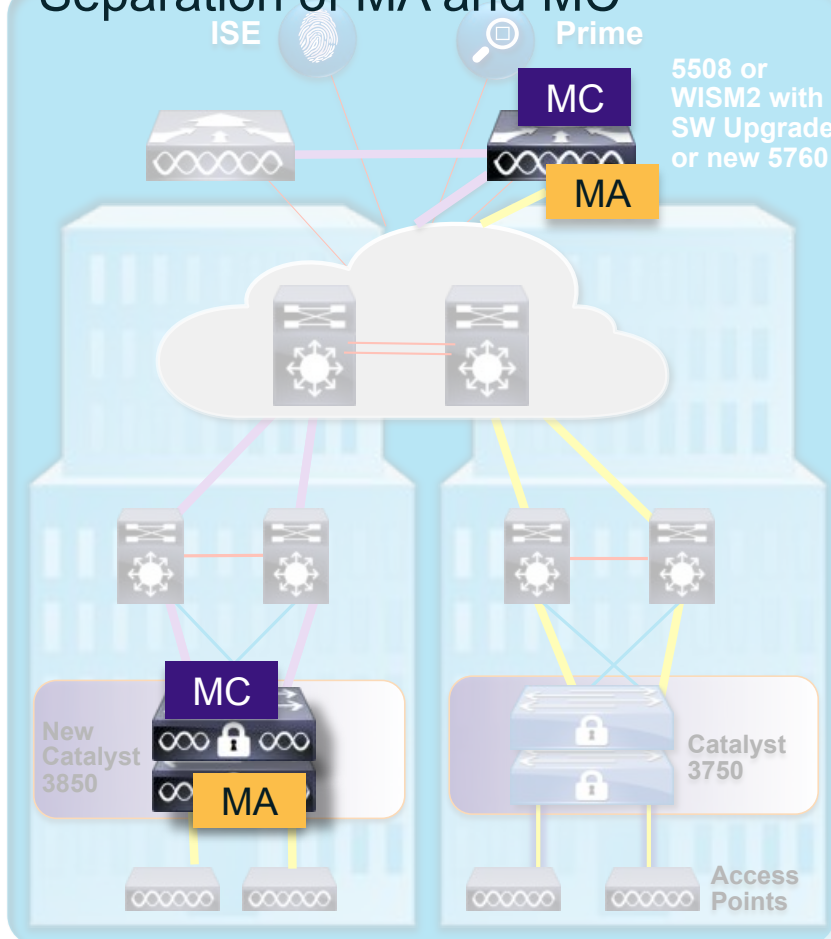# Understanding Current Deployment Model
The Wireless LAN Controller
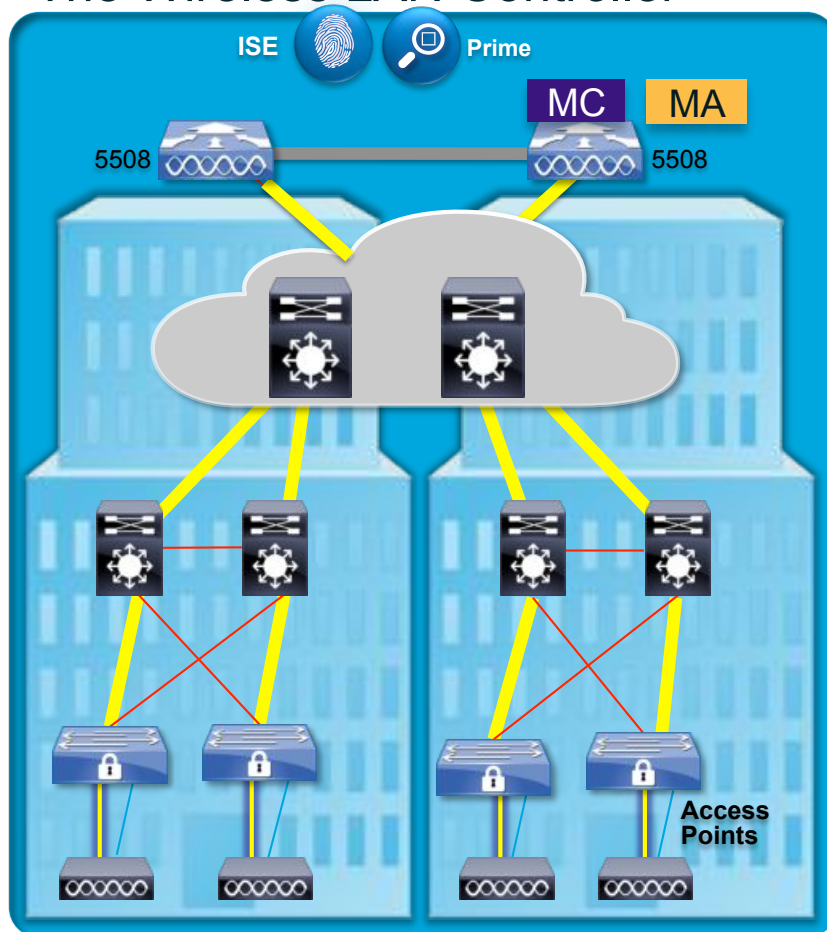
Known Deployment Model

- **Wireless is an Overlay Network**
- **Software components within the WLC today:**

- **Mobility Agent (MA) is responsible for:**
  - AP CAPWAP termination
  - Maintaining client database
  - Policy enforcement

- **Mobility Controller (MC) is responsible for:**
  - Client Mobility
  - Radio Resource Management (RRM)
  - WiPS, Spectrum Management

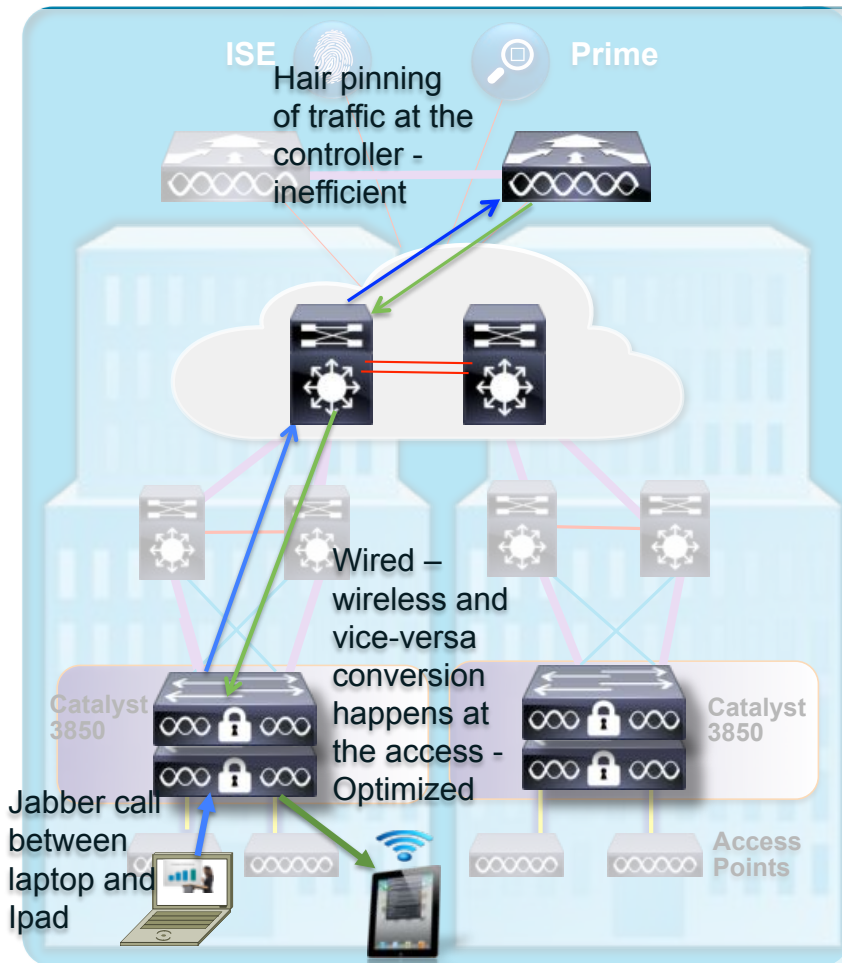Inter--Controller EoIP/CAPWAP tunnel
AP-Contoller CAPWAP tunnel

Better Scale and Bandwidth with Converged Access

Separation of MA and MC

ISE   Prime

MC

MA

5508 or
WISM2 with
SW Upgrade
or new 5760

MC

MA

New
Catalyst
3850

Catalyst
3750

Access
Points

- Traditional Controllers continue to play MA and MC

- Catalyst 3850 can play the role of both MA and MC
  - Valid for Branch and small-medium campus type deployments

- Moving the MA only to the Catalyst 3850 (typically in large campus) helps with:
  - Improved Scalability – larger mobility domains
  - Increased wireless bandwidth
  - Uniform wired/wireless policy enforcement

━━━ **AP Capwap Tunnels**   ━━━ **Mobility Tunnels**

Better Network Utilization with Unicast Optimization

ISE   Prime

Hair pinning of traffic at the controller - inefficient

Wired – wireless and vice-versa conversion happens at the access - Optimized

Catalyst 3850

Catalyst 3850

Access Points

Jabber call between laptop and Ipad

Wired Traffic   **Wireless Traffic**

Unicast with Traditional Deployments
- All wired-wireless (and vice-versa) conversion happens at the controller.
- Leads to hair-pinning
- Entire network traversed even for peer-to-peer traffic (wired-wireless or wireless-wireless) on the same switch

Unicast Optimization with Converged Access
- Wired-wireless conversion (and vice versa) happens at the 3850 switch
- Reduces the number of streams in the network and avoids hair-pinning - Optimized

Scalable Multicast Deployments
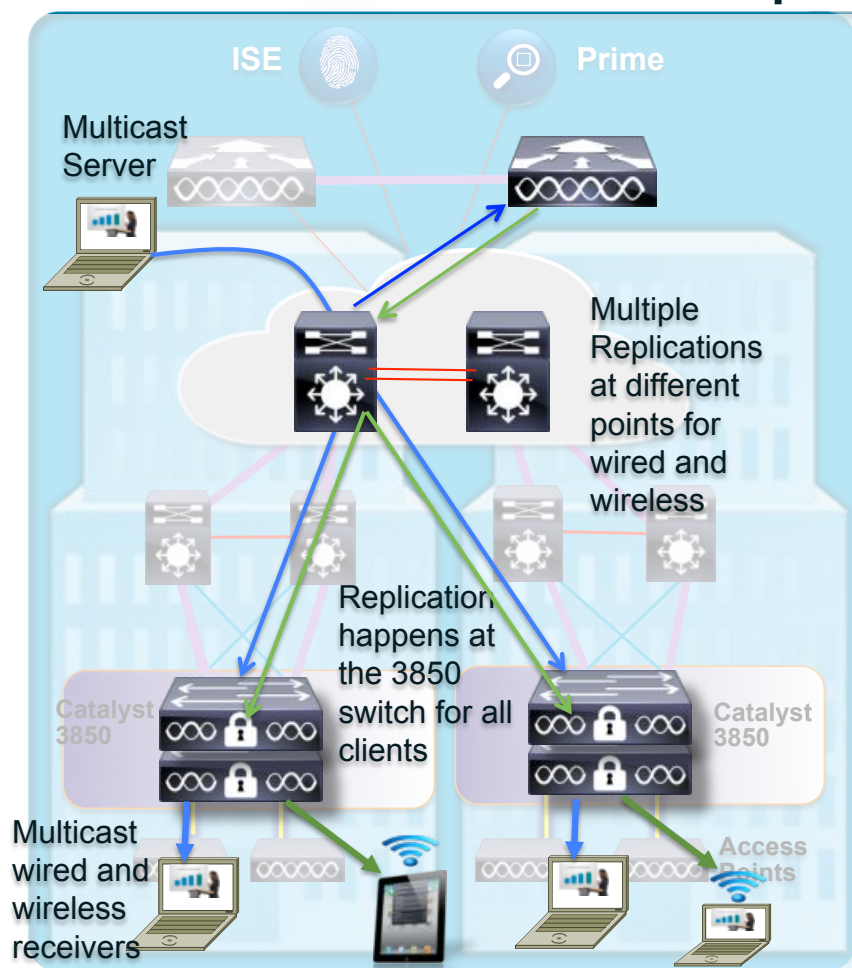
Multicast with Traditional Deployments (Multicast-Multicast mode)

• Wired Multicast Replication happens at the switch
• Wireless Multicast Replication happens at the Controller

Multicast Optimization with Converged Access

• Wired and Wireless Multicast Replication happens at the 3850 switch
• Reduces the number of streams for the same traffic type in the network

Labels within diagram:

ISE — Prime
Multicast Server
Multiple Replications at different points for wired and wireless
Replication happens at the 3850 switch for all clients
Catalyst 3850
Catalyst 3850
Multicast wired and wireless receivers
Access Points

— Wired Multicast Traffic   — Wireless Multicast Traffic

Cisco Innovation 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

Complete Your Paper "Session Evaluation"

Give us your feedback and you could win 1 of 2 fabulous prizes in a random draw.

Complete and return your paper evaluation form to the room attendant as you leave this session.

Winners will be announced today. You must be present to win!

..visit them at BOOTH# 100

Thank you.

Be sure to follow us on Twitter at *#CiscoConnect_TO*

‖‖‖‖ ‖‖‖‖
CISCO