

Co vše umí dnešní přístupová vrstva sítě

T-NET1, T-NET2 / L3

Radek Boch, Systems Engineer Cisco
rboch@cisco.com
CCIE #7095

Prosíme, ptejte se nás

- Twitter www.twitter.com/CiscoCZ
- Talk2cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600



What is an intelligent Access Switch ?

Traditional Switch



VS.

Intelligent Access Switch



When the Network Access Knows

When the Network Access Knows

Intelligent Access – Emerging Requirements



Mobility

Convergence of
wired and wireless



Green

Rising energy costs,
corporate
sustainability
mandates



Security

Provide secure
access while
managing explosive
growth in number of
devices accessing
the network



Application Performance

Need to closely
manage applications
for optimum
performance



Voice/Video

Growth of video
outstripping growth
of access network
resources

Simplify Operations, reduce management complexity

Where are we evolving from

Today's Connectivity Model

- What have we built our network access to do?
- Provide Connectivity
- Be Highly Available (spanning tree best practices)
- Implement VLAN's to isolate traffic (e.g. voice vs. data)
- Implement QoS to support phones
- Security (where we can)

```
interface FastEthernet0/24
switchport access vlan 100
switchport mode access
switchport voice vlan 200
!
switchport port-security maximum 2
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
!
srr-queue bandwidth share 10 10 60 20
queue-set 2
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qosvoipcisco-phone
!
macro description cisco-phone
!
spanning-tree portfast
spanning-tree bpduguard enable
!
service-policy input AutoQoS-Police-CiscoPhone
```

} Voice and Data VLAN's

} L2 DoS Mitigation

} QoS – Trust traffic coming from the phone

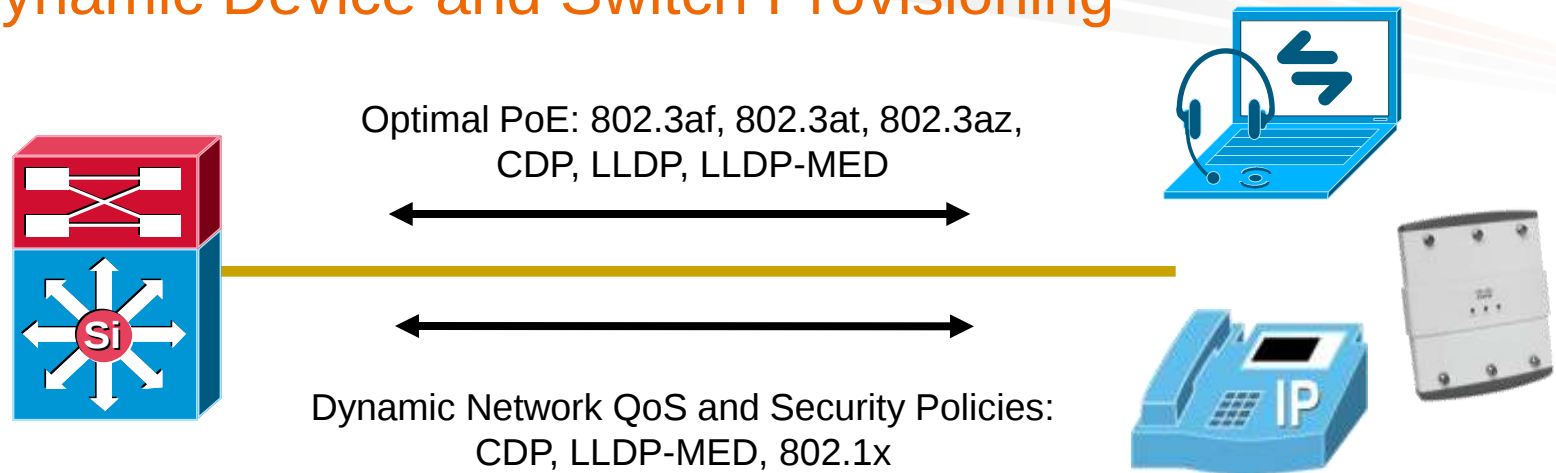
} Smartports

} Spanning Tree Tuning

} QoS

Evolving Network Services

Dynamic Device and Switch Provisioning



- Plug and play provisioning of edge devices (phones, UC applications and APs) necessary to manage operational overhead

Power negotiation / mgmt
VLAN configuration
802.1x interoperation
QoS configuration
Security configuration

The end devices relationship to the network is changing and we need an Intelligence at the edge of the network to be able to support the evolving requirements

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond**

- Energy Efficient Ethernet

- EnergyWise

- StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED

- Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

- Auto-Smartports & Smartinstall

- Netflow / Flexible Netflow

- GOLD



Why PoE in the access layer

- Ease of deployment

Using a single cable for data and power

- Centralized Power Management

EnergyWise, Energy Efficient Ethernet

- High availability

Centralized power backup, continuous operations

Power supply redundancy is built into most network architectures

Backup UPS power is used in most enterprise campus

- Minimize TCO



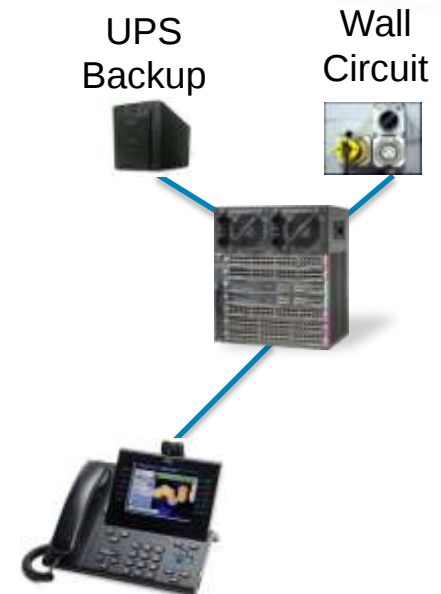
Cheap and inefficient power bricks

- Power efficiency

Bulk power supply is more efficient than cheaper power bricks

Bulk power supply efficiency curve is optimized for avg. utilization

Bulk power supply is less expensive compared to individual power brick per end device



Power Over Ethernet

Cisco Pre-Standard and 802.3af-2003



- Cisco pre-standard devices initially receive 6.3W and then optionally negotiate via CDP
- IEEE 802.3af ratified 2003

- **Specifications**

Cable Guidelines: Cat3 and Cat5/5e/6

Current level: 350mA

Voltage: PSE from 44-57 DC

Maximum power output: PSE 15.40W output

Maximum power input: PD is 12.95W input

Supported Modes: Mode A (data-pairs), Mode B (spare-pairs)

- Power negotiation is '*optional*' behavior for 802.3af devices



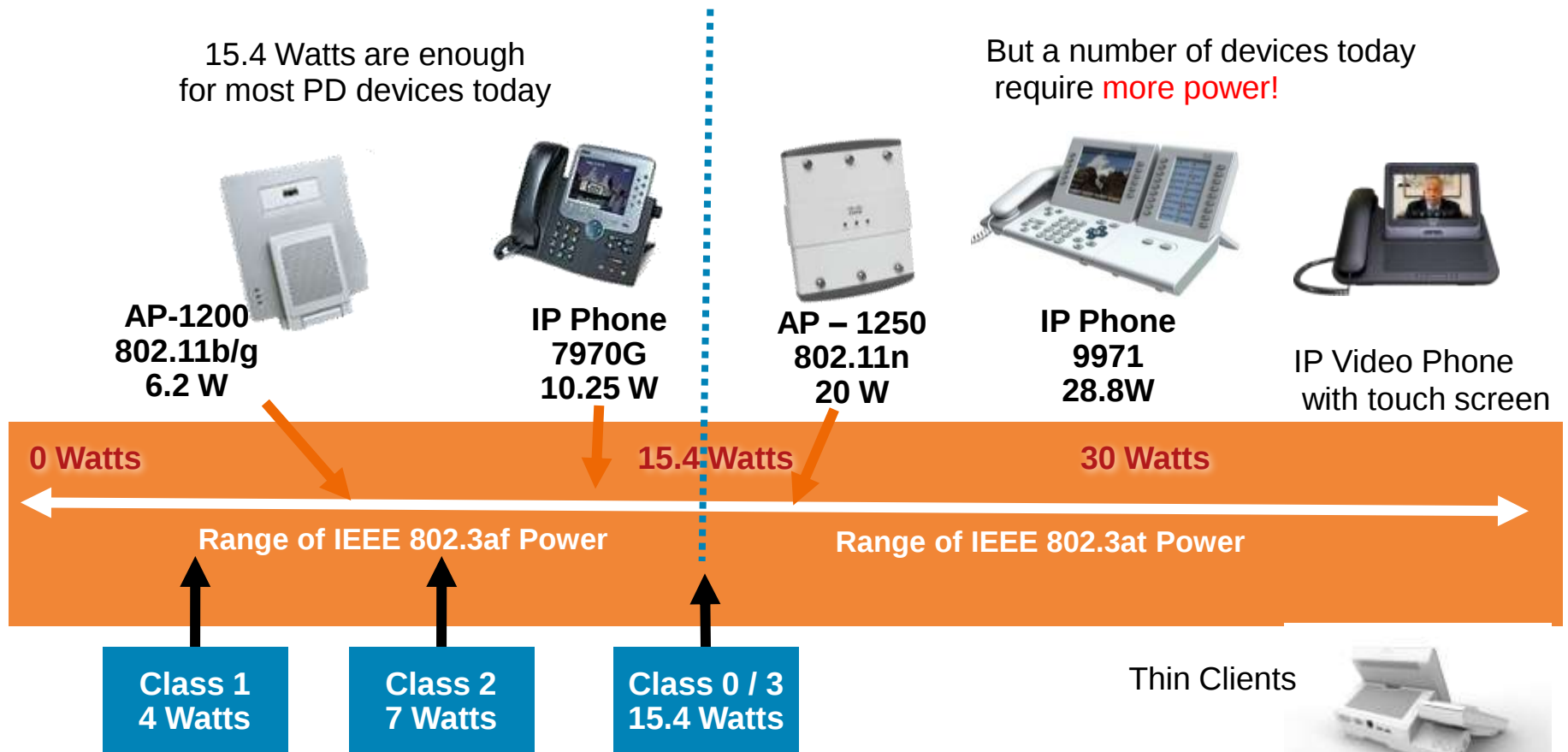
Evolving Layer 1 Services

Why do we need 802.3at (PoE+)

- Endpoint power requirements are increasing
- Green initiatives
- Need for Granular power negotiation 'and' increased power

15.4 Watts are enough
for most PD devices today

But a number of devices today
require **more power!**



Power Over Ethernet

IEEE 802.3at (PoE+)



- IEEE 802.3at ratified Sep.2009

- **Specifications**

Cable Guidelines: Cat5e or beyond

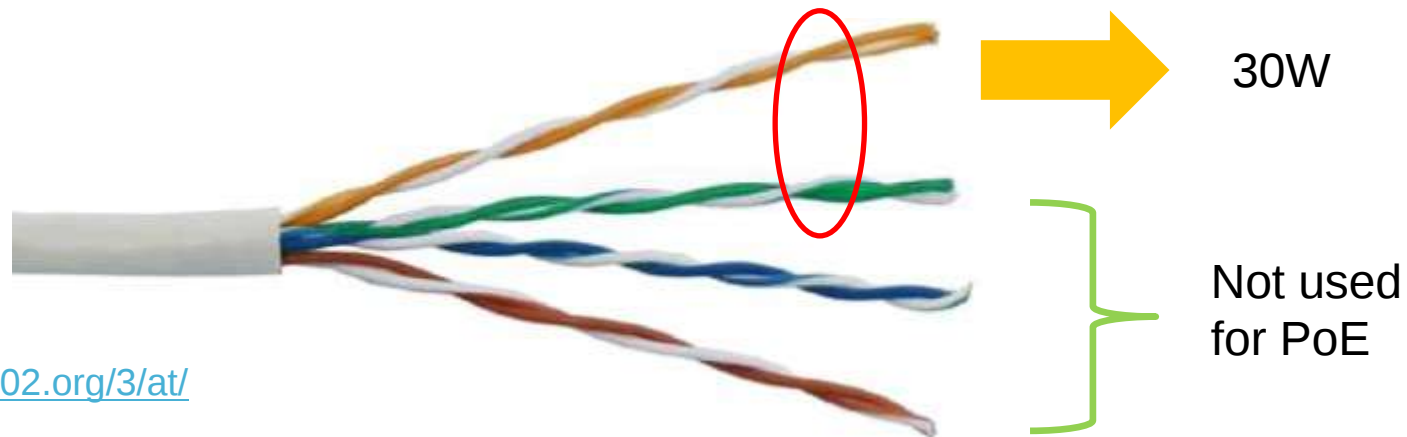
Current level: 600mA assuming cable 50° C or lower

Voltage: PSE from 50V to 57V

2-pair medium power output: PSE 30W output

Maximum power input: PD is 25.5W input

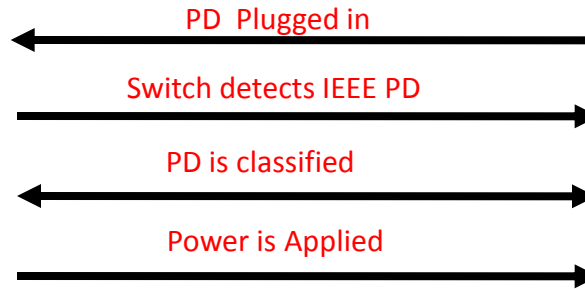
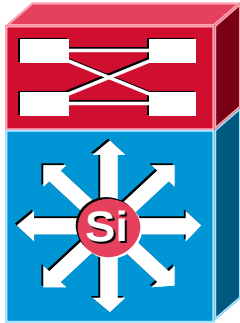
Supported Modes: Mode A (data-pairs) or Mode B (spare-pairs)



Source: <http://www.ieee802.org/3/at/>

Power over Ethernet

Detect, Classification & Power Up



1. It's a IEEE PD
2. PD Classified
3. Power Up

Class	Usage of class	Minimum Power Levels Output at the PSE	Maximum Power Levels at the Powered Device	Class description
0	Default	15.4W	0.44 to 12.95W	Classification unimplemented
1	Optional	4.0W	0.44 to 3.84W	Very Low Power
2	Optional	7.0W	3.84 to 6.49W	Low Power
3	Optional	15.4W	6.49 to 12.95W	Mid Power
4	Reserved in 802.3af	Treat as Class 0		
4	802.3at	30W	12.95W – 25.5W	High Power

Introducing Universal PoE (UPoE)

Using 4 pairs simultaneously



- Does not violate any safety specifications from cabling standards
- As simple as two independent PoE+ connections
- Specifications

Cable Guidelines: Cat5e or beyond

Current level: 600mA assuming cable 50° C or lower

Voltage: PSE from 50V to 57V

2-pair medium power output: PSE 30W output

Maximum power input: PD is 51W input

Mode: Combines Mode A (data-pairs) and Mode B (spare-pairs)

Cabling and Heating



- TIA TR42 and ISO IEC are the two standards followed for structured cabling in enterprise
- Both committees studied temperature rise on PoE powered cables
 - Used a cable bundle of 100 cables, standard Cat5e
 - Used worst case scenario of cable passing through conduits
 - All study was done with all conductors in the cable powered

TIA TR-42 Recommendation

Temperature Rise	Max Current per twisted Pair	Max Power @ 50V
5	420mA	37.5W
7.5	520mA	45.2W
10	600mA	51.0W
12.5	670mA	55.8W
15	720mA	59.0W

ISO/IEC Recommendation

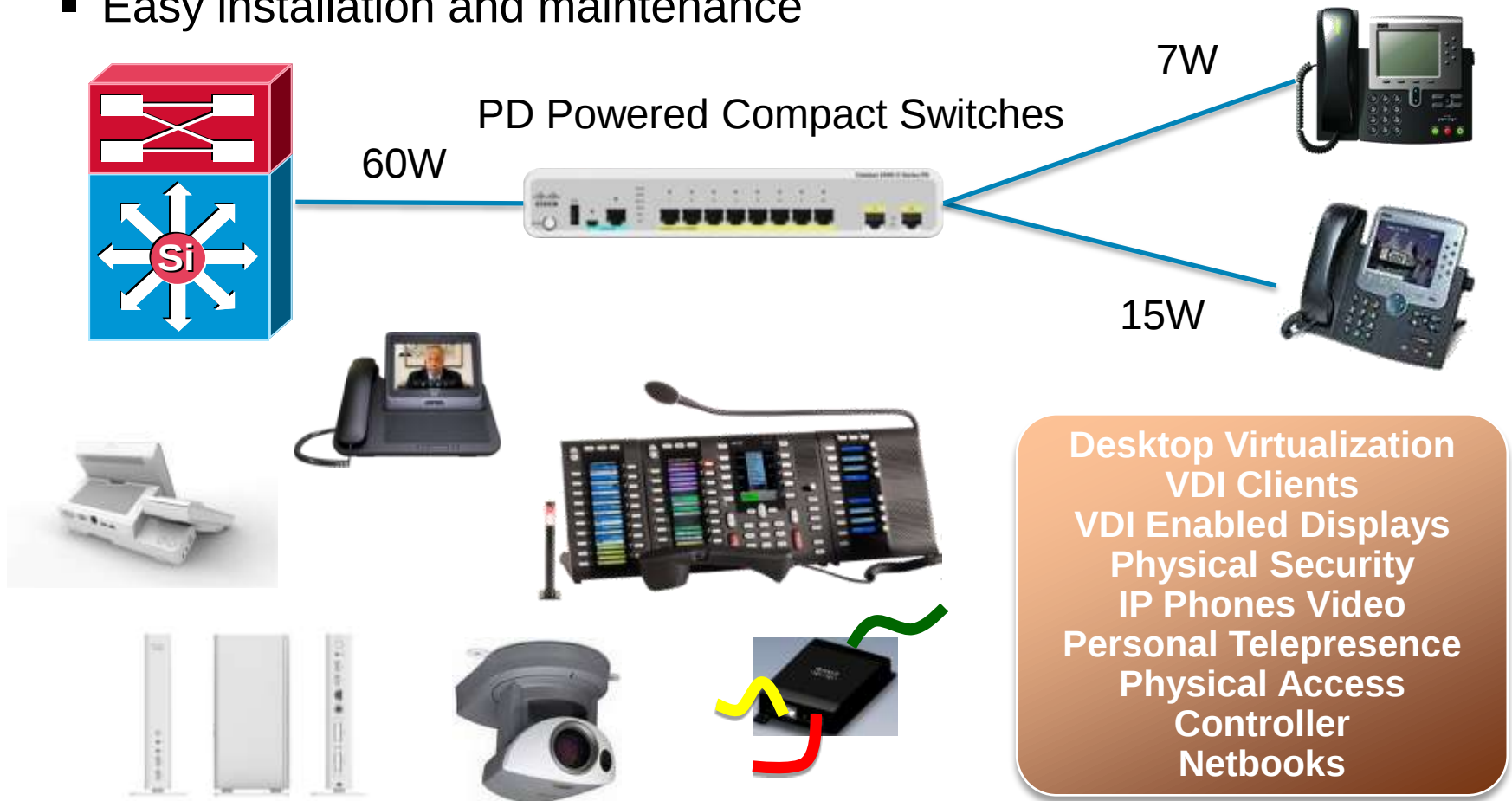
Temperature Rise	Max Current per twisted Pair	Max Power @ 50V
5	420mA	37.5W
7.5	550mA	47.4W
10	600mA	51.0W
12.5	680mA	56.4W
15	720mA	59.0W

Standard cables are rated to 60C and ambient temperature for cables are not expected to exceed 50C

Universal PoE (UPOE)

Applications

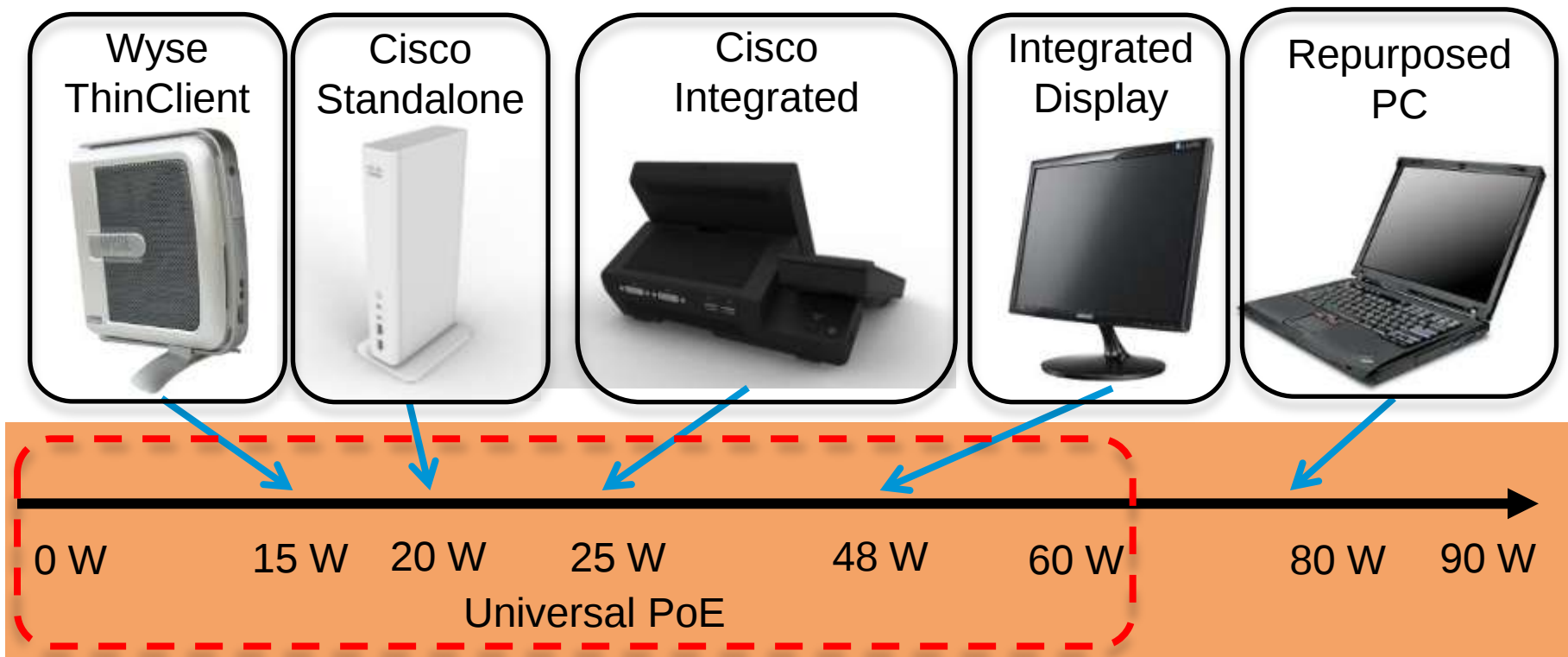
- Support applications that require high availability, e.g. 911 calls
- Minimize cabling into Workspace
- Easy installation and maintenance



Use case for UPoE

VDI Clients

- Clients consume lower power. Thin clients consume less than thick clients
- Amendable to Power Management





PoE Supported Products

Products	802.3af (15W)	EPoE (20W)	802.3at (30W)	UPOE (60W)
Catalyst 2960	Yes	No	No	No
Catalyst 2960S	Yes	Yes	Yes	No
Catalyst 3560E/3750E	Yes	Yes	No	No
Catalyst 3560X/3750X	Yes	Yes	Yes	No
Catalyst 4500	Yes	4648-RJ45V+E	4748-RJ45V+E	4748-UPOE+E
Catalyst 6500	Yes	6148-GE-AF 6548-GE-AF	6148E-GE-45AT	No

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

PoE – 802.3af, 802.3at and beyond

Energy Efficient Ethernet

EnergyWise

StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

CDP, LLDP, LLDP-MED

Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

Auto-Smartports & Smartinstall

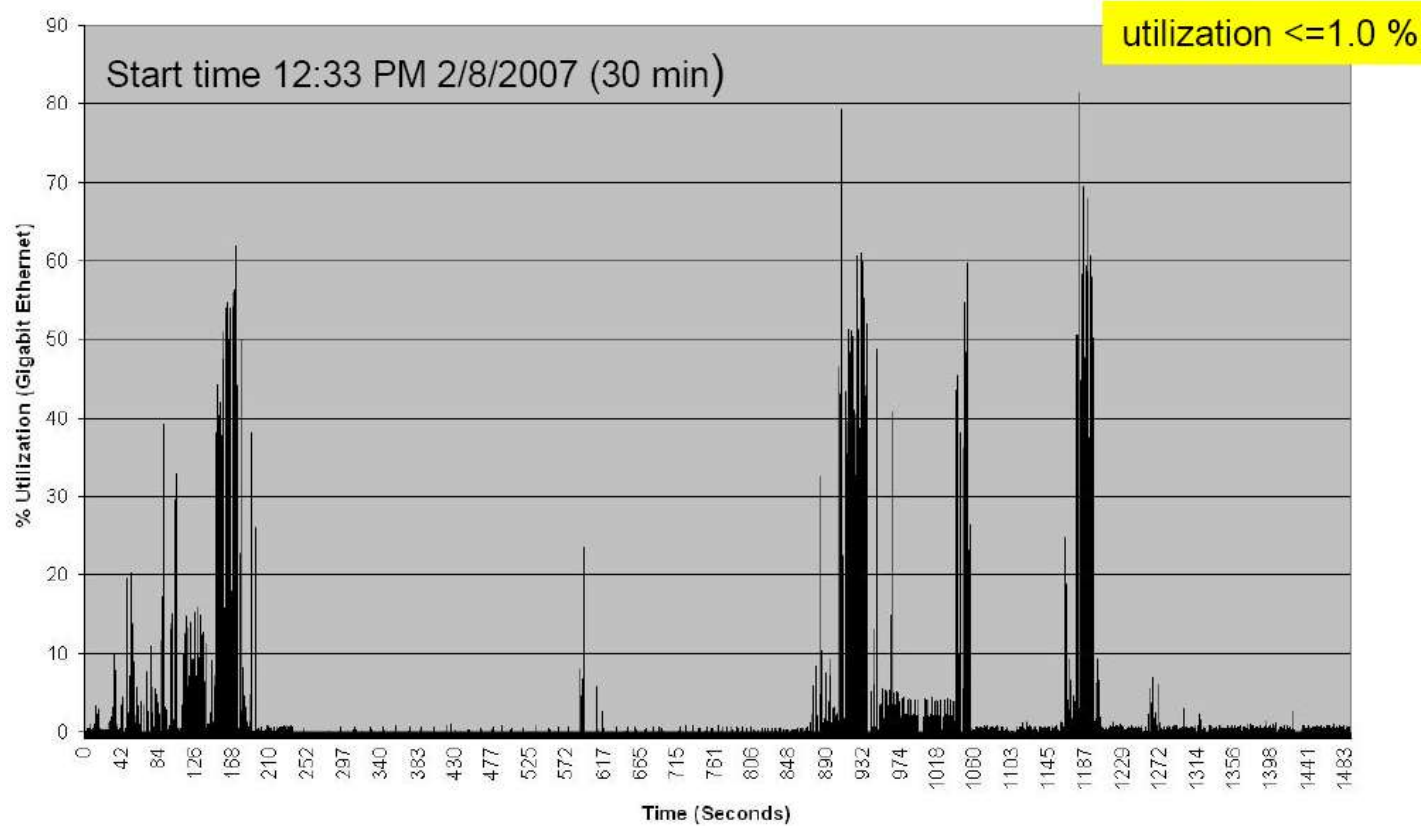
Netflow / Flexible Netflow

GOLD



Why Energy Efficient Ethernet?

Time vs. Utilization of File Server with 1G Ethernet link (Trace from LBNL)



Active



PHYs transmit Idles
when there is no
Data to send

Evolving Power Optimizations

802.3az: Energy Efficient Ethernet (EEE)

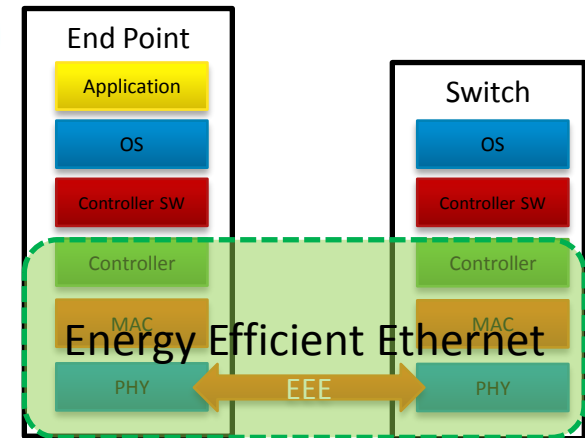
- IEEE 802.3az – Timeline

Working Group Ballot – July 2009

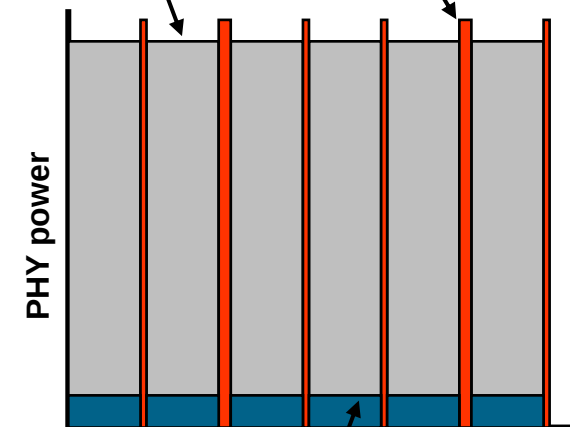
Sponsor Ballot – March 2010

Standard – Nov 2010

- Power down the PHYs during when there is no data to send
- During power-down, maintain coefficients and synchronization to allow rapid return to active state
- Asymmetric mode of operation
 - Transmit and receive circuits function independently

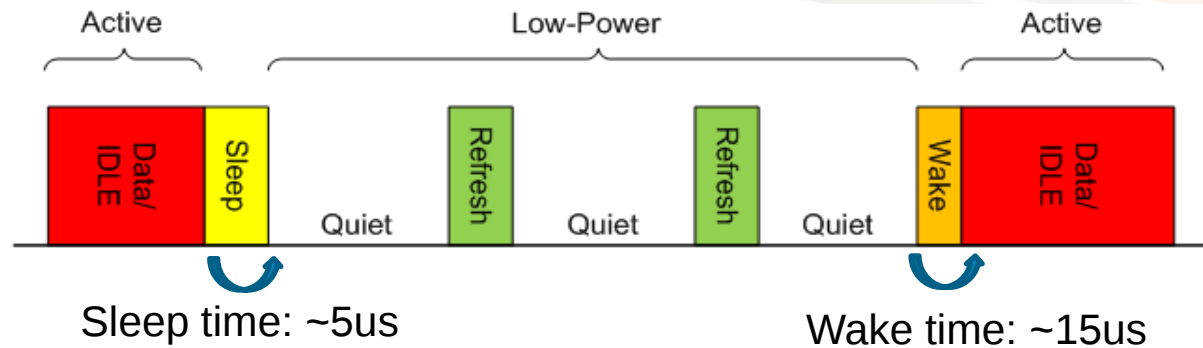


Current PHY idle power PHY active power



802.3az EEE PHY idle power

Operating States and MDI Signaling



Term	Description
Active State	Existing state used for data transmission when either data packets or Idle symbols are transmitted
Low Power state	New state used during periods of no data transmission to allow system power reduction between data packet bursts.

Term	Description
Sleep	Signal to inform link partner of entry into low power state
Quiet	No signal transmitted
Refresh	Periodic signal during low power state for PHY to maintain timing recovery and/or filter coefficients
Wake	Signal to inform link partner of entry back into active state

Linecard to support UPoE and EEE



WS-X4748-UPOE-RJ45V+E

- 60W PoE with max. line card budget of 1500W
- LLDP enhancement to negotiate beyond 30W
- Compliant with IEEE 802.3az for: 100/1000 Base-T
- Power consumption is based on link utilization

- Power down the PHYs during when there is no data to send
- During power-down, maintain coefficients and synchronization to allow rapid return to active state
- Asymmetric mode of operation
 - Transmit and receive circuits function independently

1 Gbps Port Power Consumption

No EEE	EEE
1.0 W	0.47W

50% Power Savings



Energy Efficient Ethernet - Configuration

Determine EEE Capability

```
Switch# show interface gi 1/2 capabilities
GigabitEthernet1/2
  Model:          WS-X4748-UPOE+E-RJ-45
  Type:           10/100/1000-TX
  Speed:          10,100,1000,auto
  Duplex:          half,full,auto
  Auto-MDIX:       yes
  EEE:             yes ( 100-Tx and 1000-T auto mode )
```

Configure EEE

```
Switch# conf t
Switch(config)# int gi 1/2
Switch(config-if)# power efficient-ethernet auto
```

Verify EEE

```
Switch# show platform software interface gi 1/2 status
Switch Phyport Gi1/2 Software Status
EEE: Operational
```

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

PoE – 802.3af, 802.3at and beyond
Energy Efficient Ethernet

EnergyWise

StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

CDP, LLDP, LLDP-MED

Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

Auto-Smartports & Smartinstall

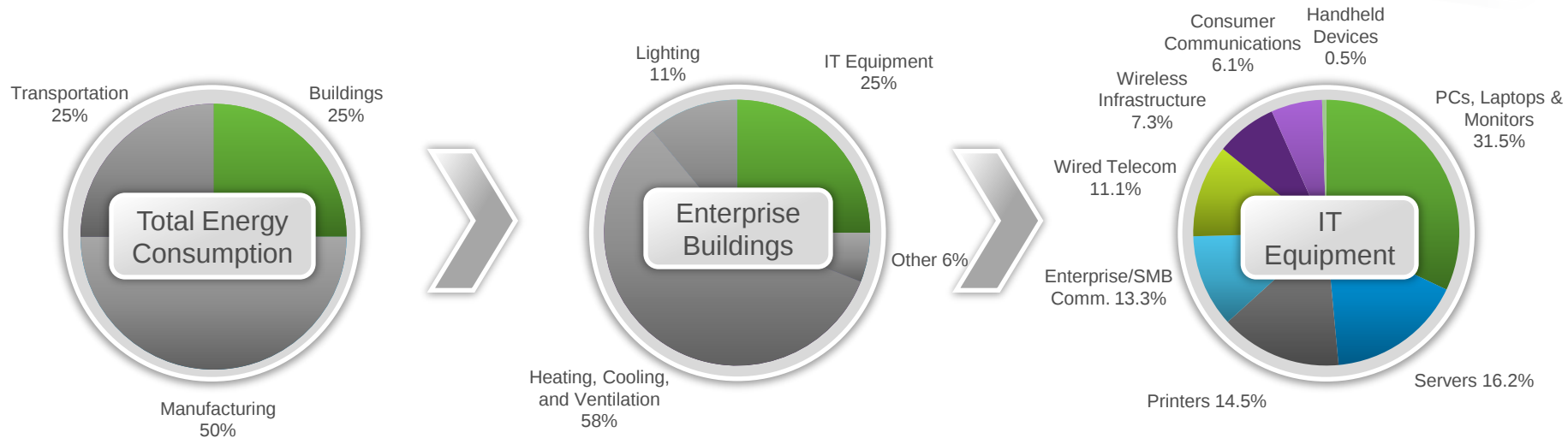
Netflow / Flexible Netflow

GOLD



Energy Operational Costs

Opportunity in Enterprise IT



Cost Savings

- Rising energy costs
- IT device proliferation
- Video applications

Sustainability Mandates

- Regulatory compliance
- Government mandates
- Company requirements

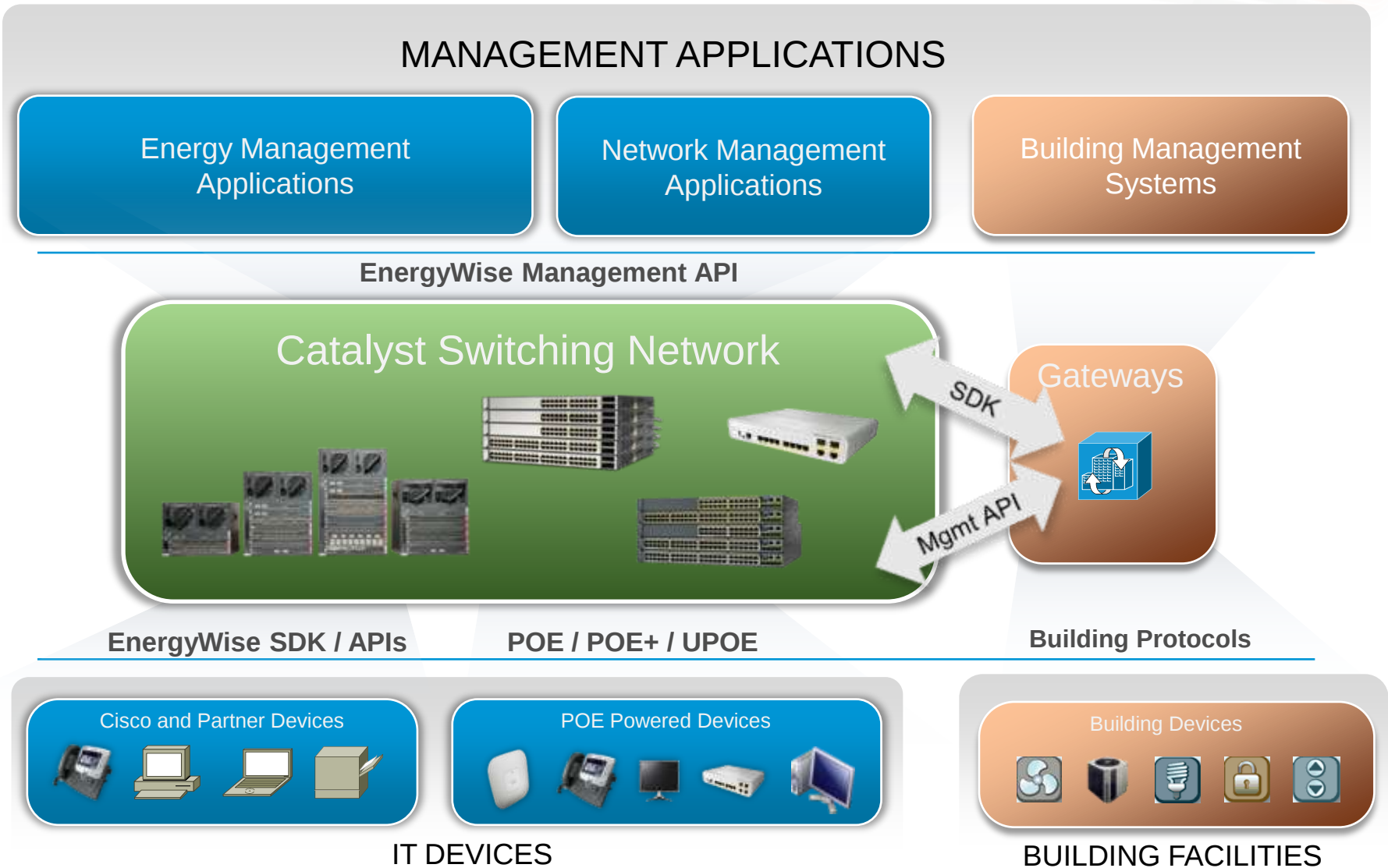
Source: BOMA 2006, EIA 2006, AIA 2006

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.

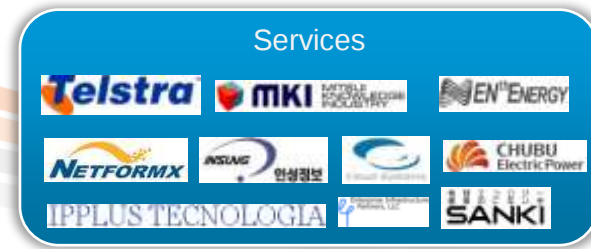
Cisco EnergyWise Architecture

Unifies Device Energy Management

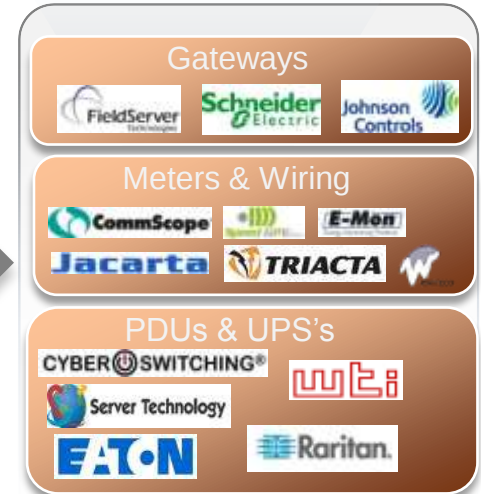
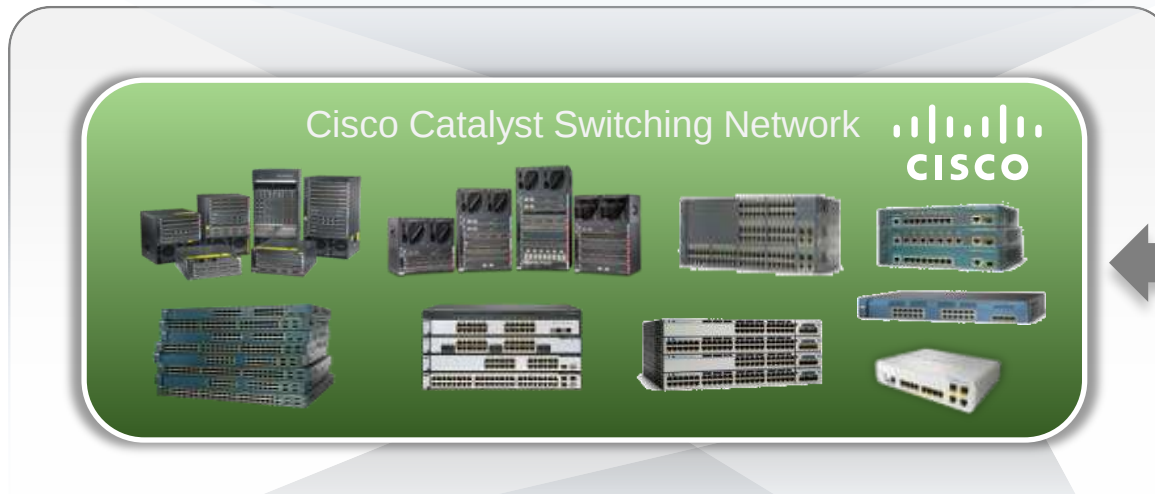


Cisco EnergyWise Architecture

Unifies Device Energy Management



MANAGEMENT APPLICATIONS

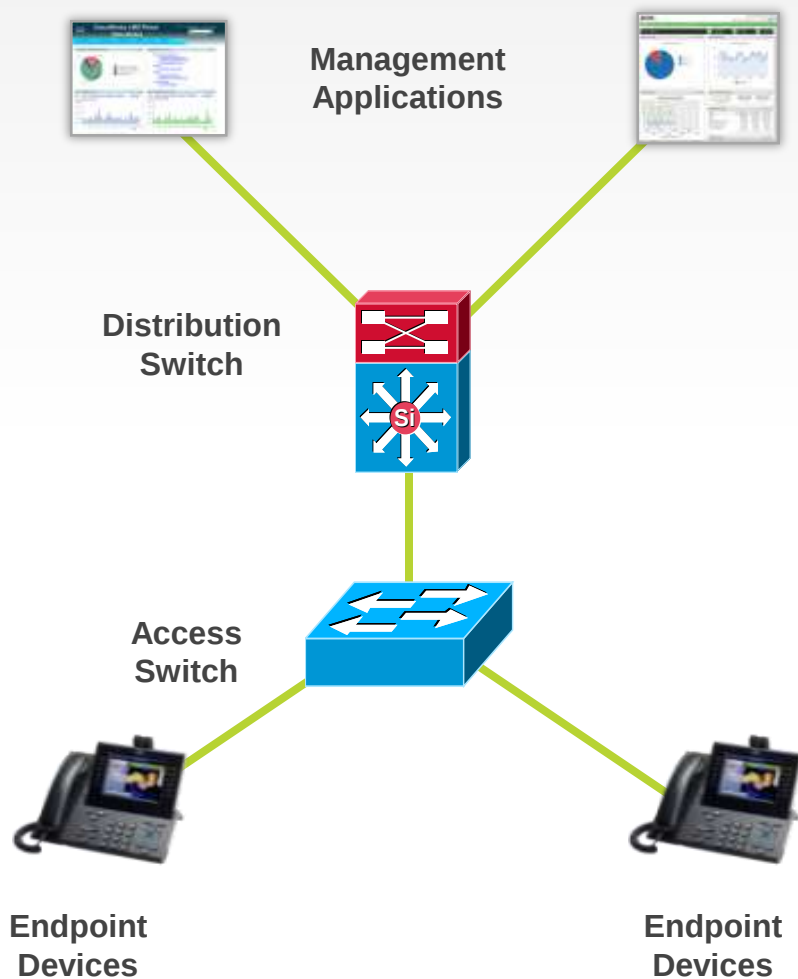


IT DEVICES

BUILDING DEVICES

EnergyWise Technology

Network-Based Energy Management

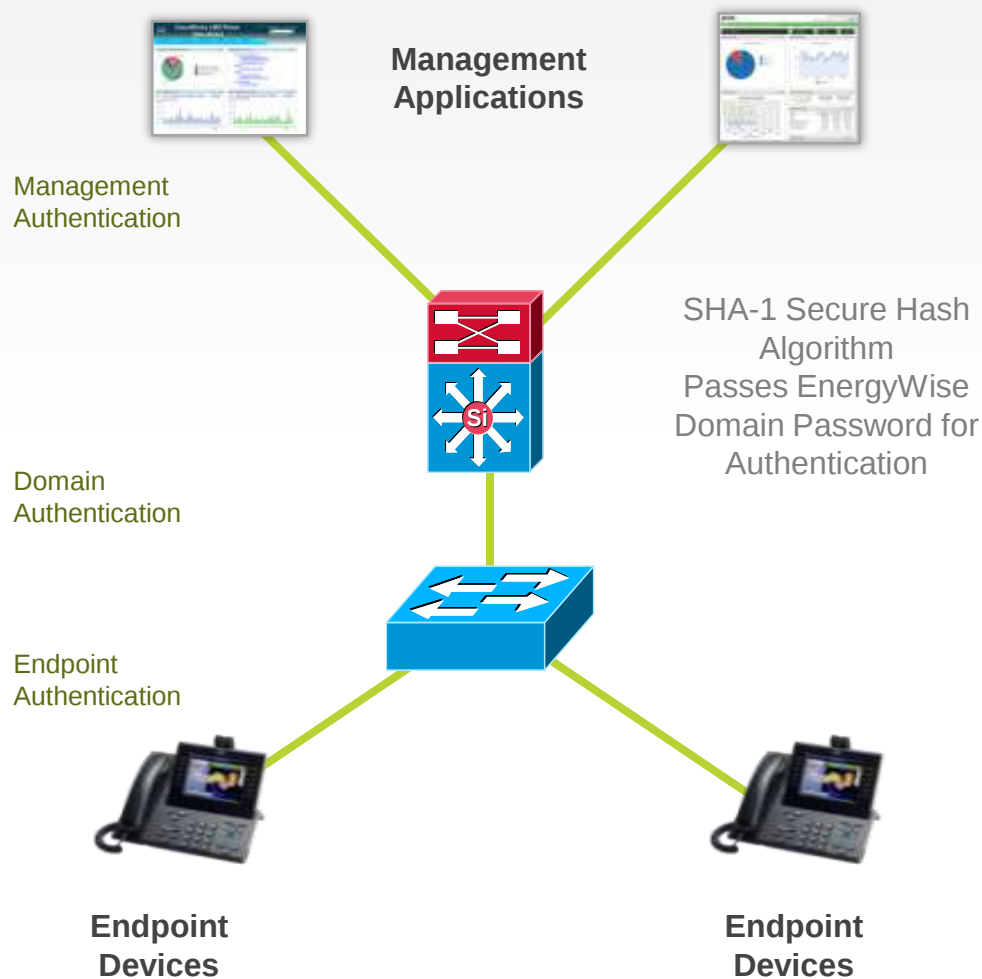


Process:

1. **Secure Authentication**
2. Auto-discover devices
3. Collect energy consumption
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management

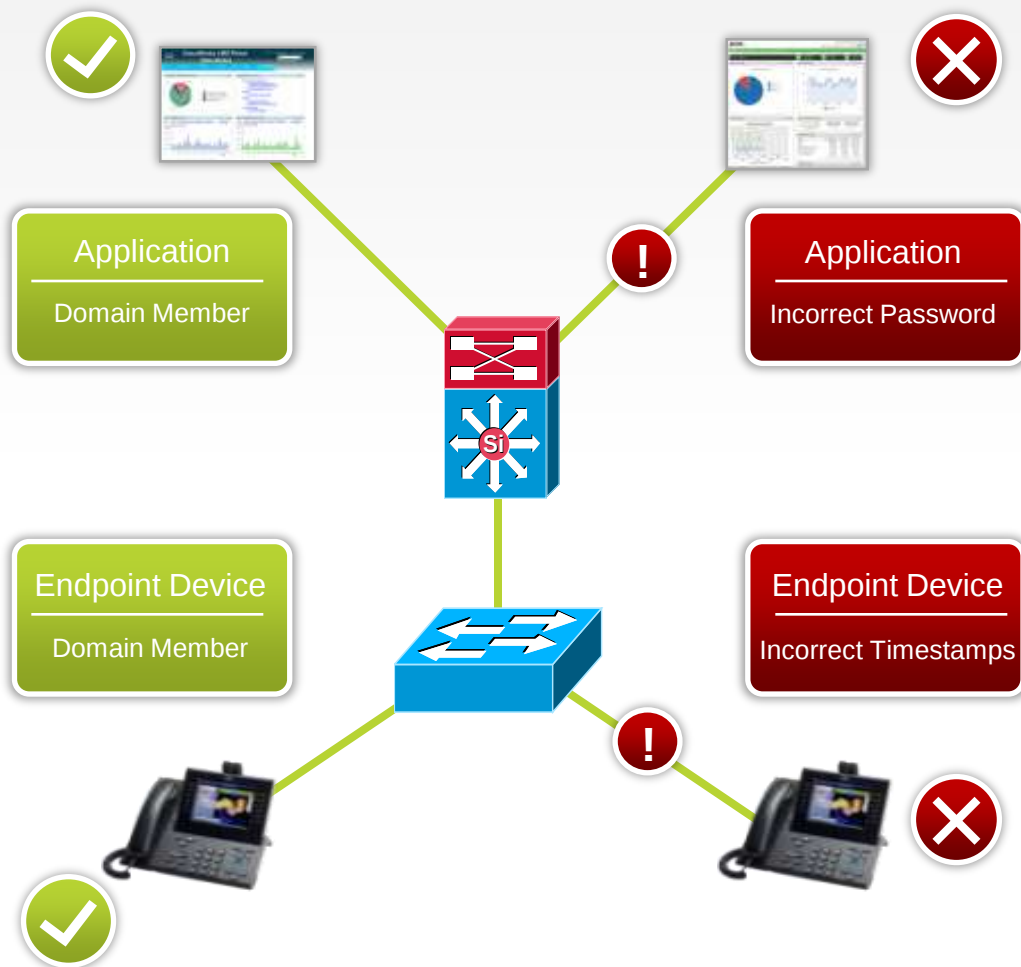


Process:

1. **Secure Authentication**
2. Auto-discover devices
3. Collect energy consumption
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management

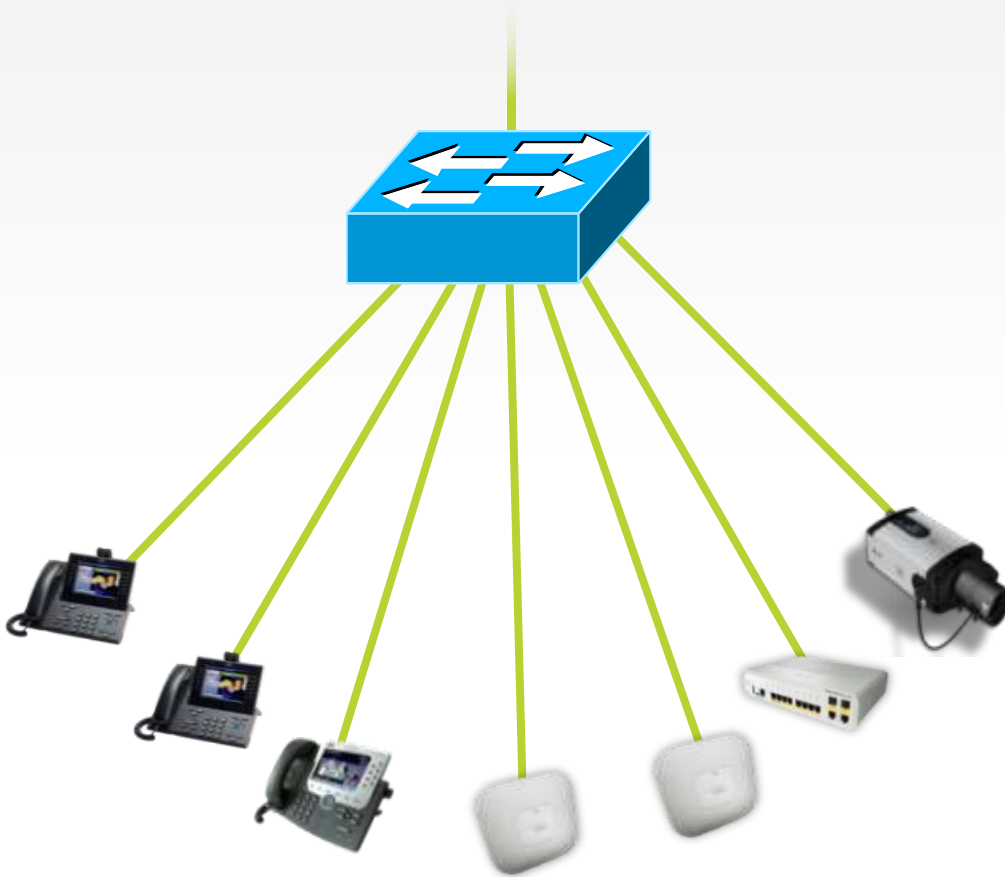


Process:

1. Secure Authentication
2. Auto-discover devices
3. Collect energy consumption
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management

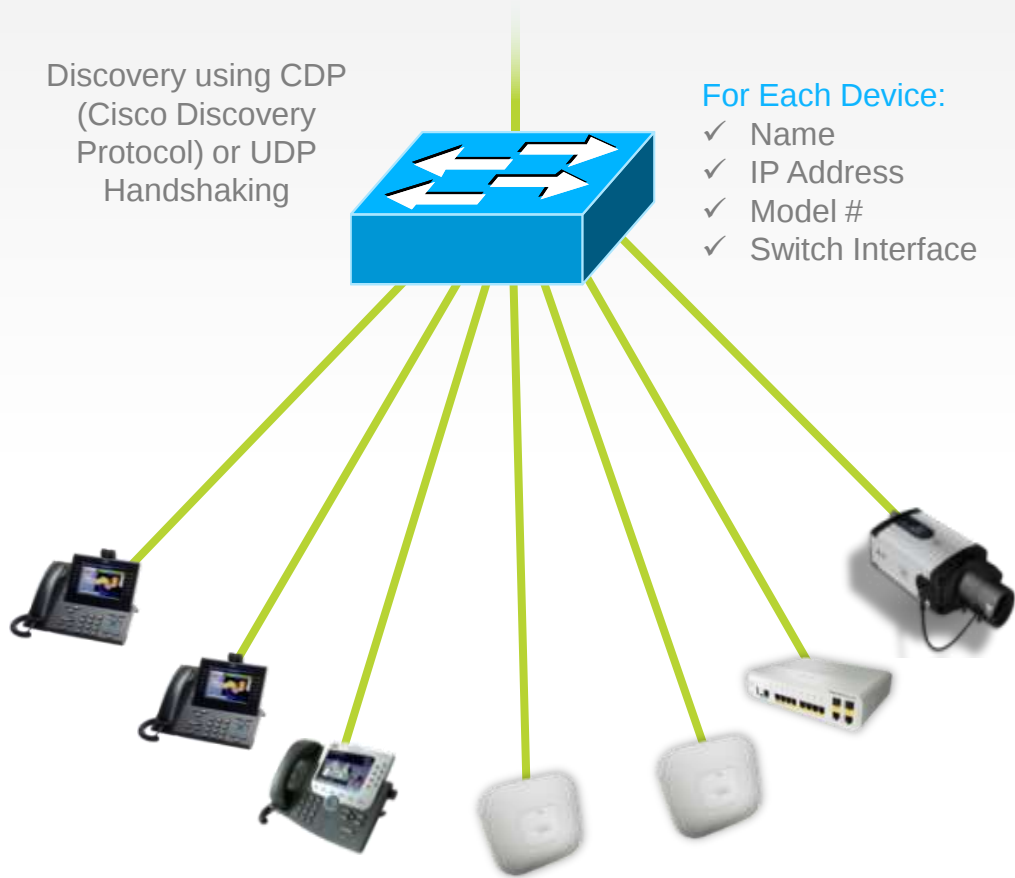


Process:

1. Secure Authentication
- 2. Auto-discover devices**
3. Collect energy consumption
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management

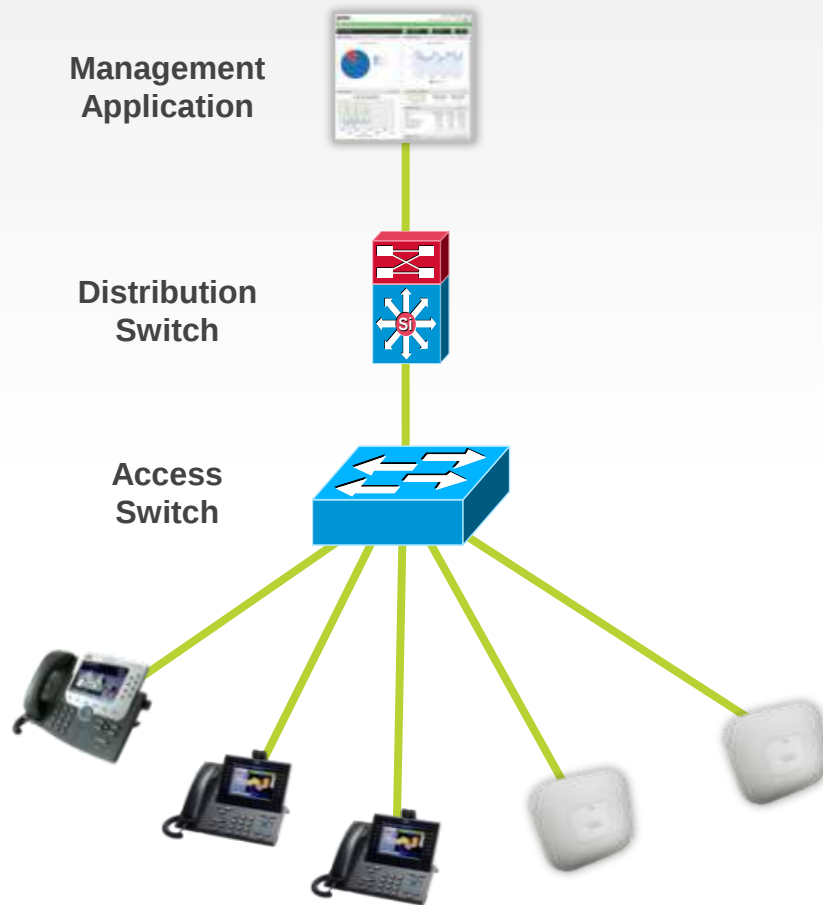


Process:

1. Secure Authentication
- 2. Auto-discover devices**
3. Collect energy consumption
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management



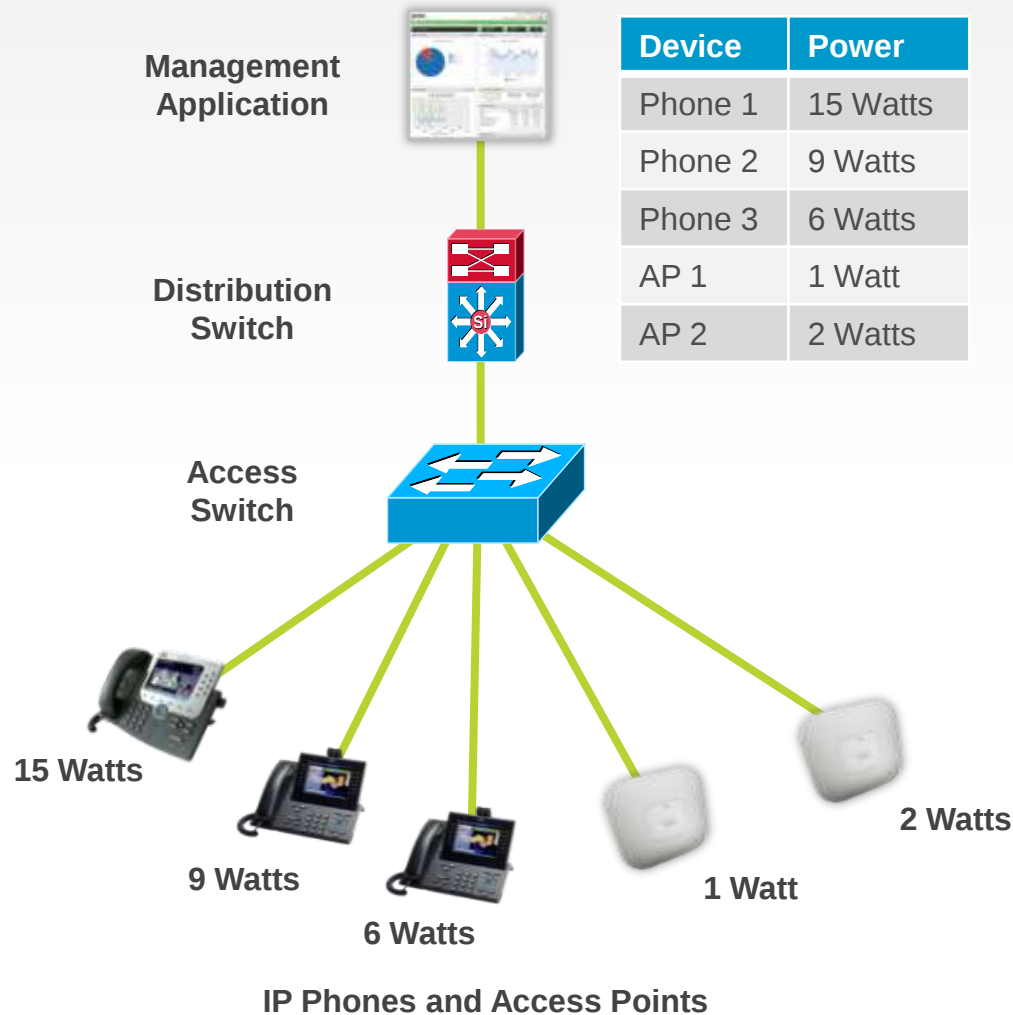
IP Phones and Access Points

Process:

1. Secure Authentication
2. Auto-discover devices
- 3. Collect energy consumption**
4. Set power level modes
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management



Process:

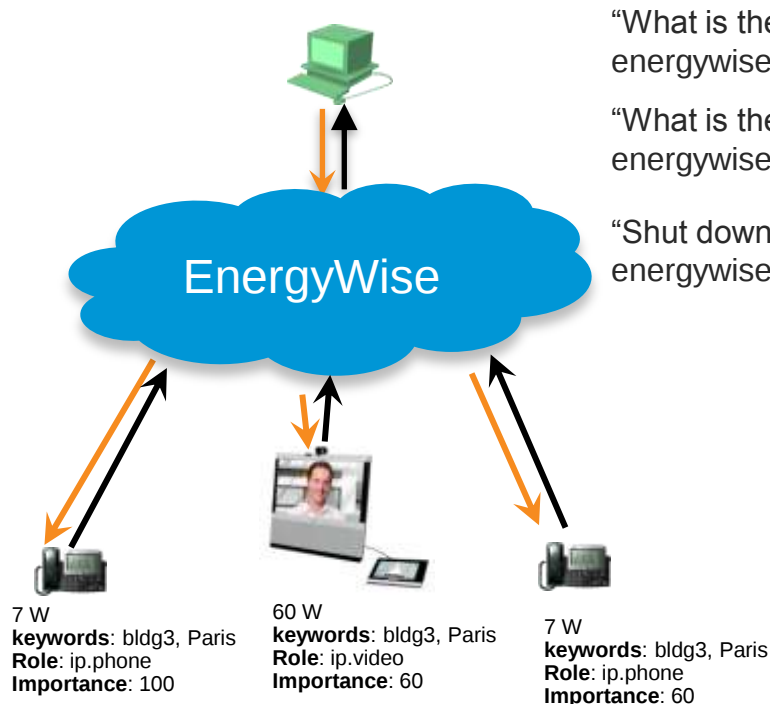
1. Secure Authentication
2. Auto-discover devices
- 3. Collect energy consumption**
4. Set power level modes
5. Configure Time of Day Policies

ICT Energy Management

Cisco EnergyWise

Services:

- **Finely** Measure (per device, per type of device, per location)
- Control (per device, or group of devices, granular power level 0-10)
- Organize (keywords, name, role, importance, business impact)
- Optimize and Report



“What is the total power usage in Paris?”

energywise query importance 100 keyword paris name * sum usage

“What is the power usage of all video endpoints?”

energywise query importance 100 keyword ip.video name * sum usage

“Shut down non-critical equipment in Paris”

energywise query importance 60 keyword paris name * set level 0

***A new paradigm
in Energy Management!***

Displaying Usage

```
c2960S-1#show energywise usage
```

Interface	Name	Usage	Category	Caliber
-----	----	-----	-----	-----
	c2960S-1-1	81.0 (W)	consumer	max
Gi1/0/4	SEP000E84C063C1	1.9 (W)	consumer	actual
Gi1/0/5	PVC300-1	4.4 (W)	consumer	actual
Gi1/0/6	Gi1.0.6	2.1 (W)	meter	actual
	SEP5475D02B3F46	6.0 (W)	consumer	presumed
Gi1/0/7	Gi1.0.7	6.0 (W)	meter	actual
	SEP8CB64FF6723F	8.8 (W)	consumer	presumed
Gi1/0/8	Gi1.0.8	2.2 (W)	meter	actual
	SEP5475D02B40BE	6.0 (W)	consumer	presumed
Gi1/0/10	Gi1.0.10	6.1 (W)	meter	actual
	SEPC0626B62AE93	8.8 (W)	consumer	presumed

```
Total Displayed: 11      Usage: 116.9
```

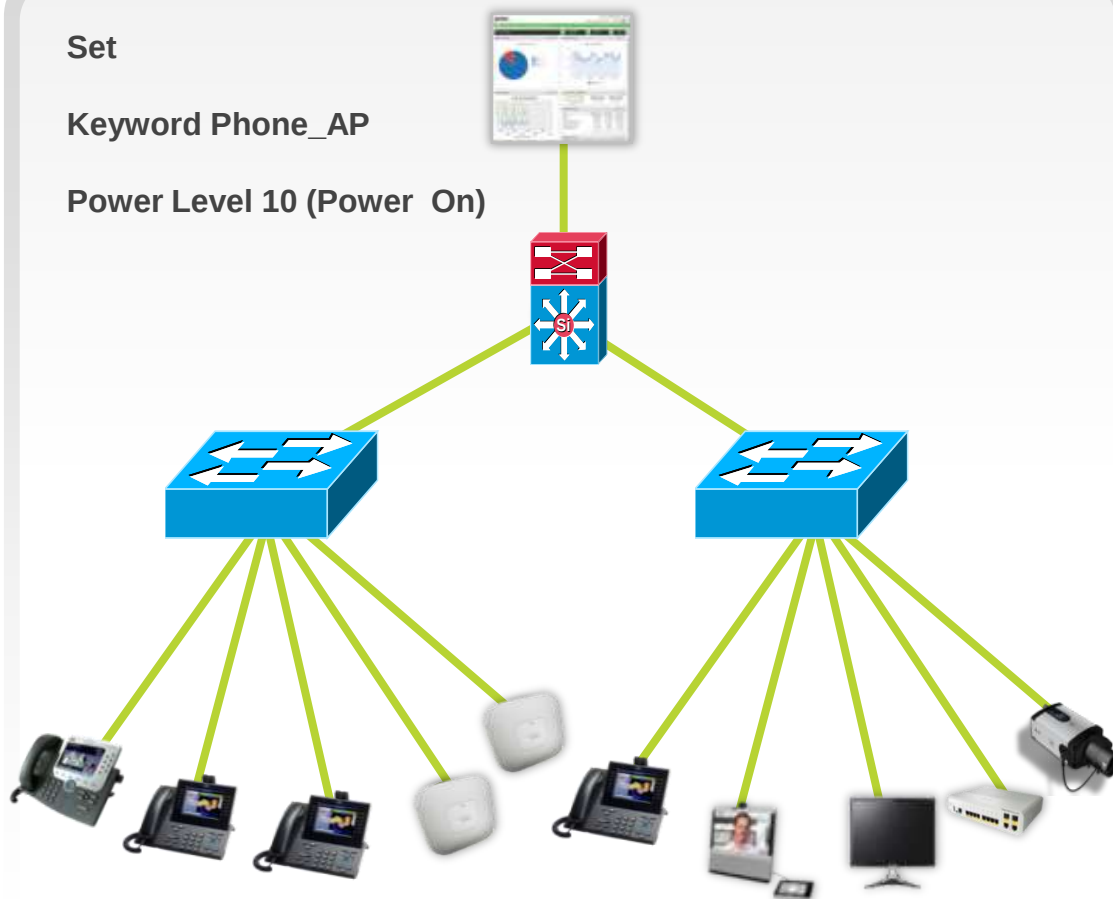
EnergyWise Technology

Network-Based Energy Management

Set

Keyword Phone_AP

Power Level 10 (Power On)

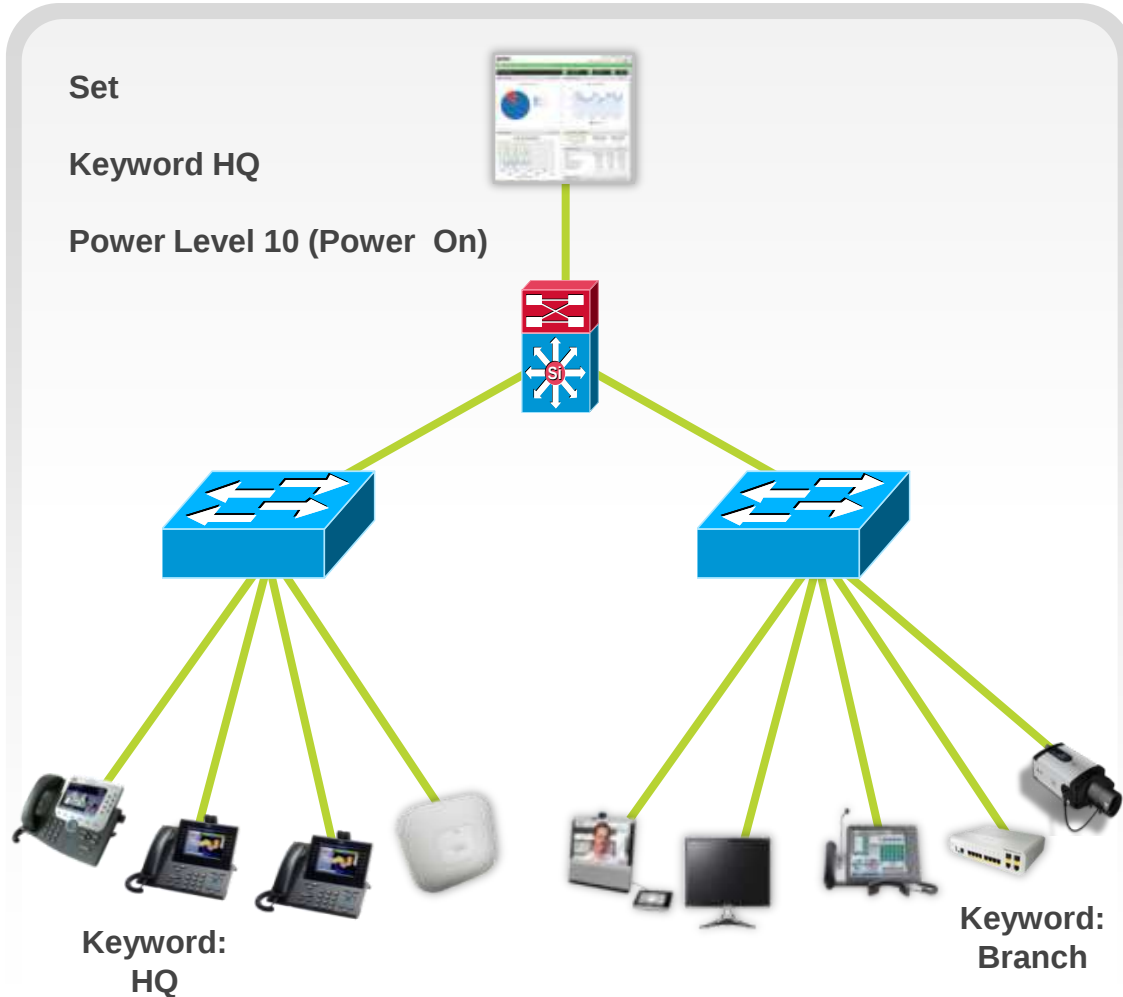


Process:

1. Secure Authentication
2. Auto-discover devices
3. Collect energy consumption
- 4. Set power level modes**
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management

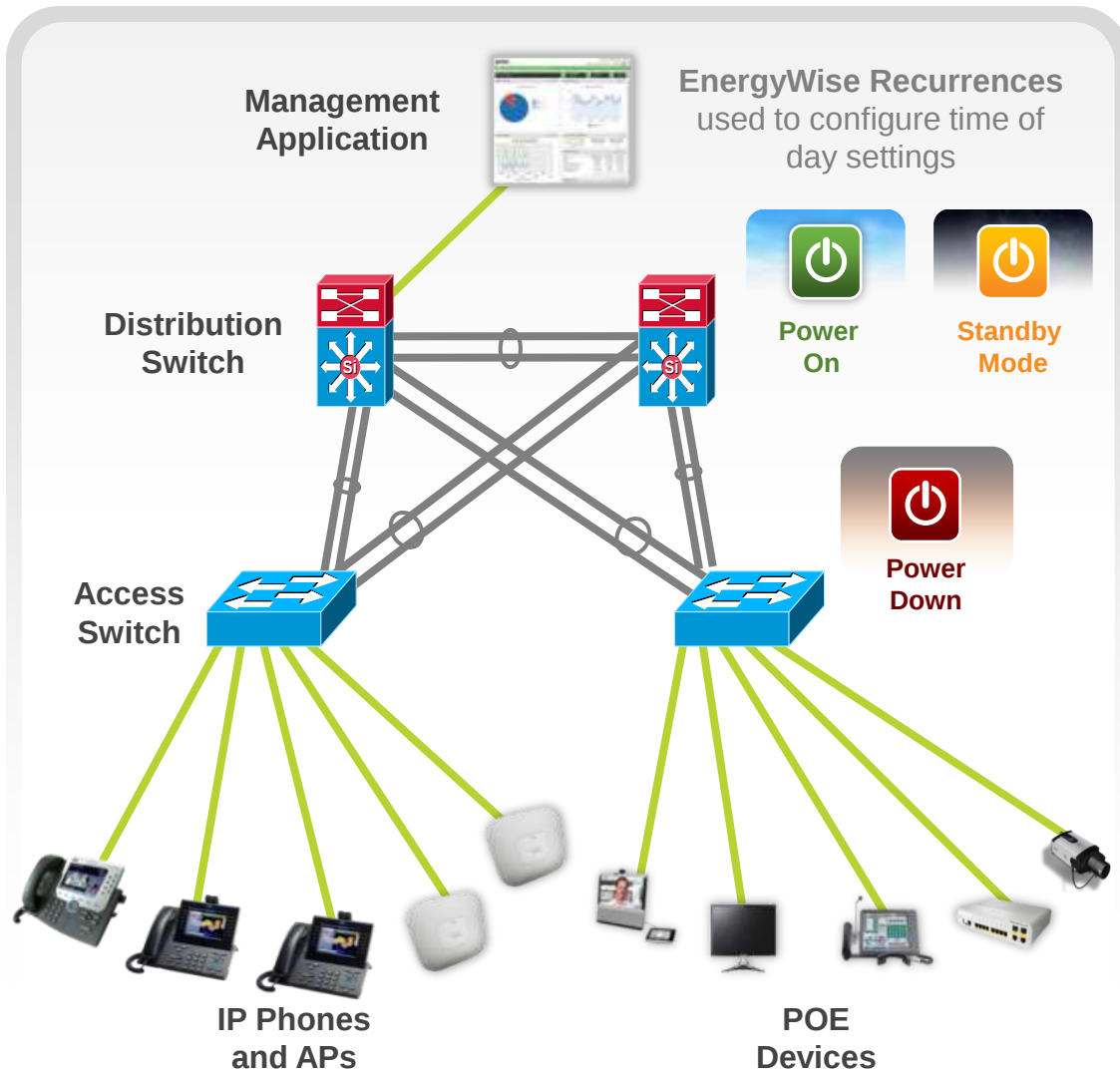


Process:

1. Secure Authentication
2. Auto-discover devices
3. Collect energy consumption
- 4. Set power level modes**
5. Configure Time of Day Policies

EnergyWise Technology

Network-Based Energy Management



Process:

1. Secure Authentication
2. Auto-discover devices
3. Collect energy consumption
4. Set power level modes
5. **Configure Time of Day Policies**

IP Phone Power States

Function	Full Power	Power Save	Power Save Plus (PSP)
Screen Backlight	On	Off	Off
CPU, Memory, interface	On	On	Off
Daisy Chained PC	Connected	Connected	Disconnected
Can receive calls?	Yes	Yes	No
Time before call can be placed	Instantaneous	250 milliseconds	60 seconds
Seen as a domain member?	Yes	Yes	No



Basic Configuration

Begin by creating an EnergyWise domain. This activates EnergyWise on the switch:

```
Switch# config t
```

```
Switch(config)# energywise domain myDomain secret 0 mySecret protocol udp port 43440 ip 2.2.4.30
```

Verify that EnergyWise is active, and report total available power

```
Switch# show energywise
```

Interface	Role	Name	Usage	Lvl	Imp	Type
-----	----	----	-----	---	---	----
	PoE Switch	C3750	86.0 (W)	10	1	parent

Lvl = Level, power level, 0-10

Imp = Importance, a relative number used in power management

```
Switch# show energywise domain
```

```
Name       : C3750-48P-149
Domain      : myDomain
Protocol    : udp
IP          : 2.2.4.30
Port       : 43440
```

EnergyWise Neighbors in Domain & Example



Neighbors are EnergyWise-aware switches and powered devices.

```
Switch# show energywise neighbors
```

Capability Codes: R-Router, T-Trans Bridge, B-Source Route Bridge S-Switch, H-Host, I-IGMP, r-Repeater, P-Phone

Id	Neighbor Name	Ip:Port	Prot	Capability
--	-----	-----	----	-----
1	TG3560G-21	2.2.2.21:43440	udp	S I
2	TG3560G-31	2.2.4.31:43440	static	S I
3	TG3560G-22	2.2.2.22:43440	cdp	S I

EnergyWise collects power usage within EnergyWise domain based on queries with very granular controls

Example: This command collects present power used by all devices in the domain which have the name “phone” (The wildcard “*” is permitted, and finds “phone.1”, “phone.lobby”, etc.)

```
Switch# energywise query importance 100 name phone* collect usage
```

EnergyWise query, timeout is 3 seconds:

Host	Name	Usage
----	----	-----
2.2.2.21	phone	15.4 (W)
2.2.2.22	phone	15.4 (W)

Queried: 9 Responded

All devices in the domain are searched, looking for devices that match the name phone.*

Cisco EnergyWise Product Portfolio



Catalyst 6500



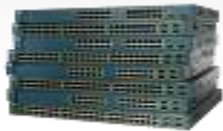
Catalyst 4500 & 4900



Catalyst 2960-S



Catalyst 2960 and 2975



Catalyst 3560-E and 3560



Catalyst 3750-E and 3750



Catalyst 3750-X and 3560-X



Integrated Services Routers
(ISR i.e. 1900/2900/3900) G2



CiscoWorks LMS



Cisco IP Phones



VDI Phone Backpack
and Tower

Software Support

- Catalyst 2960/2975/3560/3750/3560E/3750E – from 12.2(50)SE
- Catalyst 2960S/3560X/3750X – from 12.2(53)SE2
- Catalyst 4500 – from 12.2(52)SG, Catalyst 6500 – from 12.2(33)SX14
- Cisco Routers 1900/2900/3900 - Cisco IOS Software 15.0(1)M3

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

PoE – 802.3af, 802.3at and beyond
Energy Efficient Ethernet
EnergyWise

StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

CDP, LLDP, LLDP-MED
Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

Auto-Smartports & Smartinstall
Netflow / Flexible Netflow
GOLD



Evolving Power Technologies

StackPower

Innovative power interconnect system

- Share power supplies among all switches
- Power no longer confined to a particular switch, power goes where it is needed
- Pay as you grow

Flexible

- From no-power supply to up to 2.2KW per switch
- Can mix different sizes or different types (AC & DC) power supply

Highly resilient

- Enable “zero-footprint” RPS
- Unused power from one power supply can back up an other one

Intelligent load shedding

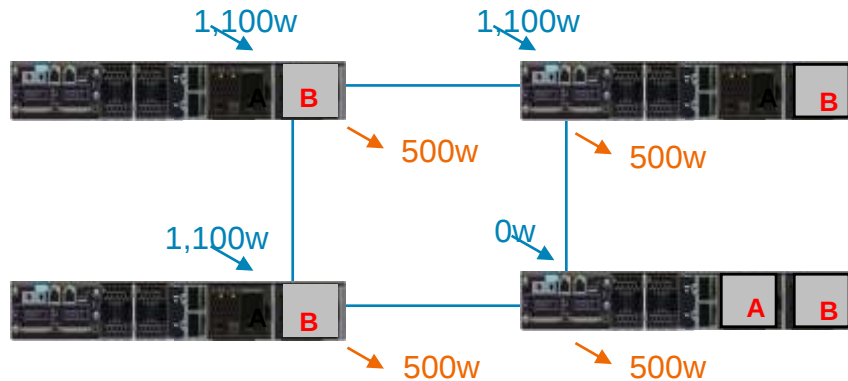
- Preserve the most critical part of your network in case of power supply failure



StackPower Modes

Power share, Redundant, RPS modes

Power Sharing mode

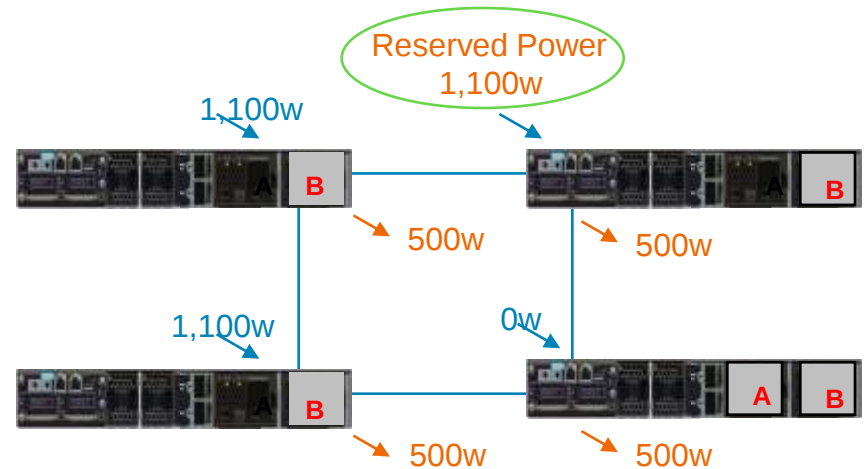


Available Pwr	Allocated Pwr	Unused Pwr
3,300 W	2,000 W	1,300 W

Entire available power of 3,300w is available to the system.

Switch and PD requests for more power is granted until all 3,300w are used. No redundancy

Redundant mode



Available	Allocated	Unused	RESERVED
3,300 W	2,000 W	200W	1,100 W

Overall capacity is 3,300w –1,100w is reserved for redundancy.

Available Power to share is 2,200w and there is an extra 200 W available for allocation.

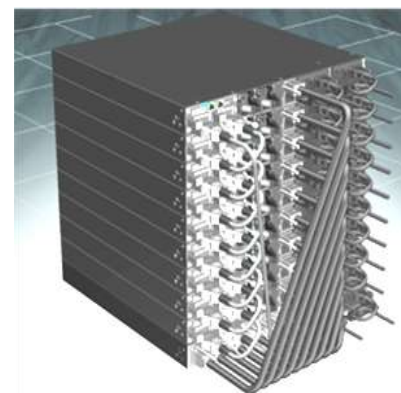
Should a PS fail, then the reserved power is made available for the stack.

eXpandable Power System – XPS 2200

StackPower & RPS Functionality



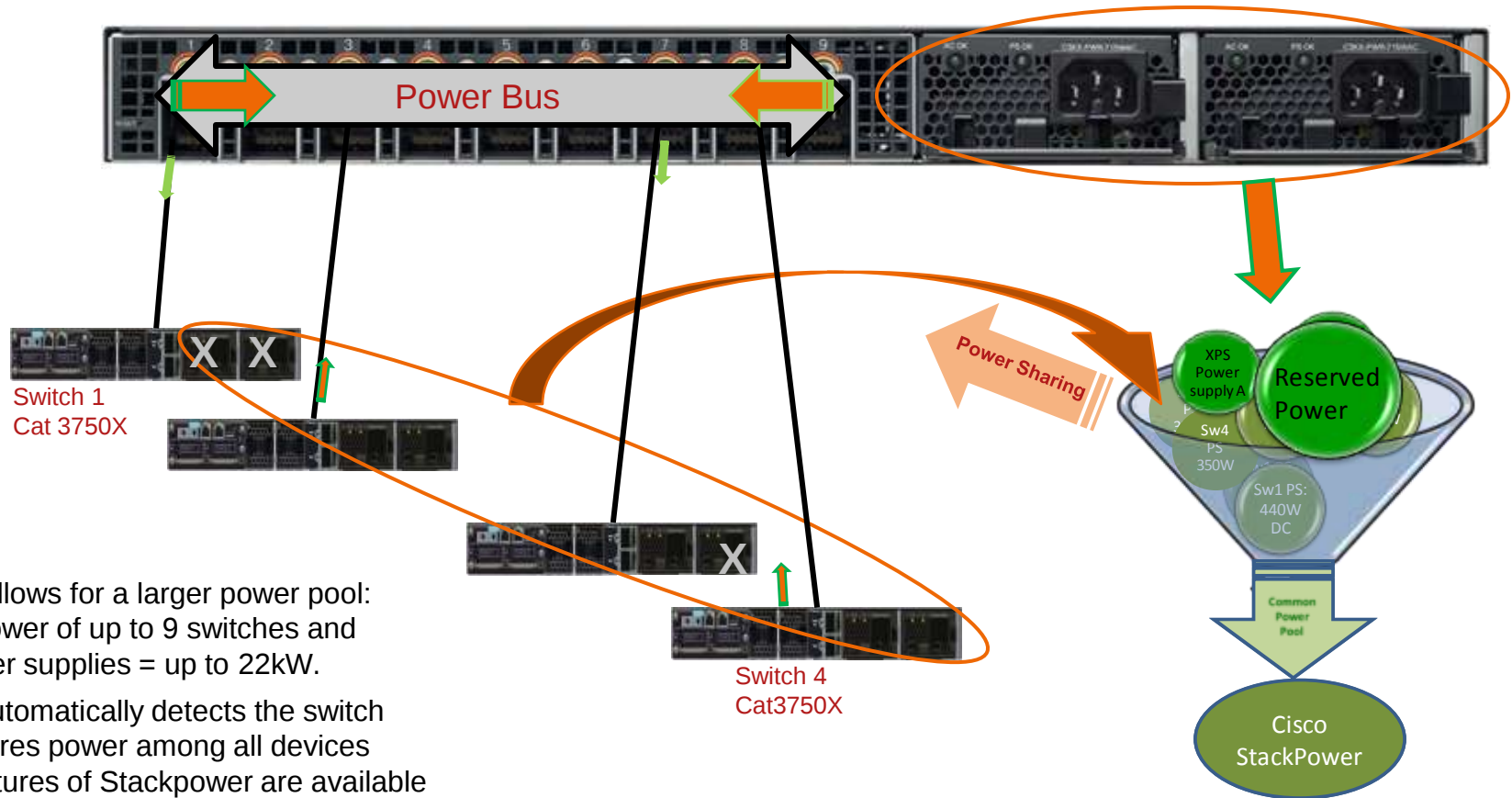
- Provides Power-sharing and RPS functionality concurrently
 - When used with the 3750-X it provides StackPower functionality to all the stack members including power supply redundancy
 - When used with the 3560-X it provides RPS functionality
- Protects up to 9 switches – stackable, standalone, or mixed
- XPS supports up to two power supplies and redundant fans
- Cat3560X/3750X – 48x 30W in 1RU – futureproof
 - That is 30W each on all 48 ports or 1440W of PoE+ plus system power.
- XPS offers full PoE+ redundancy to a 48-port switch
 - That is 30W each on all 48 ports or 1440W of PoE+ plus system power.



XPS – Power-Sharing Functionality

StackPower – Power-share & Redundant modes

Catalyst 3750X ONLY

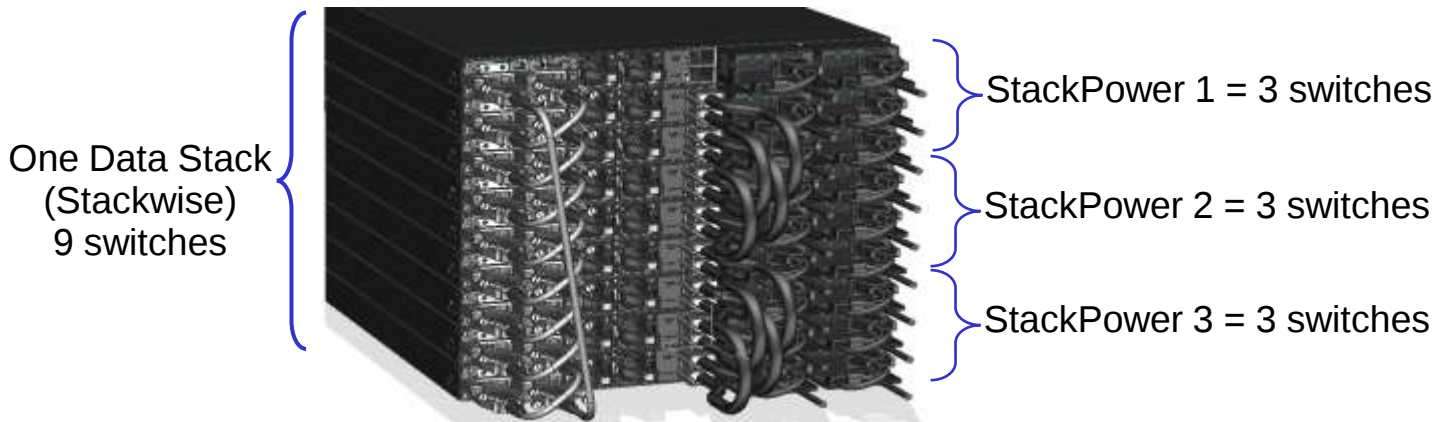


- XPS allows for a larger power pool: Stackpower of up to 9 switches and 20 power supplies = up to 22kW.
- XPS automatically detects the switch and shares power among all devices
- All features of Stackpower are available
- Including power reservation.

Valid Stackpower deployments



- **Either a Ring or a Star topology** – that is 4 or 9 switches!
 - Ring – a maximum of 4 switches in a Stackpower
 - Star – up to 9 switches, attached to an XPS 2200
- A Data stack (Stackwise) can span over two or more power stacks regardless of the topology:

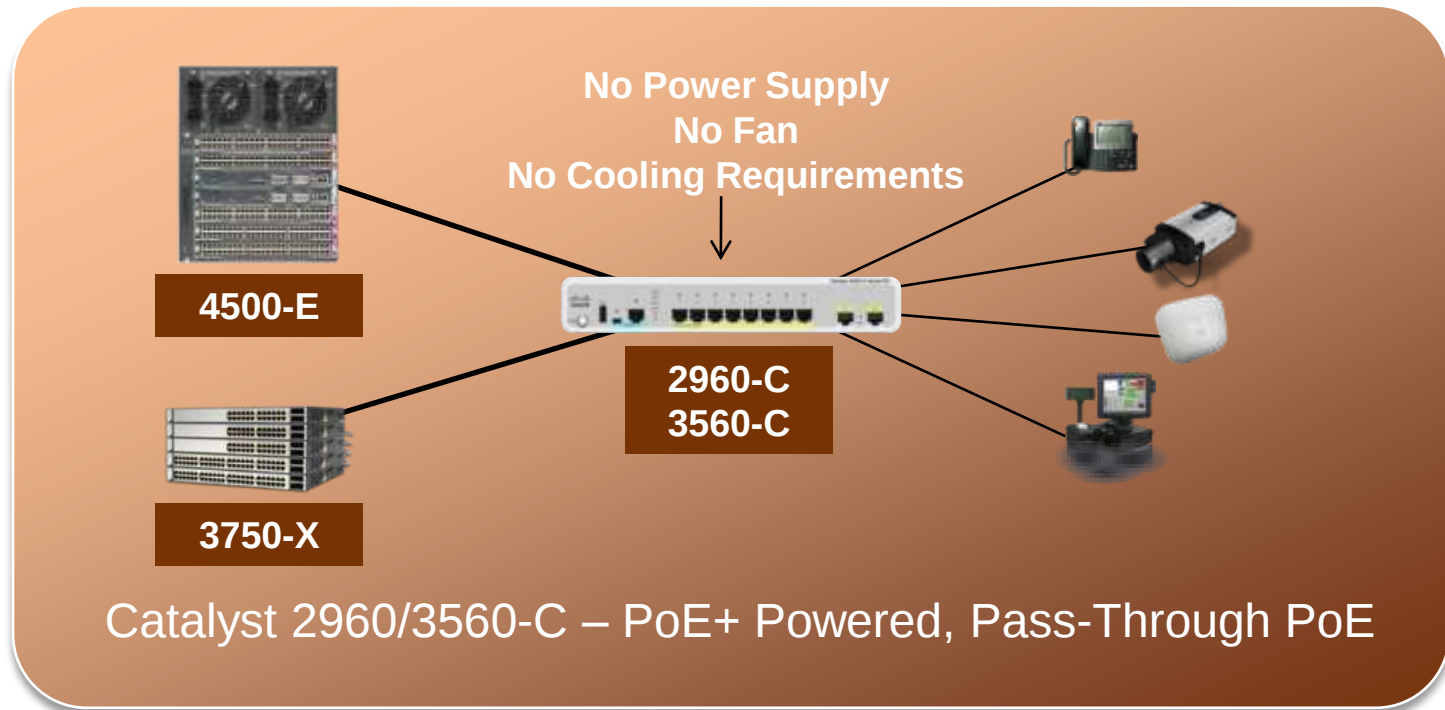


Note:

A power stack can span over two or data stacks but it is not recommended!

Cisco Catalyst Compact Switches

New PD / PSE Device



- Reduce Infrastructure and Energy Demands
- PoE/PoE+ (Input **and** Output) diminish power infrastructure
- Quiet, cool, compact design ideal for co-location



POE Budget for connected Devices

PassThrough power for a Catalyst 2960CPD-8PT-L

Switch Model	Powering Options	Available PoE Power (W)
 WS-C2960CPD-8PT-L	1 PoE Uplink	0W
	2 PoE Uplinks	7W
	1 PoE+ Uplinks	7W
	1 PoE+ and 1 PoE Uplinks	15.4W
	2 PoE+ Uplinks	22.4W
	Auxiliary Input	22.4W
 WS-C3560CPD-8PT-S	1 PoE+	0W
	2 PoE+	15.4W
	Auxiliary Input	15.4W

Power Numbers Assume CAT5 or Better Cabling
Universal PoE powering option support (roadmap)

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond
 - Energy Efficient Ethernet
 - EnergyWise
 - StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED**

- Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

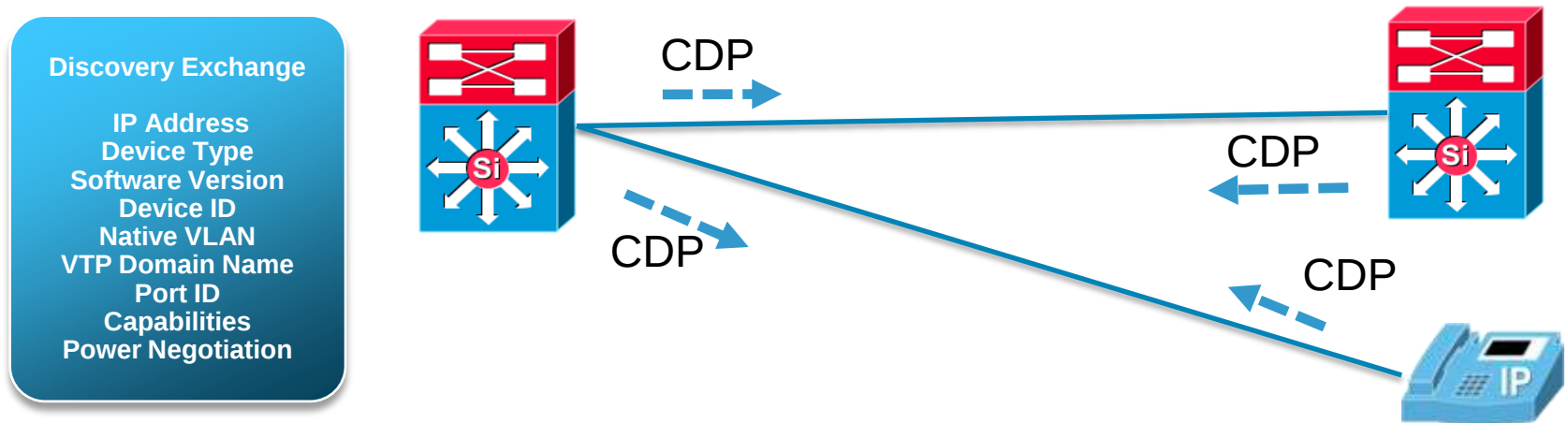
- Auto-Smartports & Smartinstall
 - Netflow / Flexible Netflow
 - GOLD



Negotiating Network Services

CDP – Cisco Discovery Protocol

Cisco Discovery Protocol is a Layer 2 advertisement protocol enabling adjacent devices to learn about each others capabilities



CDP messages are sent periodically (default every 60 seconds)

Each switch maintains its own **CDP state table** - when CDP message is sent an included TTL value tells destination device how long to keep CDP information

```
C4507R-E#sh cdp neighbors
```

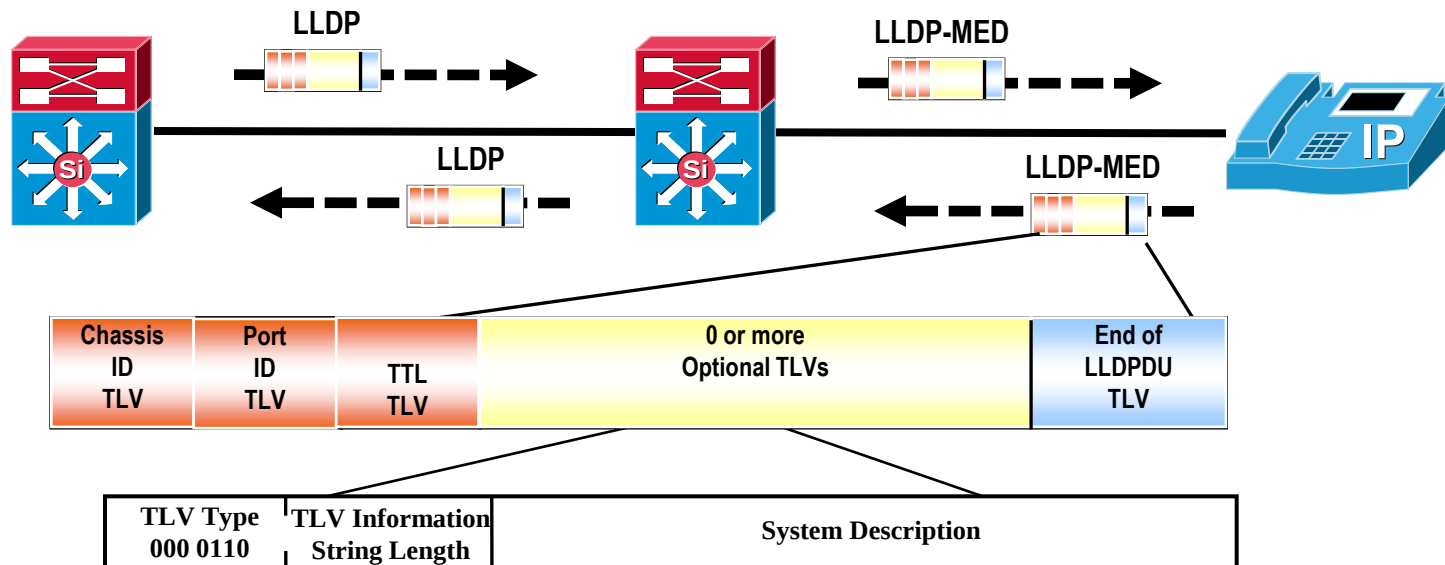
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
C4510R-E	TenGig 1/1	161	R S	WS-C4510R	TenGig 1/1
IP Phone 7961	Gig 1/1	159	P	CP-7961G	Fas 0/1

Negotiating Network Services

LLDP, LLDP-MED

- LLDP (802.1AB) - IEEE-SA Standards Board approved March 2005
- LLDP-MED (TR 41.4) – Adjunct TIA standards for Media Endpoint Discovery (specific to Unified Communications endpoints)
- Ports initialized with LLDP can transition to running the LLDP-MED after an LLDP-MED Capabilities TLV is received on a port



Negotiating Network Services

Configuring LLDP, LLDP-MED

- LLDP is disabled by default, you need to explicitly configure which optional TLV's to send
- LLDP and CDP can coexist on same interface
- LLDP, LLDP-MED support

Catalyst 6500 – 12.2(33)SXH

Catalyst 4500 and 4900 – 12.2(44)SG

Catalyst 3750, 3560, 2970, 2960 - 12.2(37)SE*

* Support for Protocol Media Extension
(3750, 3560, 2960) - 12.2(40)SE

```
cr32-4500-1(config)#lldp run
```

**Enable LLDP
Globally**

```
cr32-4500-1(config)#lldp tlv-select ?
```

mac-phy-cfg	IEEE 802.3 MAC/Phy Configuration/status TLV
management-address	Management Address TLV
port-description	Port Description TLV
port-vlan	Port VLAN ID TLV
system-capabilities	System Capabilities TLV
system-description	System Description TLV
system-name	System Name TLV

**Configure Optional Global
TLV's**

```
cr32-4500-1(config-if)#lldp med-tlv-select ?
```

inventory-management	LLDP MED Inventory Management TLV
location	LLDP MED Location TLV
network-policy	LLDP MED Network Policy TLV
power-management	LLDP MED Power Management TLV

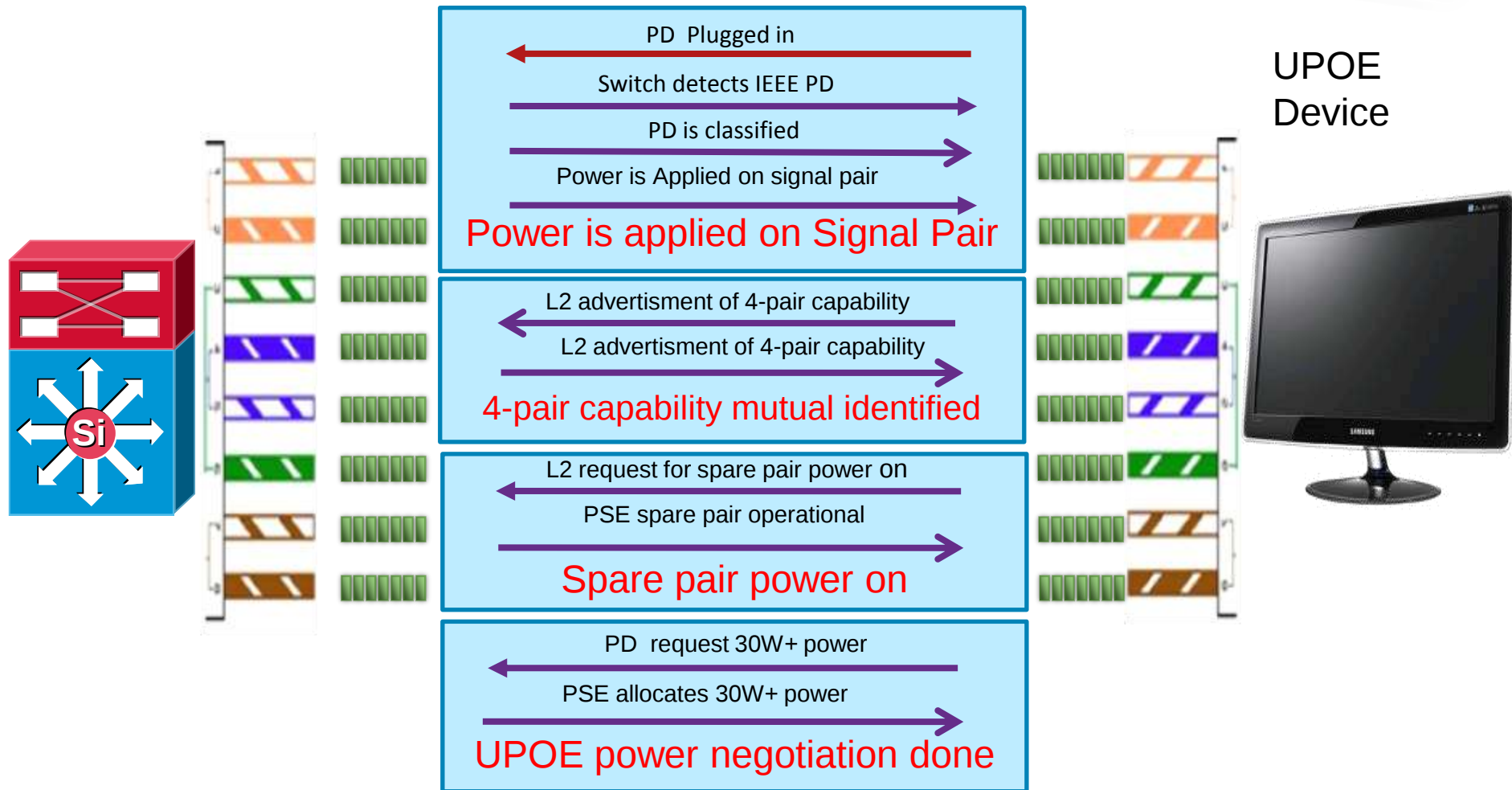
**Configure Optional Interface
TLV's**

LLDP-MED and Cisco Discovery Protocol,

http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html

UPOE Power Negotiation

Example: Evolving LLDP-MED Capabilities



- Supported with CDP & LLDP-PoE+ from IEEE 802.3at

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond
 - Energy Efficient Ethernet
 - EnergyWise
 - StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED

- Dynamic Quality of Service**

- **Intelligent Operations & Monitoring**

- Auto-Smartports & Smartinstall
 - Netflow / Flexible Netflow
 - GOLD



Campus QoS Design

Strategic QoS Design Principles

- Always perform QoS in hardware rather than software when a choice exists
- Classify and mark applications **as close to their sources** as technically and administratively feasible
- Police unwanted traffic flows **as close to their sources** as possible
- Enable queuing policies at every node where the potential for congestion exists
- Protect the control plane and data plane

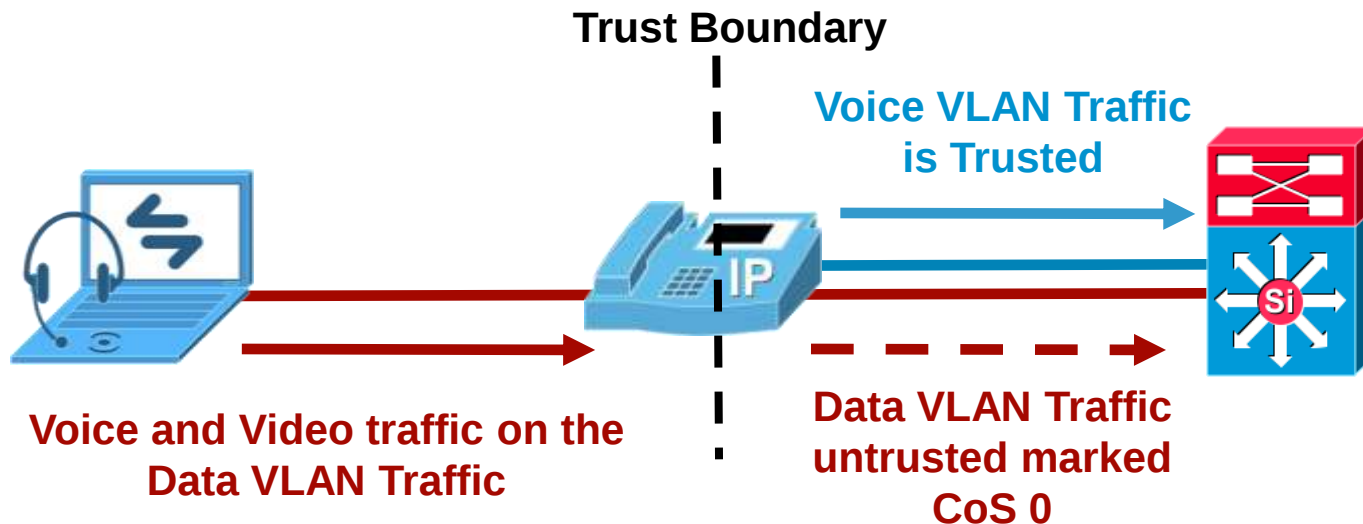
Enterprise QoS Solution Reference Network Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Intelligent Voice QoS

Trust Boundary with CDP

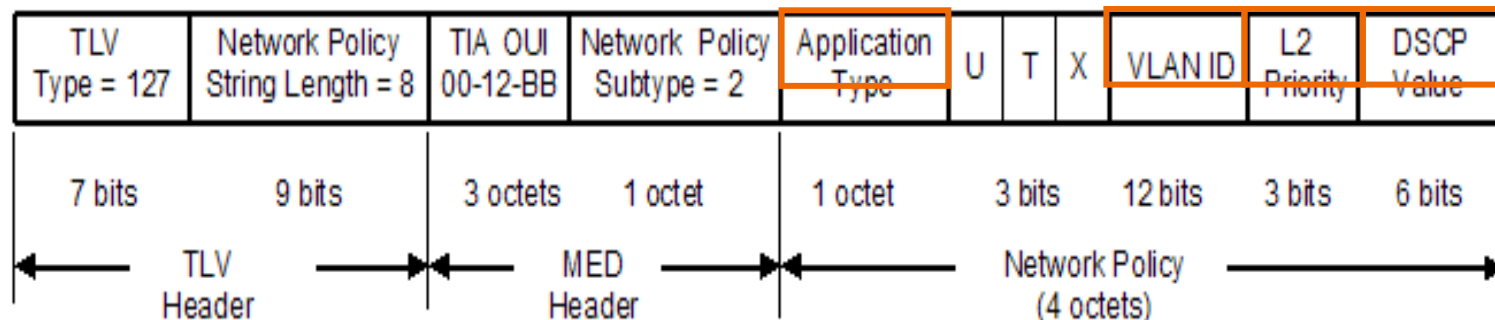
- Question: To Trust or not to Trust?
- Use Trust Boundary to prevent abuse of COS/DSCP priority.
- With existing auto-qos configuration the default switch behaviour is to not trust edge ports and remark all traffic to configured CoS/DSCP
- When switch and phone exchange CDP the trust boundary is extended to IP phone
- Phone rewrites CoS from PC port to '0', switch rewrites DSCP



Configuring Voice QoS for 3rd party phones

LLDP-MED Network Policy TLV

- The Network Policy Discovery TLV allows both Network Devices and Endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes that apply for a set of specific applications on a port
- **Application Type:** Identifies the the application(s) which should use this network policy (Voice, Control / Signaling, ...)
- **VLAN ID:** VLAN used to carry for the identified application
- **L2 Priority:** CoS value to be used on the identified application packets
- **DSCP Value:** Diffserv value to be used on the identified application packets (64 code points values)



Negotiating Network Services

LLDP-MED Network Policy TLV



- Configuration is done using “network-policy” profile in Global Configuration Mode (MQC like syntax)
- Significantly speeds up bootup time of 3rd party phones
- Currently Network Policy supports configuration for voice & voice-signaling capabilities
 - vlan
 - cos and dscp,
 - tagging mode (dot1p/ untagged/ none)

```
Switch(config)# lldp run

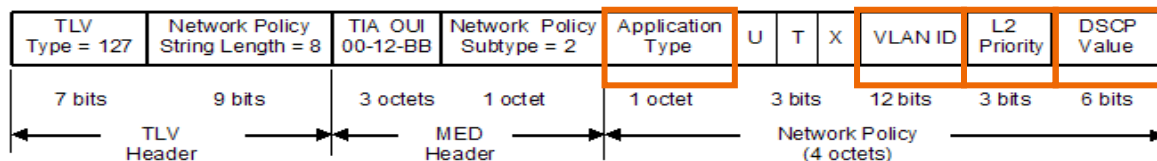
network-policy profile 10
  voice vlan 100 cos 5
  voice vlan 100 dscp 46
  voice-signaling vlan 100 cos 3
  voice-signaling vlan 100 dscp 32

network-policy profile 20
  voice vlan 20 cos 5
  voice vlan 20 dscp 46

interface gig1/0/1
  network-policy 10

interface gig1/0/2
  network-policy 20

switch# show network-policy
profile 20
Network-Policy Profile 20
  voice vlan 20 cos 5 dscp 46
```



Campus QoS Designs are evolving

Business and Technical Drivers



64% of communication is non-verbal¹

One third of the human cortex is dedicated to vision²



- New Applications and Business Requirements

 - Explosion of Video Apps

 - Impact of HD (Impact of 1 packet drop?)

 - Blurring of Voice/Video/Data application boundaries

- New Standards and RFCs

 - RFC 4594

- New Platforms and Technologies

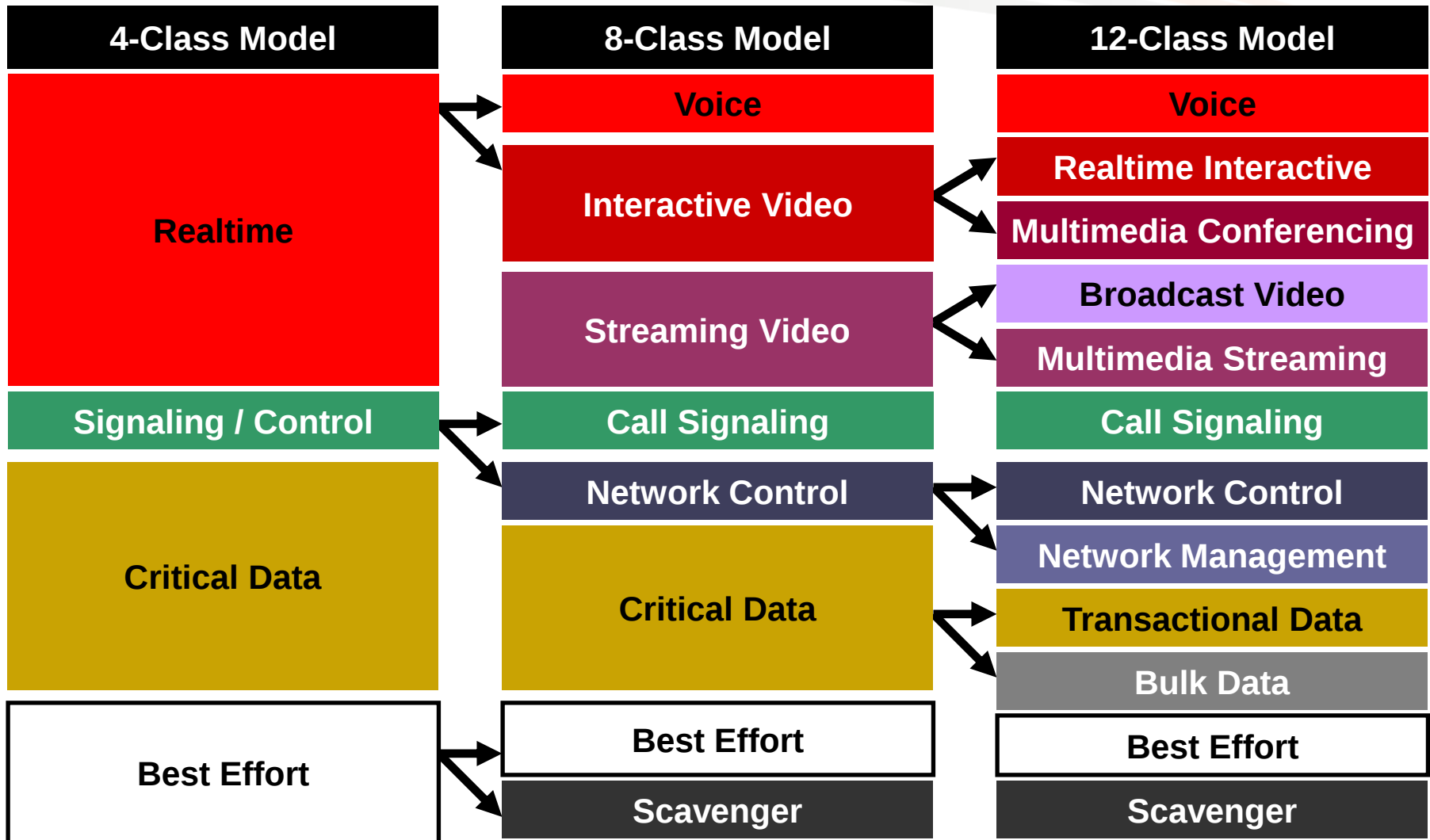
 - New Switches, Supervisors, Linecards, features, syntax

¹Kandola, Pearn "The Psychology of Effective Business Communications in Geographically Dispersed Teams", Cisco Systems, September 2006

²Vision Group Research, FMRIB, University of Oxford, UK

Evolving Business Requirements

Business Requirements Will Evolve and Expand over Time



Enterprise Medianet Quality of Service Design 4.0

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61135

Auto QoS VoIP - Making It Easy

Configures QoS for VoIP on Campus Switches

Options:

auto qos voip cisco-phone

auto qos voip cisco-softphone

auto qos voip trust



```
Access-Switch(config-if)#auto qos voip ?
```

```
cisco-phone    Trust the QoS marking of Cisco IP Phone
```

```
cisco-softphone Trust the QoS marking of Cisco IP SoftPhone
```

```
trust          Trust the DSCP/CoS marking
```

```
Access-Switch(config-if)#auto qos voip cisco-phone
```

```
Access-Switch(config-if)#exit
```

```
!
```

```
interface FastEthernet1/0/21
```

```
srr-queue bandwidth share 10 10 60 20
```

```
srr-queue bandwidth shape 10 0 0 0
```

```
mls qos trust device cisco-phone
```

```
mls qos trust cos
```

```
auto qos voip cisco-phone
```

```
end
```



Auto QOS for Media

Auto QOS not just for voice anymore



- New Auto QOS video

Classify Classify packets from untrusted device

Trust Trust the QoS marking of the device
connected

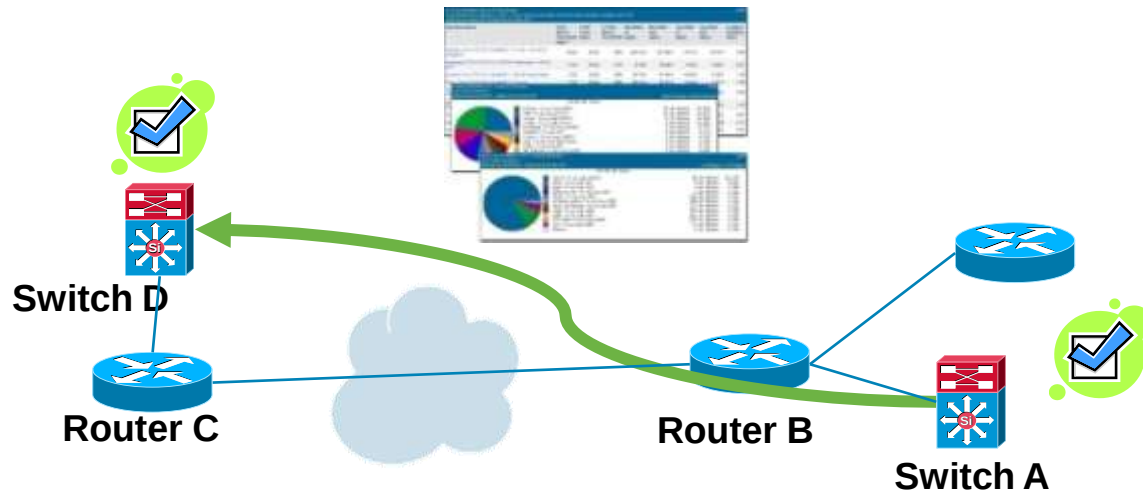
Video **Configure AutoQoS for video device**

Voip Configure AutoQoS for VoIP

- Driven by Proliferation of video in the campus
- New AutoQoS functionality available since 2HCY2010

Intelligent Operational Management

IP SLA Video - Embedded Traffic Simulator



- IPSLA known in industry for jitter, ICMP, etc. probes
- Most probes measure experience without affecting user traffic (hopefully)
- Need traffic to **stress test** network
- IPSLA VO provides
 - Realistic representation of arbitrary video (RTP) traffic
 - Packet sizes, burstiness, traffic rate, etc.
 - Pre-packaged profiles: IPTV, Video Surv, CTS, **Custom profile from packet capture**

Dynamic Monitoring with Mediatrace

- Mediatrace **discovers and queries L2 and L3 nodes** along a flow's path
- Gathers system resource, interface and flow specific (perf-mon) stats
- **Consolidates information into a single screen**
- Allows for **easy comparisons** of device behavior
 - Which interface dropping packets?
 - Where is DSCP getting reset?
- Can be requested by remote device
- Automatically (based on thresholds) via EEM script

```
initiator#show mediatrace session stats 1
Session Index: 1
...
Mediatrace Hop: 2 (host=responder2, ttl=253)
  Metrics Collection Status: Success
  Reachability Address: 10.10.34.3
  Ingress Interface: Gi0/1
  Egress Interface: Gi0/2
  Metrics Collected:
    Flow Sampling Start Timestamp: 23:45:56
    Loss of measurement confidence: FALSE
    Media Stop Event Occurred: FALSE
    IP Packet Drop Count (pkts): 0
    IP Byte Count (Bytes): 6240
    IP Packet Count (pkts): 60
    IP Byte Rate (Bps): 208
    Packet Drop Reason: 0
    IP DSCP: 0
    IP TTL: 57
    IP Protocol: 17
    Media Byte Rate Average (Bps): 168
    Media Byte Count (Bytes): 5040
    Media Packet Count (pkts): 60
    RTP Jitter Average (usec): 3911
    RTP Packets Lost (pkts): 0
    RTP Packets Expected (pkts): 60
    RTP Packet Lost Event Count: 0
    RTP Loss Percent (%): 0.00
```

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond
 - Energy Efficient Ethernet
 - EnergyWise
 - StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED
 - Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

- Auto-Smartports & Smartinstall**

- Netflow / Flexible Netflow
 - GOLD



Smart Operations – What is it?

Overview and Benefits

Smart Install

- New **Switches** - Automatic image and configuration download
 - Saves Opex
- Zero-touch deployment and switch replacement
 - Reduces Network downtime and the need for technical IT staff
- Centralized management for image and configuration
 - Single point of management

Auto Smart Ports

- Plug and Play of new **devices**
- End-points – Device-based dynamic configuration management
 - Cisco recommended interface configuration for every device type

Intelligent Operations

AutoSmartPorts

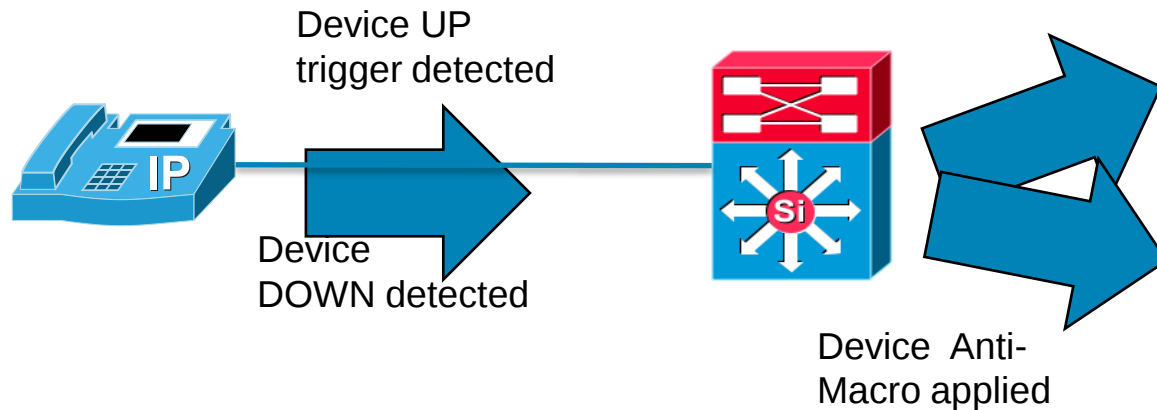
- Built-in Switch intelligence for Device Identification-based interface configuration
- Automatic & Cisco-recommended per port configuration
- Plug and Play for end-devices
- Supported Devices:
 - Switches
 - Routers
 - Access Points
 - Digital Media Player
 - IP-Phones
 - IP-Cameras
 - Other (MAC OUI, custom trigger) ...



Auto Smartports

Modes of operation

User plugs in a device



```
function CISCO_DMP_AUTO_SMARTPORT () {  
  if [[ $LINKUP -eq YES ]]; then  
    conf t  
      interface $INTERFACE  
        macro description $TRIGGER  
        switchport access vlan $ACCESS_VLAN  
        switchport mode access  
        switchport block unicast  
        mls qos trust dscp  
        spanning-tree portfast  
        switchport port-security  
        switchport port-security maximum 1  
        switchport port-security violation shutdown  
        spanning-tree bpduguard enable  
        priority-queue out  
      exit  
    end  
  fi  
}
```

```
function CISCO_DMP_AUTO_SMARTPORT () {  
  if [[ $LINKDOWN -eq YES ]]; then  
    conf t  
      interface $INTERFACE  
        no macro description $TRIGGER  
        no switchport access vlan $ACCESS_VLAN  
        no switchport mode access  
        no switchport block unicast  
        no mls qos trust dscp  
        no spanning-tree portfast  
        no switchport port-security  
        no switchport port-security maximum 1  
        no switchport port-security violation shutdown  
        no spanning-tree bpduguard enable  
        no priority-queue out  
      exit  
    end  
  fi  
}
```

Trigger - Event that detects the presence or removal of a device in the network (link up)

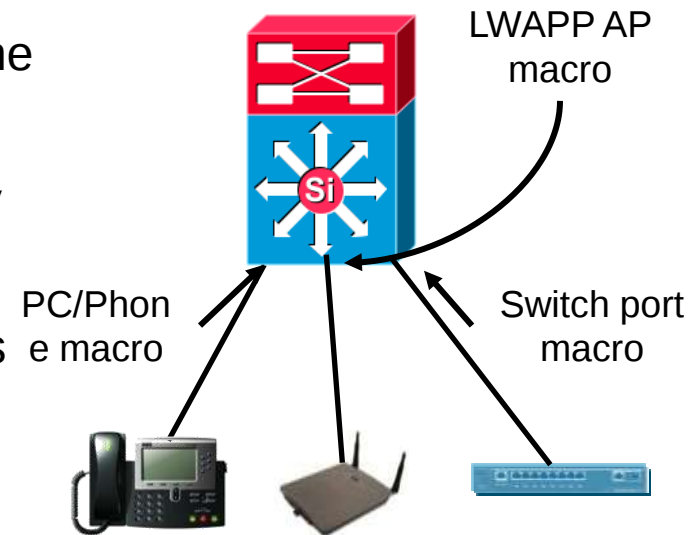
Macro - Set of configuration commands referred to as a single unit.

Anti- macro : List of config steps that gets applied to a port when a device is removed

Auto Smartports

Recommendations

- Auto smartports can be enabled on a global or per interface basis
- By default auto smartports will utilize CDP as the device identification method
- If 802.1x is enabled then macro is controlled by 802.1x
- 802.1x allows for fallback to CDP trigger events
- Decide which ports will be managed via ASP
- Supported in:
12.2(55)SE – 2960, 3560, 3750
12.2(54)SG – 4500
- Custom trigger, Custom macro



Automatic configuration of the access port as devices connect



Auto Smartports

Configuration Example

1) Define a stub configuration for the access ports

```
2960s(config)#int range GigabitEthernet 1/0/1 - 48
2960s(config-if-range)#switchport access vlan 10
2960s(config-if-range)#switchport mode access
```

2) In this example, ASP is enabled for only Lightweight Access Points and IP Phones

```
2960s(config)#macro auto global control device phone lightweight-ap
```

3) Set vlan parameters for the AP and IP phone

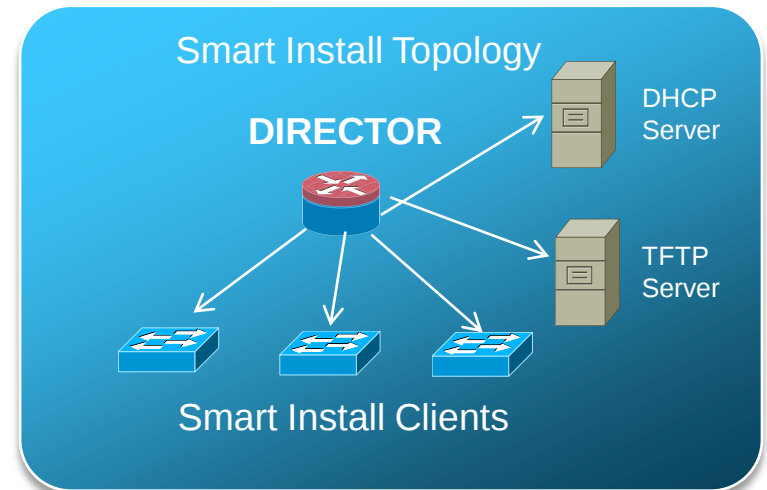
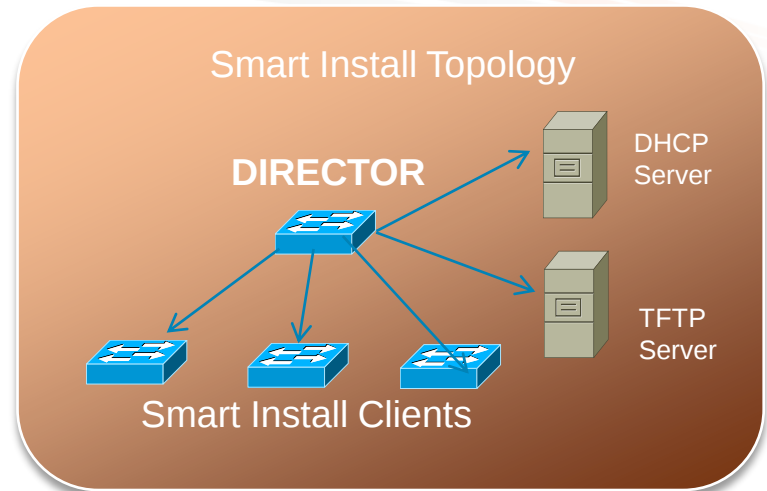
```
2960s(config)#macro auto device phone ACCESS_VLAN=11 VOICE_VLAN=10
2960s(config)#macro auto device lightweight-ap ACCESS_VLAN=11
```

4) Enable ASP

```
2960s(config)#macro auto global processing
```

Introduction to Smart Install

- Easy Deployment, Easy Maintenance, Cost Savings
- A network using Smart Install includes a group of networking devices, known as clients, that are served by a common Layer 3 switch or router that acts as a director. The director provides a single management point for images and configuration of client switches
- How it works:
 - Director snoops dhcp requests from clients.
 - The information used to determine the image and config that will be loaded is:
 - PID
 - MAC
 - STACK
 - Connectivity

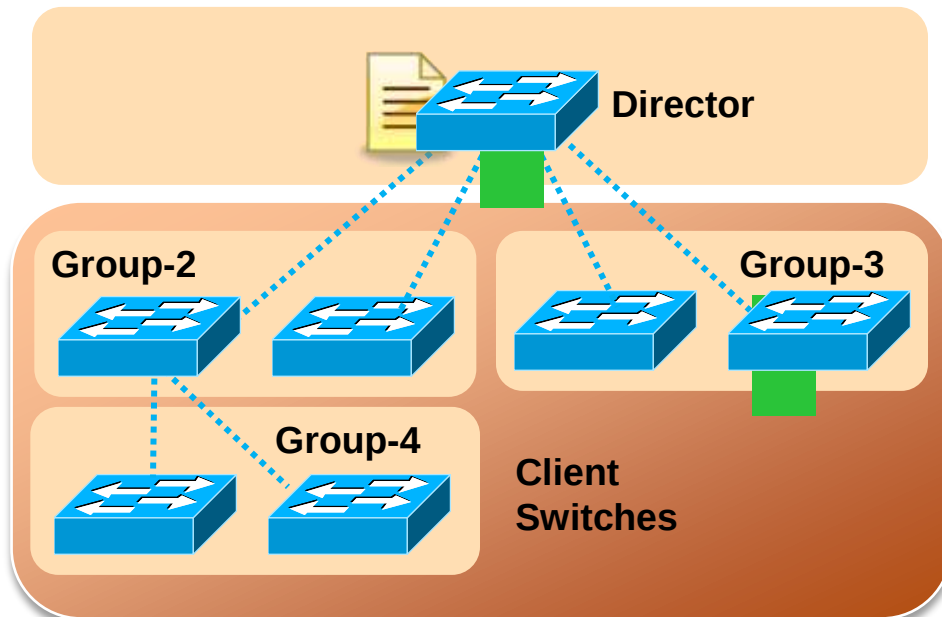


Deploying a New Switch with Smart Install

1. New switch is connected
2. DHCP request
3. DHCP Snooping Mgmt VLAN
4. Switch assigned to Group 3
5. Hostname/IP assigned
6. Download config and image

Guidelines for the Director

- Total flash memory space (used and free) must be large enough for Clients
- Flash must be large enough to contain Director configuration and image also
- IOS images vary in size depending on Client type, flash memory is limited
- If more than one product ID on the network, best to use separate TFTP server



SmartInstall – Configuration Guidelines

Enabling the Director & DHCP Server & Copying an Image



- **Step #1 – execute the ‘vstack enable’, ‘director’, ‘basic’ commands**

```
Switch(config)#vstack director 10.10.0.1
Switch(config)#vstack basic
Switch(config)#vstack vlan 10
```

- **Step #2 – execute the ‘vstack dhcp local-server ‘ command**

```
Switch(config)#vstack dhcp local-server smart-install-switches
Switch(config-vstack-dhcp)#address-pool 10.10.0.0 255.255.255.0
Switch(config-vstack-dhcp)#default-router 10.10.0.1
Switch(config-vstack-dhcp)#file-server 10.10.0.1
Switch(config-vstack-dhcp)#exit
Switch(config)#ip dhcp remember
```

- **Step #3 – copy image and config file to director with ‘copy tftp flash’**

```
Switch#copy tftp flash
...
Accessing tftp://10.10.0.100/c3750-image.tar...
...
Accessing tftp://10.10.0.100/smart-install.txt...
```

- **Step #4 – assign default image and config with ‘vstack’ command**

```
Switch(config)#vstack image flash:c3750-image.tar
Switch(config)#vstack config flash:smart-install.txt
```

- **Optional Step #5 – configure groups & assign image and config with ‘vstack group’ product-id/connectivity/mac/stack/ command**



Addition of a new Client Switch

- To verify the download status:

```
Switch#show vstack download-status
```

```
Total no of entries : 1
```

No	client-IP	client-MAC	Method	Image-status	Config-status
1	10.10.0.2	000f.349a.e000	zero-touch	UPGRADED	UPGRADED

- To see new switch:

```
Switch#show vstack status
```

```
Code :
```

```
HOP 0 : Director          HOP N : Nth Hop in the Network
```

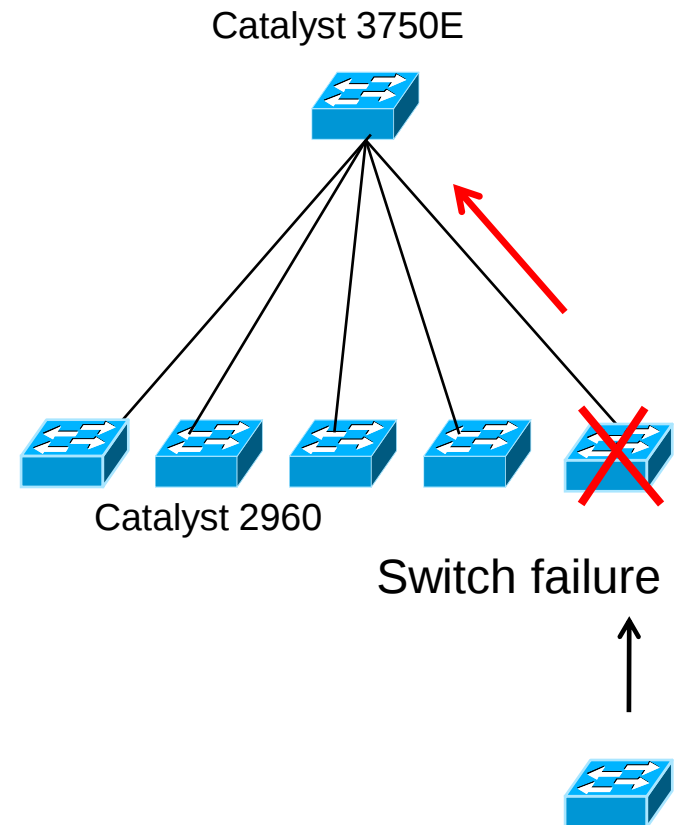
```
HOP ** : Reachability Unknown / Unreachable
```

```
Director Database :
```

MAC Address	Product-ID	IP_addr	DevID	HOP
0018.b995.0600	WS-C3750G-24PS	10.10.0.1	3750_switch	0
0011.2123.5e00	WS-C3550-24-PWR	35.1.1.1	3550_switch	1
0019.554f.c300	2851	11.1.1.2	top_2821	1
000f.349a.e000	WS-C3750G-24TS	10.10.0.2	smart-install-s	1

Zero Touch Switch Replacement

- Client Switch goes bad
 - Director gets an update
 - Network personnel replaces the bad switch with a new switch of the exact same model and on the same switch port
-
- New client switch downloads image and most recent configuration of the failed switch
-
- Client switch reboots and is ready for use



Smart Install also provide

- **Zero Touch Switch Installation/Replacement**
- **Configuration Protection** - Constant client switch configuration backup
- **Secured Switch Upgrade – Join Window**
- **On Demand (Group) Upgrades**
- **Use Cases – Campus and Branch topologies:**
 - With different switch models
 - Different software images
 - Different configurations
 - Managed via an ISR Router or a Catalyst 3560/3750 switch

Supported Hardware Platforms



Director Switches:

- 3750, 3750v2, 3750E, 3560, 3560v2, 3560E - Software version : **12.2.(55)SE** & above
- 3750X, 3560X - Software version : **12.2.(55)SE2** & above
- **Catalyst 4k series – Will support SmartInstall Director functionality in the future**
- Recommended version for switches : **12.2.(55)SE3** because of enhancements

Director Routers:

- G1: 1841, 2801, 2811, 2821, 2851, 3825, 3845
- G2: 1921, 1941, 2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E, NM-16-ESW
- Minimum Software version : **15.1.(3)T**

Client Switches

- 3k – 3750, 3750E, 3750X, 3560, 3560E, 3560X, 3560C
- 2k – 2960, 2960C, 2960S, 2975, 2960G.
- NME-16ES-1G-P, SM-ES3SM-ES2-16-P
- **Special Cases:** 3560v2, 3750v2, Industrial Ethernet series switches (custom groups)

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond
 - Energy Efficient Ethernet
 - EnergyWise
 - StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED
 - Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

- Auto-Smartports & Smartinstall
 - Netflow / Flexible Netflow**
 - GOLD



Service Planning

Flexible NetFlow (FNF)

- Traditional NetFlow with the v5, v7, or v8 NetFlow export

- NetFlow Version 9 (RFC3954)

Advantages: **extensibility**

Integrate new technologies/data types quicker
(MPLS, IPv6, BGP next hop, etc.)

Integrate new aggregations quicker

Basis for IETF IPFIX Standard (RFC5101 & RFC5102)

**Exporting
Process**

- Flexible NetFlow

Advantages: cache and export content **flexibility**

User selection of flow keys

User definition of the records

**Metering
Process**

Traditional NetFlow vs. Flexible NetFlow



Traditional NetFlow

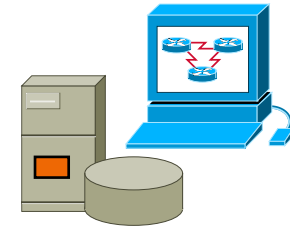
Fixed 7 keys

Fixed definition of flow record globally

Export only to one collector

NetFlow Cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	SrcPort	DstPort
Fa1/0	173.100.2	Fa0/0	10.0.227.11	11	00A2	00A2
Fa1/0	173.100.3	Fa0/0	10.0.227.6	6	15	15
Fa1/0	173.100.2	Fa0/0	10.0.227.11	11	00A1	00A1
Fa1/0	173.100.6	Fa0/0	10.0.227.6	6	19	19



Flexible NetFlow

Flow Monitor 1

Flow Monitor 2

Flow Monitor 3

Flow cache 1

DstIPadd	Protocol	TOS
10.0.227.12	11	80
10.0.227.12	6	40
10.0.227.12	11	80
10.0.227.12	6	40

Flow cache 2

Protocol	TOS	Flgs
11	80	10
6	40	0
11	80	10
6	40	0

Flow cache 3

SrcIf	SrcIPadd	DstIf
Fa1/0	173.100.21.2	Fa0/0
Fa1/0	173.100.3.2	Fa0/0
Fa1/0	173.100.20.2	Fa0/0
Fa1/0	173.100.6.2	Fa0/0



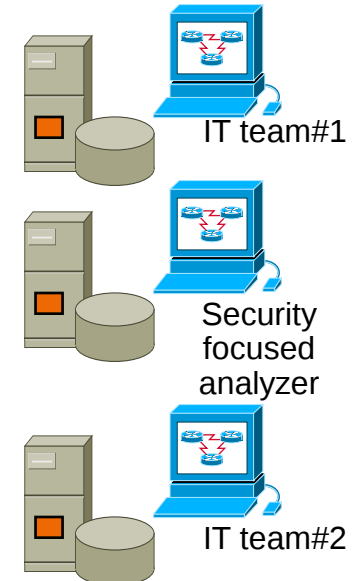
Destination 1



Destination 2



Destination 3



Flexible definition of flow records applied to selected interface or VLAN

Ability to export flow information to multiple collectors/analyzers

Flexible NetFlow (FNF)

Use cases



Monitoring Security

- Detect network anomalies - Identify and mitigate network attacks
- Forensics and Incident investigation
- Network Acceptable Use



Usage/Billing

- Develop billing strategies based on data, video and voice usage per port.
- Bill users for data usage on a per port basis
- Enforce policies to limit usage

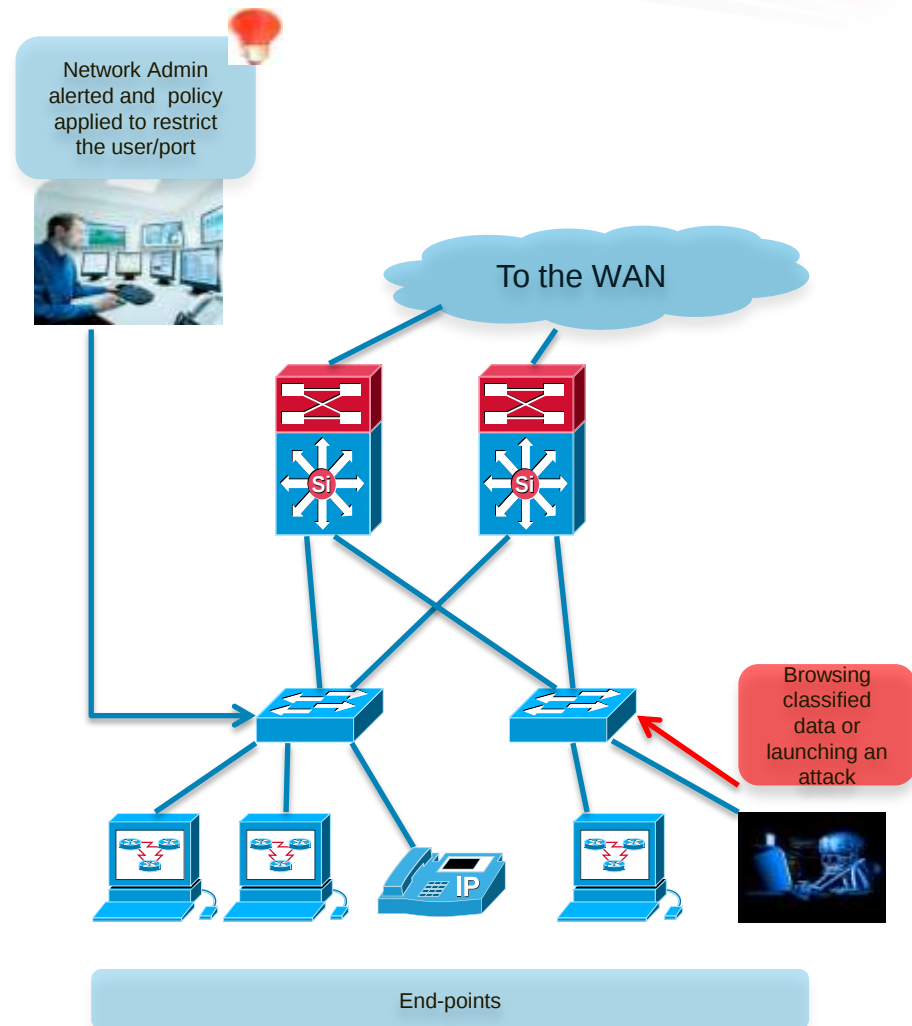


Capacity planning

- Identify the top talkers in the LAN
- Identify traffic patterns and data usage trends over a time period
- Identify types of applications in different parts of the network

Monitoring and Security at the Access

- Security a key concern for IT admins.
- **Problem:**
Lack of visibility into user at the access
 - Questions asked by the IT admin:
 - Which end-point visited which site?
 - For how long?
 - Is a user allowed to access that information?
 - Is a user expected to be online at this time?
 - Why is the volume of traffic sent by the user abnormally high?

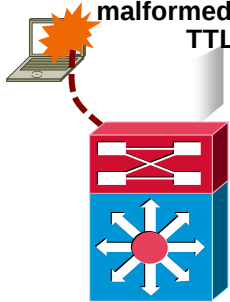


Flexible NetFlow Automation with EEM

Embedded Event Manager

Example I: Malformed Packets Detection & Reporting

Attacker sending
malformed pkts with
TTL=0



NetFlow cache

srcIf	SrcIPadd	DstIf	DstIPadd	TTL
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	0
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	10
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	200

TTL = 0 triggers an EEM event

```
*MAR 29 2010 12:29:02.604 UTC:  
%HA_EM-6-LOG: my-ttl-applet: flow  
record with zero TTL
```

syslog message generated
based on pre-configured
policies

Example II : Anomaly Flow Detection and Mitigation

Compromised
phone sending
traffic with high rate



NetFlow cache

srcIf	SrcIPadd	DstIf	DstIPadd	bytes
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	34346
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	300
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	1000

NetFlow ED triggers policies to monitor flow rate.
Typically, voice conversations are 64kbps

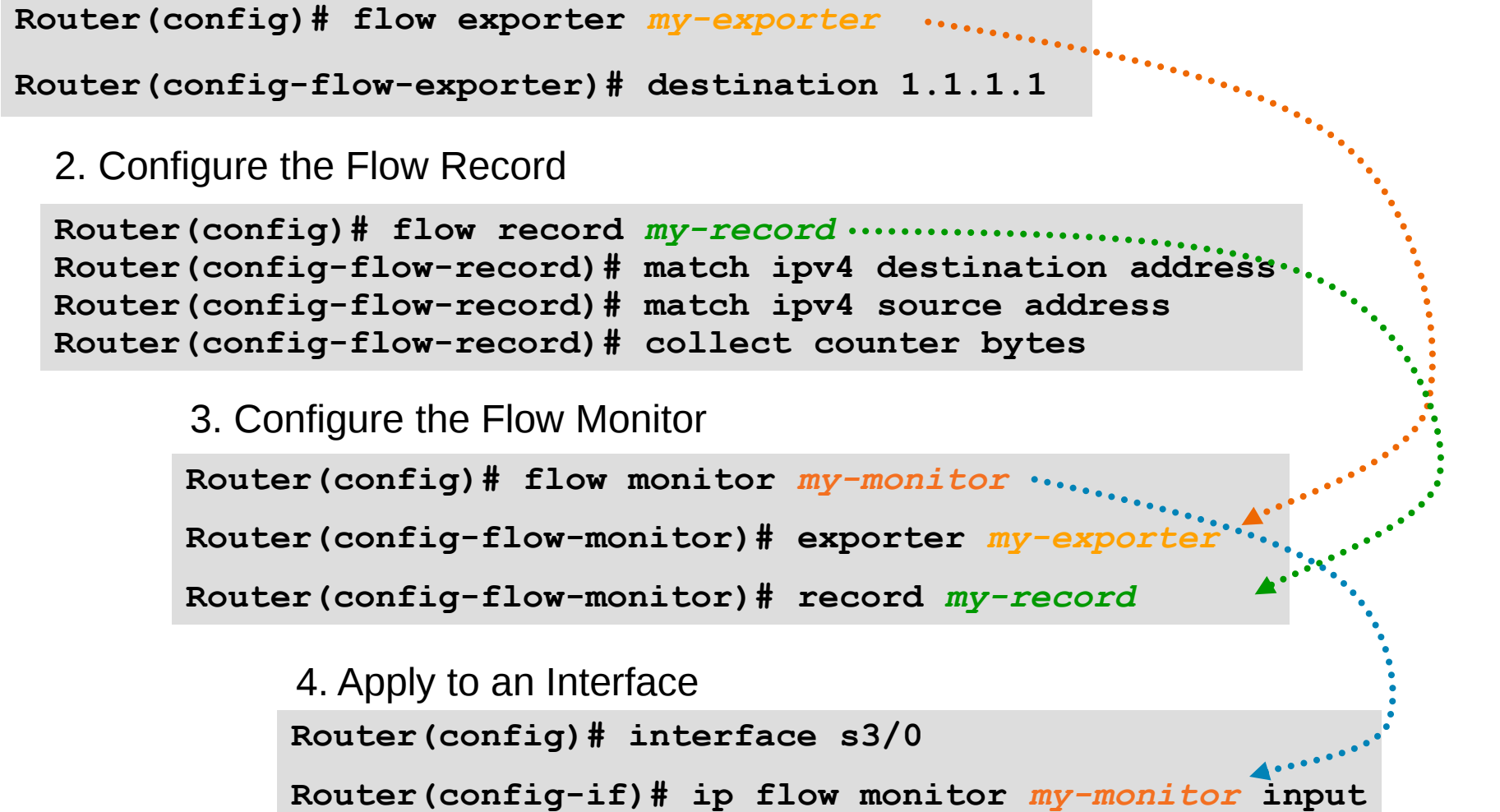
```
*Feb 18 01:24:30.455: %LINK-5-  
CHANGED: Interface FastEthernet  
1/0, changed state to  
administratively down
```

interface Fa1/0 is shut down when
the flow rate exceeds
1Mbps

Flexible NetFlow (FNF) – Configuration Example

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) – Key Fields – 1/2

Flow	IPv4		IPv6	
Sampler ID	IP (Source or Destination)	Payload Size	IP (Source or Destination)	Payload Size
Direction	Prefix (Source or Destination)	Packet Section (Header)	Prefix (Source or Destination)	Packet Section (Header)
Interface	Mask (Source or Destination)	Packet Section (Payload)	Mask (Source or Destination)	Packet Section (Payload)
Input	Minimum-Mask (Source or Destination)	TTL	Minimum-Mask (Source or Destination)	DSCP
Output	Protocol	Options bitmap	Protocol	Extension Headers
Layer 2	Fragmentation Flags	Version	Traffic Class	Hop-Limit
Source VLAN	Fragmentation Offset	Precedence	Flow Label	Length
Dest VLAN	Identification	DSCP	Option Header	Next-header
Dot1q VLAN	Header Length	TOS	Header Length	Version
Dot1q priority	Total Length		Payload Length	
Source MAC address				
Destination MAC address				

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

Routing	Transport		Application
src or dest AS	Destination Port	TCP Flag: ACK	Application ID*
Peer AS	Source Port	TCP Flag: CWR	
Traffic Index	ICMP Code	TCP Flag: ECE	
Forwarding Status	ICMP Type	TCP Flag: FIN	
IGP Next Hop	IGMP Type*	TCP Flag: PSH	
BGP Next Hop	TCP ACK Number	TCP Flag: RST	
Input VRF Name	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		

Multicast

- Replication Factor*
- RPF Check Drop*
- Is-Multicast

***: IPv4 Flow only**

Flexible NetFlow (FNF) – Non-Key Fields

Counters	Timestamp	IPv4	IPv4 and IPv6
Bytes	sysUpTime First Packet	Total Length Minimum (*)	Total Length Minimum (**)
Bytes Long	sysUpTime First Packet	Total Length Maximum (*)	Total Length Maximum (**)
Bytes Square Sum		TTL Minimum	
Bytes Square Sum Long		TTL Maximum	
Packets			
Packets Long			

- Plus any of the potential “key” fields: will be the value from the first packet in the flow

(*) IPV4_TOTAL_LEN_MIN, IPV4_TOTAL_LEN_MAX
(**)IP_LENGTH_TOTAL_MIN, IP_LENGTH_TOTAL_MAX

Three Types of NetFlow Caches

- Normal cache (traditional NetFlow)
 - More flexible active and inactive timers: one second minimum
- Immediate cache
 - Flow accounts for a single packet
 - Desirable for real-time traffic monitoring, DDoS detection, logging
 - Desirable when only very small flows are expected (ex: sampling)
 - Caution: may result in a large amount of export data
- Permanent cache
 - To track a set of flows without expiring the flows from the cache
 - Entire cache is periodically exported (update timer)
 - After the cache is full (size configurable), new flows will not be monitored
 - Uses update counters rather than delta counters

Flexible NetFlow (FNF) – Top Talkers Example

- 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 (FNF) and EEM – Low-TTL Detection

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

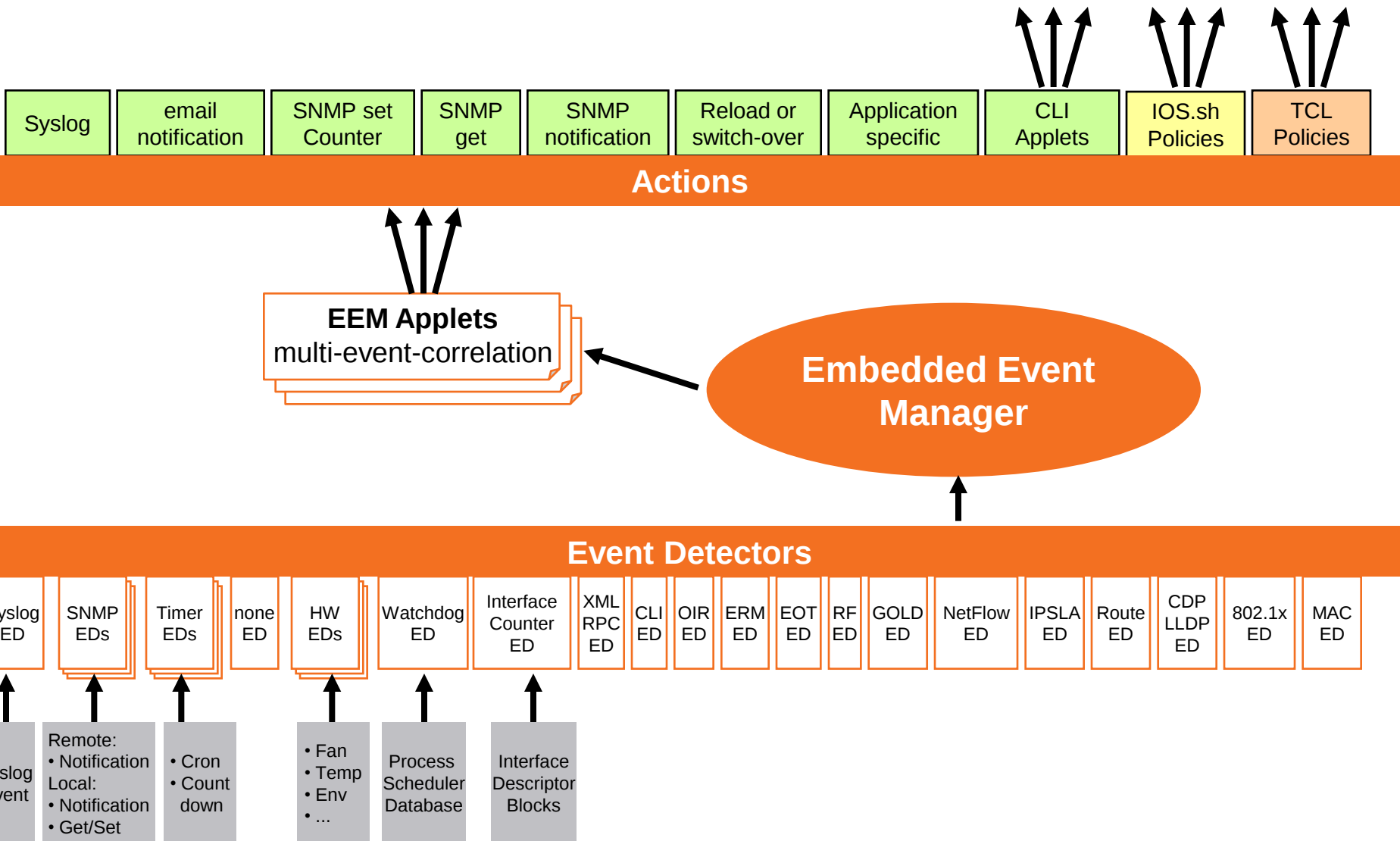
```
event manager applet my-ttl-applet
  event nf monitor-name "my-ttl-monitor" event-type create event1
  entry-value "5" field ipv4 ttl entry-op lt
  action 1.0 syslog msg "Low-TTL flow from $_nf_source_address"
```

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
```

Service Planning

EEM Architecture



Access platforms supporting Flexible Netflow

SUPERVISOR ENGINE 7-E

- Optimized for Large Campus
- 848 Gbps Switching Capacity
- 250 MPPS, 256K Routes
- Flexible Netflow
- Wireshark Services
- TrustSec, VSS*



SUPERVISOR ENGINE 7L-E

- Optimized for Small/Mid Size Campus
- 520 Gbps (48G/slot)
- 225 MPPS, 64K Routes
- Flexible Netflow
- Wireshark Services



New Module: 3KX-SM-10G

- Services module for the Catalyst 3750X and 3560X models
- Capable of Flexible Network in HW
- Line rate – 40 Gbps
- Supports Netflow version 9
- Available in the IP Base and above
- Capable of Switch-to-Switch MACSec (802.1ae)



* Roadmap

*** 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 a great thing ...

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

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

Agenda

The Evolving Network Edge

- **Power Technologies & Management**

- PoE – 802.3af, 802.3at and beyond
 - Energy Efficient Ethernet
 - EnergyWise
 - StackPower + PoE-Passthrough

- **Neighboring Services & QoS**

- CDP, LLDP, LLDP-MED
 - Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

- Auto-Smartports & Smartinstall
 - Netflow / Flexible Netflow

GOLD



Troubleshooting & Optimization

Generic OnLine Diagnostics (GOLD)

CLI and scheduling for Functional Runtime Diagnostics

- Bootup Diagnostics (upon bootup and OIR)
- Periodic Health Monitoring (during operation)
- OnDemand (from CLI)
- Scheduled Testing (from CLI)
- Test Types include:

- Packet switching tests

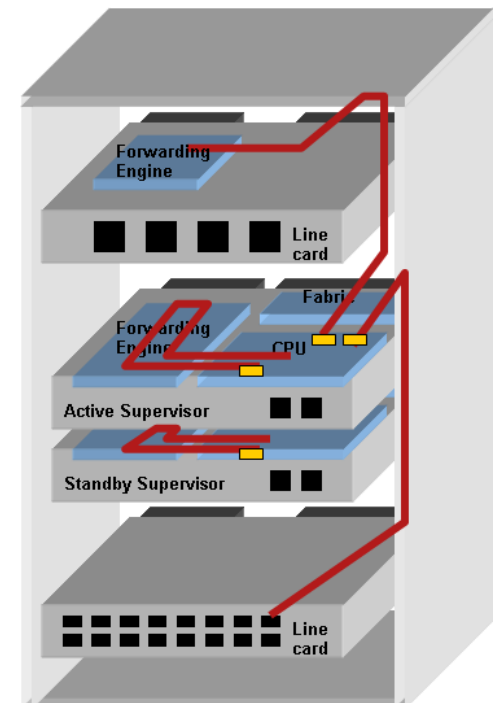
- Are supervisor control plane & forwarding plane functioning properly?
- Is the standby supervisor ready to take over?
- Are linecards forwarding packets properly?
- Are all ports working?
- Is the backplane connection working?

- Memory Tests

- Error Correlation Tests

- Complementary to POST

Good Practice: schedule all non-disruptive tests periodically



Available from: CatOS 8.5(1), IOS 12.2(14)SX

Platforms: CBS 3xxx, Cat 3560, 3750, 6500, ME6524, 72xx, 10k, CRS

Summary

The Evolving Network Edge

- **Power Technologies & Management**

PoE – 802.3af, 802.3at and beyond
Energy Efficient Ethernet
StackPower + PoE-Passthrough
EnergyWise

- **Neighboring Services & QoS**

CDP, LLDP, LLDP-MED
Dynamic Quality of Service

- **Intelligent Operations & Monitoring**

Auto-Smartports & Smartinstall
Netflow / Flexible Netflow

- **Security Mechanisms**

 - Přednáška T-NET3**

 - IEEE 802.1X Authentication
 - TrustSec, MacSec - IEEE 802.1AE

 - Přednáška T-NET5**

 - IPv6



Incorporating the intelligent Access Layer



Mobility

Convergence of wired and wireless



Green

Rising energy costs, corporate sustainability mandates



Security

Provide secure access while managing explosive growth in number of devices accessing the network



Application Performance

Need to closely manage applications for optimum performance



Voice/Video

Growth of video outstripping growth of access network resources

Simplify Operations, reduce management complexity

When the Network Access Knows

Otázky a odpovědi

- Twitter www.twitter.com/CiscoCZ
 - Talk2Cisco www.talk2cisco.cz/dotazy
 - SMS 721 994 600
-
- Zveme Vás na **Ptali jste se...** v sále **LEO**
1.den 17:45 – 18:30
2.den 16:30 – 17:00

**Prosíme, ohodnot'te
tuto přednášku.**

