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](www.twitter.com/CiscoCZ)
- Talk2cisco  [www.talk2cisco.cz/dotazy](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)

```plaintext
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
```
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**
  - **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!

<table>
<thead>
<tr>
<th>Device</th>
<th>Power Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP-1200 802.11b/g</td>
<td>6.2 W</td>
</tr>
<tr>
<td>IP Phone 7970G 802.11n</td>
<td>10.25 W</td>
</tr>
<tr>
<td>AP – 1250 802.11n</td>
<td>20 W</td>
</tr>
<tr>
<td>IP Phone 9971 802.11n</td>
<td>28.8 W</td>
</tr>
</tbody>
</table>

15.4 Watts are enough for most PD devices today

But a number of devices today require more power!

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

© 2012 Cisco and/or its affiliates. All rights reserved.
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)

# Power over Ethernet

## Detect, Classification & Power Up

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

---

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

<table>
<thead>
<tr>
<th>Temperatur e Rise</th>
<th>Max Current per twisted Pair</th>
<th>Max Power @ 50V</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>420mA</td>
<td>37.5W</td>
</tr>
<tr>
<td>7.5</td>
<td>520mA</td>
<td>45.2W</td>
</tr>
<tr>
<td>10</td>
<td>600mA</td>
<td>51.0W</td>
</tr>
<tr>
<td>12.5</td>
<td>670mA</td>
<td>55.8W</td>
</tr>
<tr>
<td>15</td>
<td>720mA</td>
<td>59.0W</td>
</tr>
</tbody>
</table>

### ISO/IEC Recommendation

<table>
<thead>
<tr>
<th>Temperatur e Rise</th>
<th>Max Current per twisted Pair</th>
<th>Max Power @ 50V</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>420mA</td>
<td>37.5W</td>
</tr>
<tr>
<td>7.5</td>
<td>550mA</td>
<td>47.4W</td>
</tr>
<tr>
<td>10</td>
<td>600mA</td>
<td>51.0W</td>
</tr>
<tr>
<td>12.5</td>
<td>680mA</td>
<td>56.4W</td>
</tr>
<tr>
<td>15</td>
<td>720mA</td>
<td>59.0W</td>
</tr>
</tbody>
</table>

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

PD Powered Compact Switches

- 60W
- 7W
- 15W

Desktop Virtualization
VDI Clients
VDI Enabled Displays
Physical Security
IP Phones Video
Personal Telepresence
Physical Access
Controller
Netbooks
Use case for UPoE
VDI Clients

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

Wyse ThinClient
Cisco Standalone
Cisco Integrated
Integrated Display
Repurposed PC

Universal PoE
0 W
15 W
20 W
25 W
48 W
60 W
80 W
90 W
# PoE Supported Products

<table>
<thead>
<tr>
<th>Products</th>
<th>802.3af (15W)</th>
<th>EPoE (20W)</th>
<th>802.3at (30W)</th>
<th>UPOE (60W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 2960S</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 3560E/3750E</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 3560X/3750X</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 4500</td>
<td>Yes</td>
<td>4648-RJ45V+E</td>
<td>4748-RJ45V+E</td>
<td>4748-UPOE+E</td>
</tr>
<tr>
<td>Catalyst 6500</td>
<td>Yes</td>
<td>6148-GE-AF</td>
<td>6148E-GE-45AT</td>
<td>No</td>
</tr>
</tbody>
</table>
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)

Start time 12:33 PM 2/8/2007 (30 min)

utilization <= 1.0 %

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
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

Sleep time: ~5us  
Wake time: ~15us
Linecard to support UPoE and EEE

- 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

WS-X4748-UPOE-RJ45V+E

- 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

<table>
<thead>
<tr>
<th></th>
<th>No EEE</th>
<th>EEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Power Consumption</td>
<td>1.0 W</td>
<td>0.47W</td>
</tr>
</tbody>
</table>

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

- Rising energy costs
- IT device proliferation
- Video applications

- Regulatory compliance
- Government mandates
- Company requirements

Source: UK Energy Efficiency Best Practice Program; Energy Consumption Guide 19: Energy Use in Offices
Cisco EnergyWise Architecture
Unifies Device Energy Management

MANAGEMENT APPLICATIONS

- Energy Management Applications
- Network Management Applications
- Building Management Systems

EnergyWise Management API

Catalyst Switching Network

EnergyWise SDK / APIs  POE / POE+ / UPOE

Gateways

Build Management Protocols

Cisco and Partner Devices

POE Powered Devices

IT DEVICES

BUILDING FACILITIES
Cisco EnergyWise Architecture
Unifies Device Energy Management

MANAGEMENT APPLICATIONS

Energy Management Applications

Network Management Applications

Building Mgmt Systems

Gateways

Meters & Wiring

PDUs & UPS’s

Cisco Catalyst Switching Network

IT DEVICES

BUILDING DEVICES

EnergyWise SDK

POE / POE+ / UPOE

Building Devices

BRKCRS-2437

© 2012 Cisco and/or its affiliates. All rights reserved.

Cisco Public
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
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

<table>
<thead>
<tr>
<th>Device</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone 1</td>
<td>15 Watts</td>
</tr>
<tr>
<td>Phone 2</td>
<td>9 Watts</td>
</tr>
<tr>
<td>Phone 3</td>
<td>6 Watts</td>
</tr>
<tr>
<td>AP 1</td>
<td>1 Watt</td>
</tr>
<tr>
<td>AP 2</td>
<td>2 Watts</td>
</tr>
</tbody>
</table>

IP Phones and Access Points
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**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Name</th>
<th>Usage</th>
<th>Category</th>
<th>Caliber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/4</td>
<td>SEP000E84C063C1</td>
<td>1.9 (W)</td>
<td>consumer</td>
<td>actual</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>PVC300-1</td>
<td>4.4 (W)</td>
<td>consumer</td>
<td>actual</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Gi1.0.6 SEP5475D02B3F46</td>
<td>2.1 (W)</td>
<td>meter</td>
<td>actual</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>Gi1.0.7 SEP8CB64FF6723F</td>
<td>6.0 (W)</td>
<td>consumer</td>
<td>presumed</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>Gi1.0.8 SEP5475D02B40BE</td>
<td>2.2 (W)</td>
<td>meter</td>
<td>actual</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>Gi1.0.10 SEPC0626B62AE93</td>
<td>6.1 (W)</td>
<td>meter</td>
<td>actual</td>
</tr>
</tbody>
</table>

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

Set
Keyword HQ
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
# IP Phone Power States

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Name</th>
<th>Usage</th>
<th>Lvl</th>
<th>Imp</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE Switch</td>
<td></td>
<td>C3750</td>
<td>86.0 (W)</td>
<td>10</td>
<td>1</td>
<td>parent</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Id</th>
<th>Neighbor Name</th>
<th>Ip:Port</th>
<th>Prot</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TG3560G-21</td>
<td>2.2.2.21:43440</td>
<td>udp</td>
<td>S I</td>
</tr>
<tr>
<td>2</td>
<td>TG3560G-31</td>
<td>2.2.4.31:43440</td>
<td>static</td>
<td>S I</td>
</tr>
<tr>
<td>3</td>
<td>TG3560G-22</td>
<td>2.2.2.22:43440</td>
<td>cdp</td>
<td>S I</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Host</th>
<th>Name</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.21</td>
<td>phone</td>
<td>15.4 (W)</td>
</tr>
<tr>
<td>2.2.2.22</td>
<td>phone</td>
<td>15.4 (W)</td>
</tr>
</tbody>
</table>

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)SXI4
- 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 another 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

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

<table>
<thead>
<tr>
<th>Available Pwr</th>
<th>Allocated Pwr</th>
<th>Unused Pwr</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,300 W</td>
<td>2,000 W</td>
<td>1,300 W</td>
</tr>
</tbody>
</table>

Redundant mode

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.

Reserved Power 1,100w
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

Catalyst 2960/3560-C – PoE+ Powered, Pass-Through PoE
## POE Budget for connected Devices

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

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Powering Options</th>
<th>Available PoE Power (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C2960CPD-8PT-L</td>
<td>1 PoE Uplink</td>
<td>0W</td>
</tr>
<tr>
<td></td>
<td>2 PoE Uplinks</td>
<td>7W</td>
</tr>
<tr>
<td></td>
<td>1 PoE+ Uplinks</td>
<td>7W</td>
</tr>
<tr>
<td></td>
<td>1 PoE+ and 1 PoE Uplinks</td>
<td>15.4W</td>
</tr>
<tr>
<td></td>
<td>2 PoE+ Uplinks</td>
<td>22.4W</td>
</tr>
<tr>
<td></td>
<td>Auxiliary Input</td>
<td>22.4W</td>
</tr>
<tr>
<td>WS-C3560CPD-8PT-S</td>
<td>1 PoE+</td>
<td>0W</td>
</tr>
<tr>
<td></td>
<td>2 PoE+</td>
<td>15.4W</td>
</tr>
<tr>
<td></td>
<td>Auxiliary Input</td>
<td>15.4W</td>
</tr>
</tbody>
</table>

*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
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

---

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

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

---

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
```

---

LLDP-MED and Cisco Discovery Protocol,
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

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.

Trust Boundary

Voice VLAN Traffic
is Trusted

Voice and Video traffic on the
Data VLAN Traffic

Data VLAN Traffic
untrusted marked
CoS 0
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 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

<table>
<thead>
<tr>
<th>TLV Type</th>
<th>Network Policy String Length</th>
<th>TIA OUI</th>
<th>Network Policy Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>127</td>
<td>8</td>
<td>00-12-8B</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Type</th>
<th>U</th>
<th>T</th>
<th>X</th>
<th>VLAN ID</th>
<th>L2 Priority</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network Policy (4 octets)
Campus QoS Designs are evolving
Business and Technical Drivers

- 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

64% of communication is non-verbal\(^1\)

One third of the human cortex is dedicated to vision\(^2\)


\(^2\)Vision Group Research, FMRIB, University of Oxford, UK
Evolving Business Requirements
Business Requirements Will Evolve and Expand over Time

4-Class Model
- Realtime
- Critical Data
- Signaling / Control
- Best Effort

8-Class Model
- Voice
- Interactive Video
- Streaming Video
- Call Signaling
- Network Control
- Critical Data
- Best Effort
- Scavenger

12-Class Model
- Voice
- Realtime Interactive
- Multimedia Conferencing
- Broadcast Video
- Multimedia Streaming
- Call Signaling
- Network Control
- Network Management
- Transactional Data
- Bulk Data
- Best Effort
- Scavenger

Enterprise Medianet Quality of Service Design 4.0
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 packets from untrusted device
  - 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
- 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

```bash
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

- **Device UP** trigger detected
- **Device Macro** applied
- **Device DOWN** detected
- **Device Anti-Macro** applied

---

**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

---

```
function CISCO_DMP_AUTO_SMARTPORT () {
  if ([ $LINKUP -eq YES ]; then
    conf $INTERFACE
    interface $INTERFACE
    macro description $TRIGGER
    switchport access vlan $ACCESS_VLAN
    switchport mode access
    switchport block unicast
    mls qos trust deep
    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 $INTERFACE
    interface $INTERFACE
    no macro description $TRIGGER
    no switchport access vlan $ACCESS_VLAN
    no switchport mode access
    no switchport block unicast
    no mls qos trust deep
    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
```
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)

- Flexible NetFlow
  
  Advantages: cache and export content flexibility
  
  User selection of flow keys
  
  User definition of the records
Traditional NetFlow vs. Flexible NetFlow

**Tradational NetFlow**
- Fixed definition of flow record globally
- Export only to one collector

<table>
<thead>
<tr>
<th>NetFlow Cache</th>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Protocol</th>
<th>SrcPort</th>
<th>DstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.100.21.2</td>
<td>Fa0/0</td>
<td>10.0.227.11</td>
<td>00A2</td>
<td>00A2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.3.2</td>
<td>Fa0/0</td>
<td>10.0.227.6</td>
<td>15</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.20.2</td>
<td>Fa0/0</td>
<td>10.0.227.11</td>
<td>00A1</td>
<td>00A1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.6.2</td>
<td>Fa0/0</td>
<td>10.0.227.6</td>
<td>19</td>
<td>19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Flexible NetFlow**
- Flow Monitor 1
- Flow Monitor 2
- Flow Monitor 3

**Flexible definition of flow records applied to selected interface or VLAN**

**Ability to export flow information to multiple collectors/analyzers**

**Flow cache 1**
- DstIPadd: 10.0.227.12
- Protocol: 11
- TOS: 80

**Flow cache 2**
- DstIPadd: 10.0.227.12
- Protocol: 6
- TOS: 40

**Flow cache 3**
- DstIPadd: 10.0.227.12
- Protocol: 11
- TOS: 80

**Destination 1**
- IT team#1
- Security focused analyzer

**Destination 2**
- IT team#2
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

<table>
<thead>
<tr>
<th>srcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>0</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>10</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>200</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>srcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>34346</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>300</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.1.1.2</td>
<td>Fa0/0</td>
<td>10.0.277.1</td>
<td>1000</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Flow</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampler ID</td>
<td>IP (Source or Destination)</td>
<td>IP (Source or Destination)</td>
</tr>
<tr>
<td>Direction</td>
<td>Payload Size</td>
<td>Payload Size</td>
</tr>
<tr>
<td>Interface</td>
<td>Prefix (Source or Destination)</td>
<td>Prefix (Source or Destination)</td>
</tr>
<tr>
<td>Input</td>
<td>Packet Section (Header)</td>
<td>Packet Section (Header)</td>
</tr>
<tr>
<td>Output</td>
<td>Packet Section (Payload)</td>
<td>Packet Section (Payload)</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Mask (Source or Destination)</td>
<td>Mask (Source or Destination)</td>
</tr>
<tr>
<td>Source VLAN</td>
<td>Minimum-Mask (Source or Destination)</td>
<td>Minimum-Mask (Source or Destination)</td>
</tr>
<tr>
<td>Dest VLAN</td>
<td>TTL</td>
<td>DSCP</td>
</tr>
<tr>
<td>Dot1q VLAN</td>
<td>Protocol</td>
<td>Protocol</td>
</tr>
<tr>
<td>Dot1q priority</td>
<td>Fragmentation Flags</td>
<td>Extension Headers</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>Fragmentation Offset</td>
<td>Traffic Class</td>
</tr>
<tr>
<td>Destination</td>
<td>Identification</td>
<td>Flow Label</td>
</tr>
<tr>
<td>MAC address</td>
<td>Header Length</td>
<td>Length</td>
</tr>
<tr>
<td>Total Length</td>
<td>Total Length</td>
<td>Option Header</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Next-header</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Header Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Payload Length</td>
</tr>
</tbody>
</table>
## Flexible NetFlow (FNF) – Key Fields – 2/2

<table>
<thead>
<tr>
<th>Routing</th>
<th>Transport</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>src or dest AS</td>
<td>Destination Port</td>
<td>Application ID*</td>
</tr>
<tr>
<td>Peer AS</td>
<td>Source Port</td>
<td></td>
</tr>
<tr>
<td>Traffic Index</td>
<td>ICMP Code</td>
<td></td>
</tr>
<tr>
<td>Forwarding Status</td>
<td>ICMP Type</td>
<td></td>
</tr>
<tr>
<td>IGP Next Hop</td>
<td>IGMP Type*</td>
<td></td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>TCP ACK Number</td>
<td>TCP Flag: FIN</td>
</tr>
<tr>
<td><strong>Input VRF Name</strong></td>
<td>TCP Header Length</td>
<td>TCP Flag: FIN</td>
</tr>
<tr>
<td></td>
<td>TCP Sequence Number</td>
<td>TCP Flag: SYN</td>
</tr>
<tr>
<td></td>
<td>TCP Window-Size</td>
<td>TCP Flag: URG</td>
</tr>
<tr>
<td></td>
<td>TCP Source Port</td>
<td>UDP Message Length</td>
</tr>
<tr>
<td></td>
<td>TCP Destination Port</td>
<td>UDP Source Port</td>
</tr>
<tr>
<td></td>
<td>TCP Urgent Pointer</td>
<td>UDP Destination Port</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: ACK</td>
<td>TCP Flag: CWR</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: CWR</td>
<td>TCP Flag: ECE</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: ECE</td>
<td>TCP Flag: FIN</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: FIN</td>
<td>TCP Flag: PSH</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: RST</td>
<td>TCP Flag: SYN</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: SYN</td>
<td>TCP Flag: URG</td>
</tr>
<tr>
<td></td>
<td>TCP Flag: URG</td>
<td>UDP Message Length</td>
</tr>
<tr>
<td></td>
<td>TCP Sequence Number</td>
<td>UDP Source Port</td>
</tr>
<tr>
<td></td>
<td>TCP Window-Size</td>
<td>UDP Destination Port</td>
</tr>
<tr>
<td></td>
<td>TCP Source Port</td>
<td>TCP Flag: ACK</td>
</tr>
</tbody>
</table>

* IPv4 Flow only
**Flexible NetFlow (FNF) – Non-Key Fields**

<table>
<thead>
<tr>
<th>Counters</th>
<th>Timestamp</th>
<th>IPv4</th>
<th>IPv4 and IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>sysUpTime First Packet</td>
<td>Total Length Minimum (*)</td>
<td>Total Length Minimum (**)</td>
</tr>
<tr>
<td>Bytes Long</td>
<td>sysUpTime First Packet</td>
<td>Total Length Maximum (*)</td>
<td>Total Length Maximum (**)</td>
</tr>
<tr>
<td>Bytes Square Sum</td>
<td></td>
<td>TTL Minimum</td>
<td></td>
</tr>
<tr>
<td>Bytes Square Sum Long</td>
<td></td>
<td>TTL Maximum</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets Long</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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>
   :
   ```

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

   ```
   ```
**Service Planning**

**EEM Architecture**

**Actions**

- Syslog
- email notification
- SNMP set Counter
- SNMP get
- SNMP notification
- Reload or switch-over
- Application specific
- CLI Applets
- IOS.sh Policies
- TCL Policies

**EEM Applets**

- multi-event-correlation

**Event Detectors**

- Syslog ED
- SNMP EDs
- Timer EDs
- none ED
- HW EDs
- Watchdog ED
- Interface Counter ED
- XML RPC ED
- CLI ED
- OIR ED
- ERM ED
- EOT ED
- RF ED
- GOLD ED
- NetFlow ED
- IPSLA ED
- Route ED
- CDP LLDP ED
- 802.1x ED
- MAC ED

**Syslog Event**

- Remote:
  - Notification
  - Local:
  - Notification
  - Get/Set

- Cron
- Temp
- Env
- ...

**Process Scheduler Database**

**Interface Descriptor Blocks**
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)
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

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](http://www.twitter.com/CiscoCZ)
- Talk2Cisco  [www.talk2cisco.cz/dotazy](http://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, ohodnoťte tuto přednášku.