# Das Design muss mitwachsen: Der Einfluss der neuen Endgeräte-Vielfalt auf das Campus Design mit Catalyst Switches

**Dieter Hadwiger – SE – dhadwige@cisco.com**

**Gerd Pflueger – CSE – gerd@cisco.com**

# Abstract

- Das Design muss mitwachsen: Der Einfluss der neuen Endgeräte-Vielfalt auf das Campus Design mit Catalyst Switches

  Eine immer groessere werdende Anzahl von neuen Endgeraeten findet sich heute in den modernen Firmen-Netzwerken. Waren es frueher "nur" PC, die an den Etagenswitches angeschlossen worden sind, so finden wir heute neben Notebooks auch Kameras, WLAN Accesspoint oder auch Softphones auf Desktop-Rechnern vor. In unserem Vortrag werden wir beleuchten, welchen Einfluss diese neue Klasse von Endgeraeten auf den Etagenswitch hat und welche Auswirkungen auf das Netzwerkdesign zu erwarten sind. Betrachten Sie mit uns die verschiedenen Optionen zum automatisierten Management, die Ihnen die intelligenten Access-Switches von Cisco heute schon bieten.

# Key-Objectives

- Entwicklungen im Bereich PoE
- Anforderungen durch QoS am Access-Switch
- Moeglichkeiten der Automatisierung durch Auto-Smartports

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

**Selbst-Konfigurierender Access-Layer**

- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

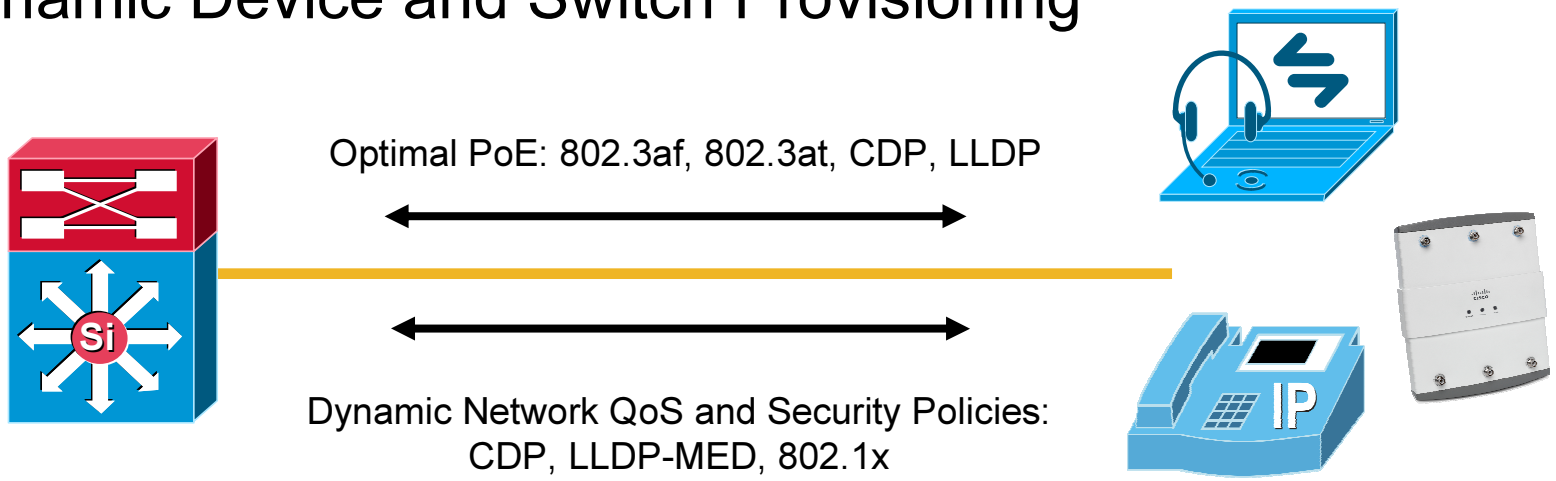
# Evolution of Switching Design

## Evolving Requirements and Technology

- The access environment is becoming more specialized to meet the needs of the evolving endpoints
- Campus
  - Desktop based Unified Communications
  - Collaborative applications
  - High Definition Video
- Data Center
  - Virtualization (FCoE, DCE, VNTag)
  - Low Latency (Grid, Cluster and HPC)
- Emerging Technology
  - 802.11n, 802.3at, 802.3az, LLDP-MED, Deep packet inspection

# 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
  - 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

# 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 qos voip cisco-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

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

**Selbst-Konfigurierender Access-Layer**

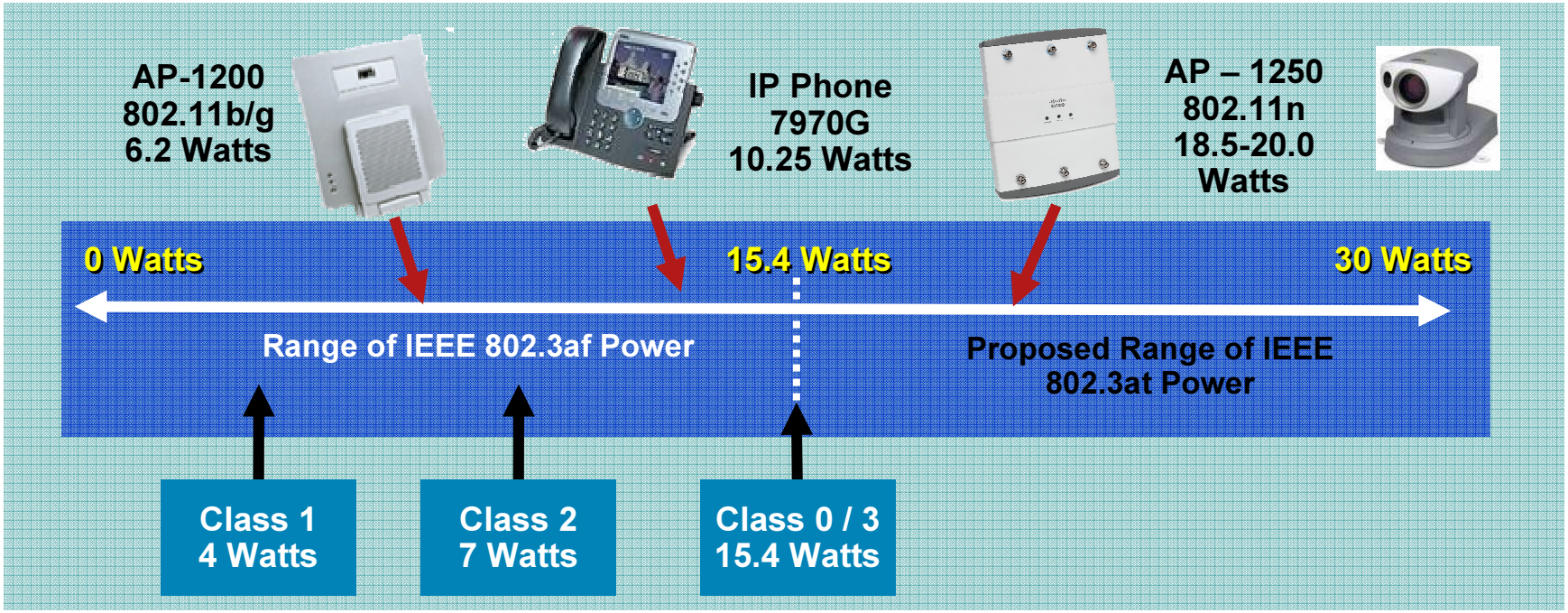
- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

# Evolving Layer 1 Services

## Evolving PoE Requirements

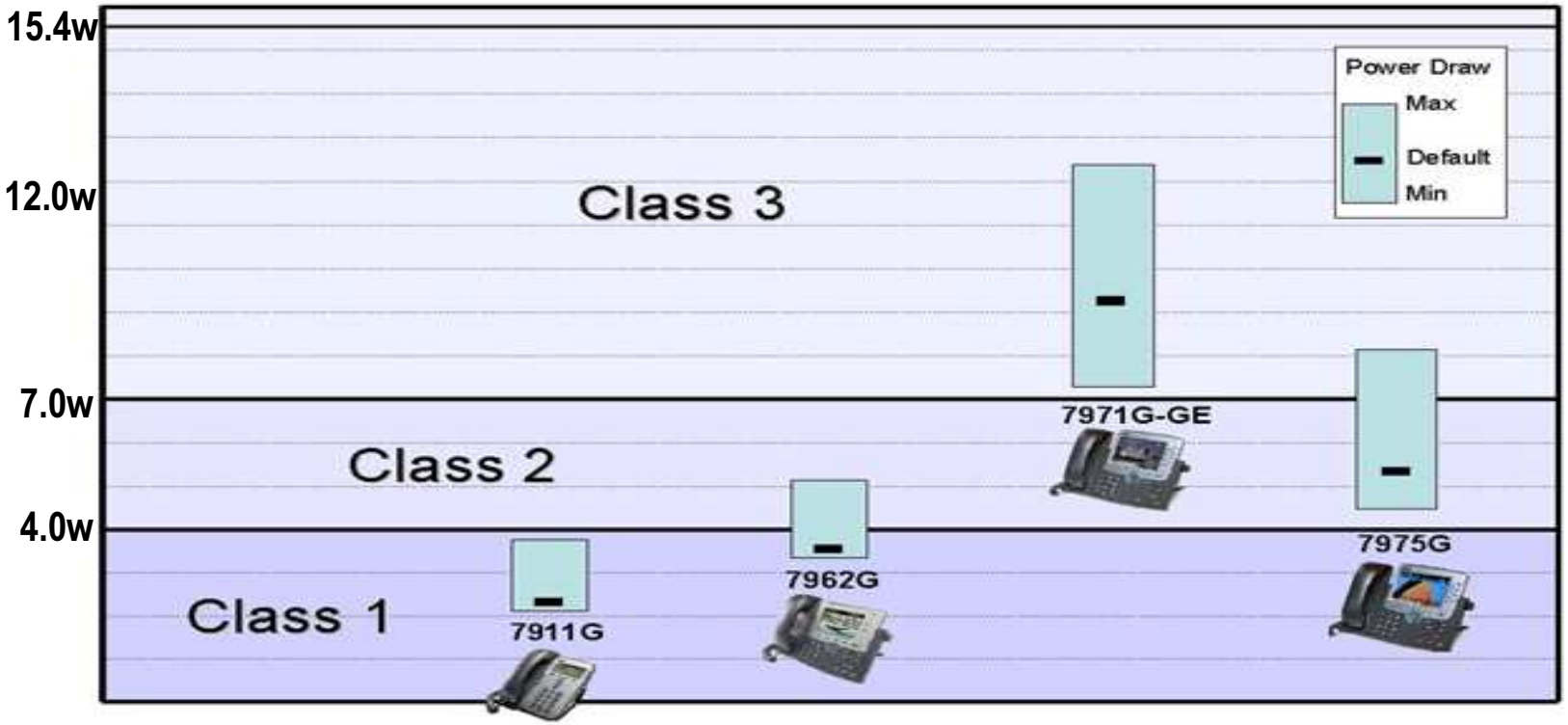
- **Endpoint power requirements are increasing**
  - **Dual Radio AP's, Remote Controlled Video Camera's**
- **Green initiatives**
- **802.3at standard estimated to be ratified September 2009**
- **Need for Granular power negotiation 'and' increased power**



# Power Over Ethernet

## Power Utilization and IEEE 802.3af Classes

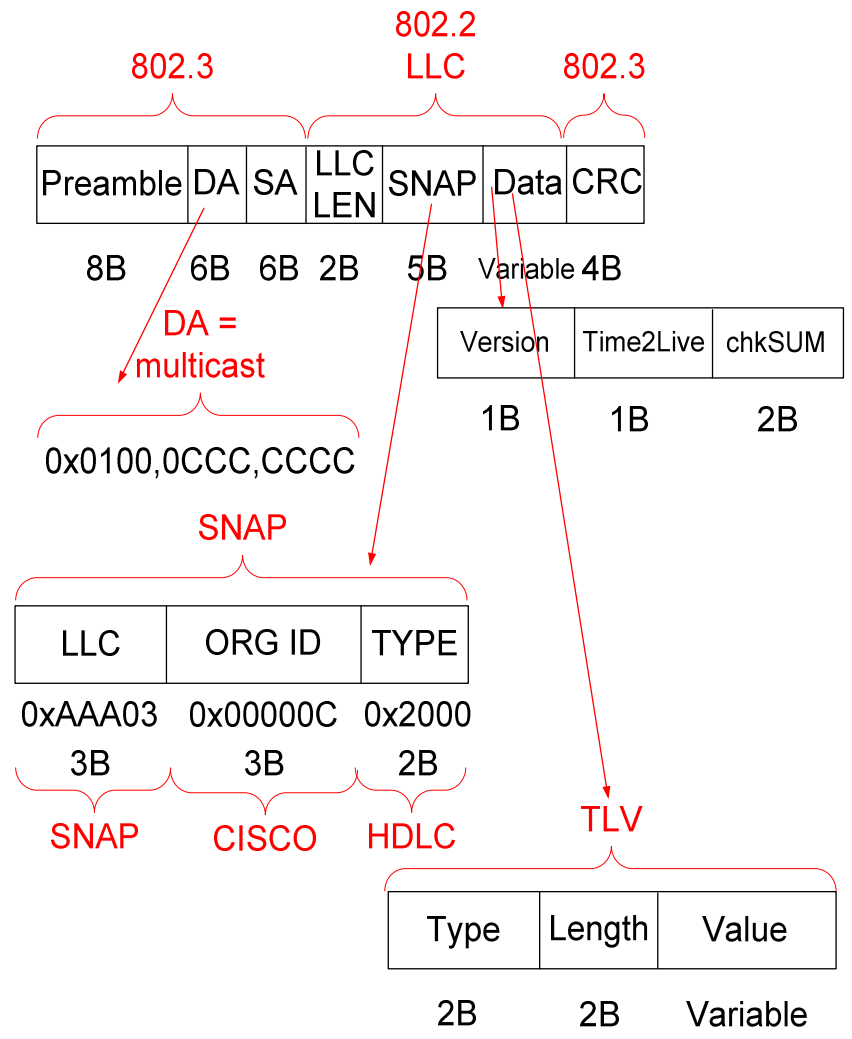
- Power utilization for a device does not fall cleanly along power classification lines
- Power optimizations involve both granular power negotiation capabilities as well as power monitoring and tuning



# Power Over Ethernet

## Granular PoE negotiation

- Two potential mechanisms that can be used to negotiate power
  - Layer 1 – e.g. 802.3af
  - Layer 2 – e.g. CDP
- CDP originally just provided notification of power
  - Power Consumption TLV
- Bidirectional CDP (Intelligent Power Management) provides the ability to negotiate power via a 3-way handshake
  - 1)Power Request TLV (32 bit integer measured in mW)
  - 2)Power Available TLV
  - 3)Power Consumption TLV




**CDP Frame Format**

# Power Over Ethernet

## Enhanced PoE (EPoE) – 802.11n AP's


- Enhanced PoE - greater than class 3, but less than 20 watts/port

  This is not 802.3at / PoE+
- AP1250 comes up as 802.3af class 3 device with radios disabled
- Negotiating 18.5 watts via bidirectional CDP enables both radios

| Power Mode | 802.3af | Cisco Enhanced PoE |
|---|---|---|
| Max Power at PSE | 15.4 W | 16.8-20 W |
| # of radios supported | 1 or 2 | 2 |
| MIMO Mode (Tx x Rx) | 1 radio: 2x3, 2 radios: 1x3 | 2x3 |
| Dual radio Limitations | Maximum PHY data-rate 157.5 Mbps/radio | Max PHY data-rate 300 Mbps/radio |

# Power Over Ethernet

## IEEE 802.3at (PoE+)

- IEEE PoE+ working group evolved into 802.3at

  http://www.ieee802.org/3/at/

  Should be ratified in September 2009

- As of '*today*' the standard proposes

  802.3at operates on CAT5E and higher infrastructure

  Maximum current set at 600mA (just over twice the maximum current in 802.3af - 350mA)

  Raising the minimum PSE output voltage from 44V to 50V (increases the power to the PD by 16% with virtually no cost involved)

  Max power supported at the PSE is 30W and the max power supported at the PD is 25.5W

  Support the operation of midspan PSEs for 1000BASE-T

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

**Selbst-Konfigurierender Access-Layer**

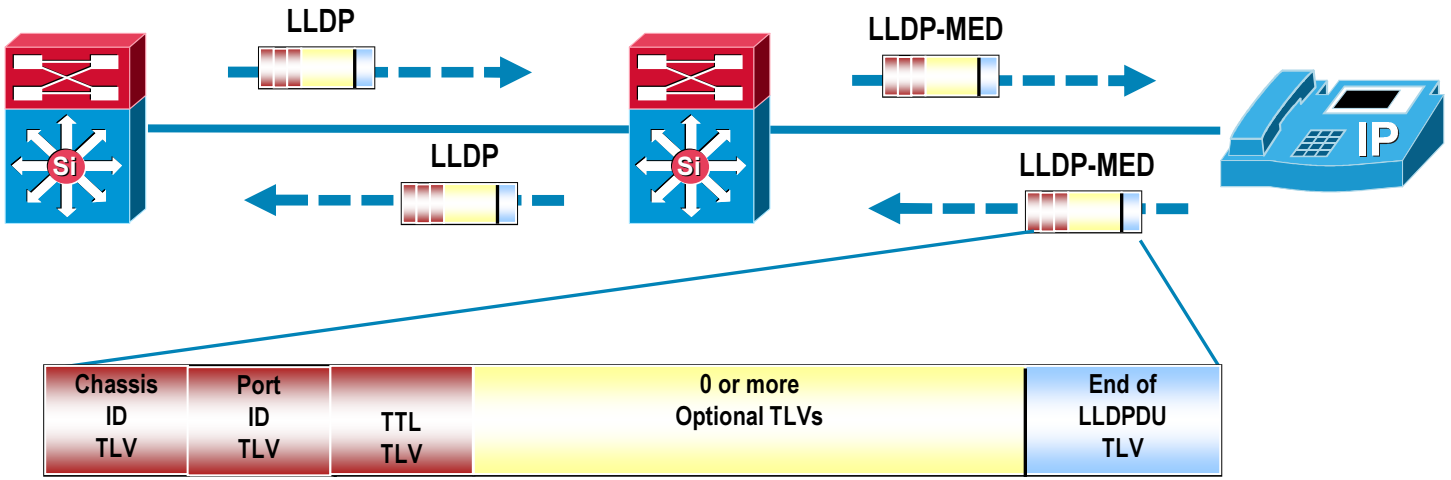
- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

# Negotiating Network Services
## LLDP, LLDP-MED

- March, 2005 IEEE-SA Standards Board approved 802.1AB (LLDP) standard
- IEEE intent that the protocol not be used for configuration purposes
- Despite IEEE, TIA standards body worked toward an adjunct standard for Link Layer Discovery Protocol for Media Endpoint Discovery (LLDP-MED) TR 41.4
- Operates in Transmit or Advertise mode only (no state kept between 2 entities)
- Periodic messages sent
- Send Device Info, Capabilities, and Media Specific Info
- 802 Link Layer protocol (no frame, ATM, … support)
- Either LLDP or LLDP-MED runs on a port, not both. LLDP-MED spec details how to transition from LLDP to LLDP-MED if an LLDP-MED endpoint is detected

# Negotiating Network Services
## LLDP, LLDP-MED




**Mandatory TLVs**
Chassis ID, Port ID, TTL

**Optional TLVs**
Port Description
System Name
System Description
System Capabilities
Management Address
Capabilities (LLDP MED)
Network (LLDP MED)
Extend Power-via-MDI (LLDP MED)
Inventory Management (LLDP MED)
IEEE 802.3 MAC/PHY Configuration/Status (LLDP MED)
Port VLAN ID (LLDP MED)

LLDP-MED TLV's designed to support VoIP endpoints

# Negotiating Network Services
## 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*

```
cr32-4500-1(config)#lldp run                                  <- Enable LLDP Globally

cr32-4500-1(config)#lldp tlv-select ?                         <- Configure Optional Global TLV's
  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 ?                  <- Configure Optional Interface TLV's
  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
```

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

# Negotiating Network Services

## CDP and LLDP

```
cr40-6500-1# sh lldp entry *
. . .
Chassis id: 0014.6947.93c0
Port id: Te3/1
Port Description: TenGigabitEthernet3/1
System Name: cr32-4500-1.cisco.com

System Description:
Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M), Version 12.2(44)
. . .
Time remaining: 96 seconds
System Capabilities: B,R
Enabled Capabilities: B,R
Management Addresses - not advertised
Auto Negotiation - supported, enabled
. .
```

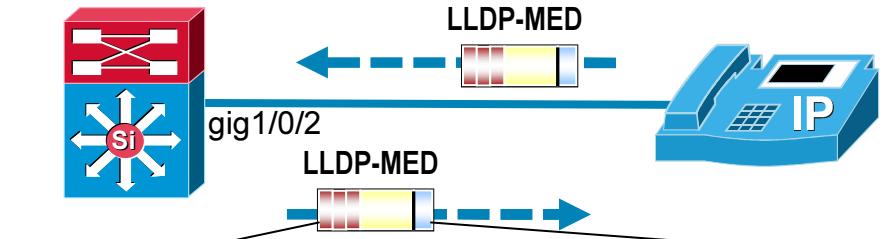
```
cr40-6500-1#sh cdp neigh ten 3/7 detail
------------------------
Device ID: cr32-4500-1
Entry address(es):
  IP address: 172.26.160.86
Platform: cisco WS-C4507R-E,  Capabilities: Router Switch IGMP
Interface: TenGigabitEthernet3/7,  Port ID (outgoing port): TenGigabitEthernet3/1
. . .
Version :
Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M), Version 12.2(44)
. . .
VTP Management Domain: 'campus3-test'
Native VLAN: 902
Duplex: full
Management address(es):
  IP address: 172.26.160.86
```

Currently CDP provides information not supported in LLDP and LLDP-MED

# Negotiating Network Services
## LLDP–MED Network Policy TLV

- Configuration is done using “network-policy” profile in Global Configuration Mode (MQC like syntax)
- Currently Network Policy supports configuration for voice & voice-signaling capabilities
  - vlan
  - cos and dscp,
  - tagging mode (dot1p/ untagged/ none)

```
network-policy profile 10
  voice vlan 100 cos 4
  voice vlan 100 dscp 34
  voice-signaling vlan 100 cos 5
  voice-signaling vlan 100 dscp 8

network-policy profile 20
  voice vlan 20 cos 3
  voice vlan 20 7

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 3 dscp 7
```




| TLV Type = 127 | Network Policy String Length = 8 | TIA OUI 00-12-BB | Network Policy Subtype = 2 | Voice | U | T | X | Vlan = 20 | Cos=3 | dscp=7 |
|---|---|---|---|---|---|---|---|---|---|---|

# Negotiating Network Services

## CDP & LLDP

| | CDP | LLDP, LLDP-MED |
|---|---|---|
| PoE | Bi-Directional CDP power negotiation | Power notification only |
| 7940, 7960 | Yes | No |
| 7941, 7961, 7970, 7971, … | Yes | Yes |
| Inventory Discovery | Yes | Yes |
| Location | Yes | Yes, additional data formats |
| Capabilities Discovery | Yes | Yes |
| QoS Trust Boundary Extension | Yes | No |
| Communication to PC running behind a phone | Yes | No, LLDP is a non bridgable frame |
| 802.1x phone bypass | Yes | No |
| Emergence Responder (E911) | Yes | No |
| Network Policy | VLAN and QoS information | VLAN and QoS information (not used by Cisco phones) |

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

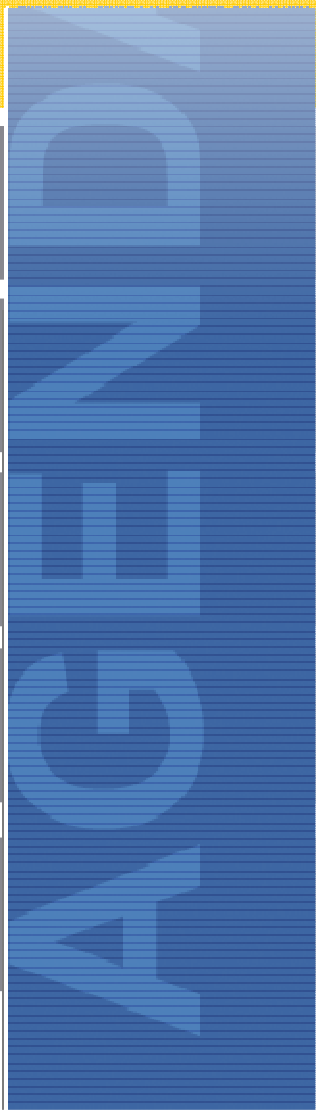
**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

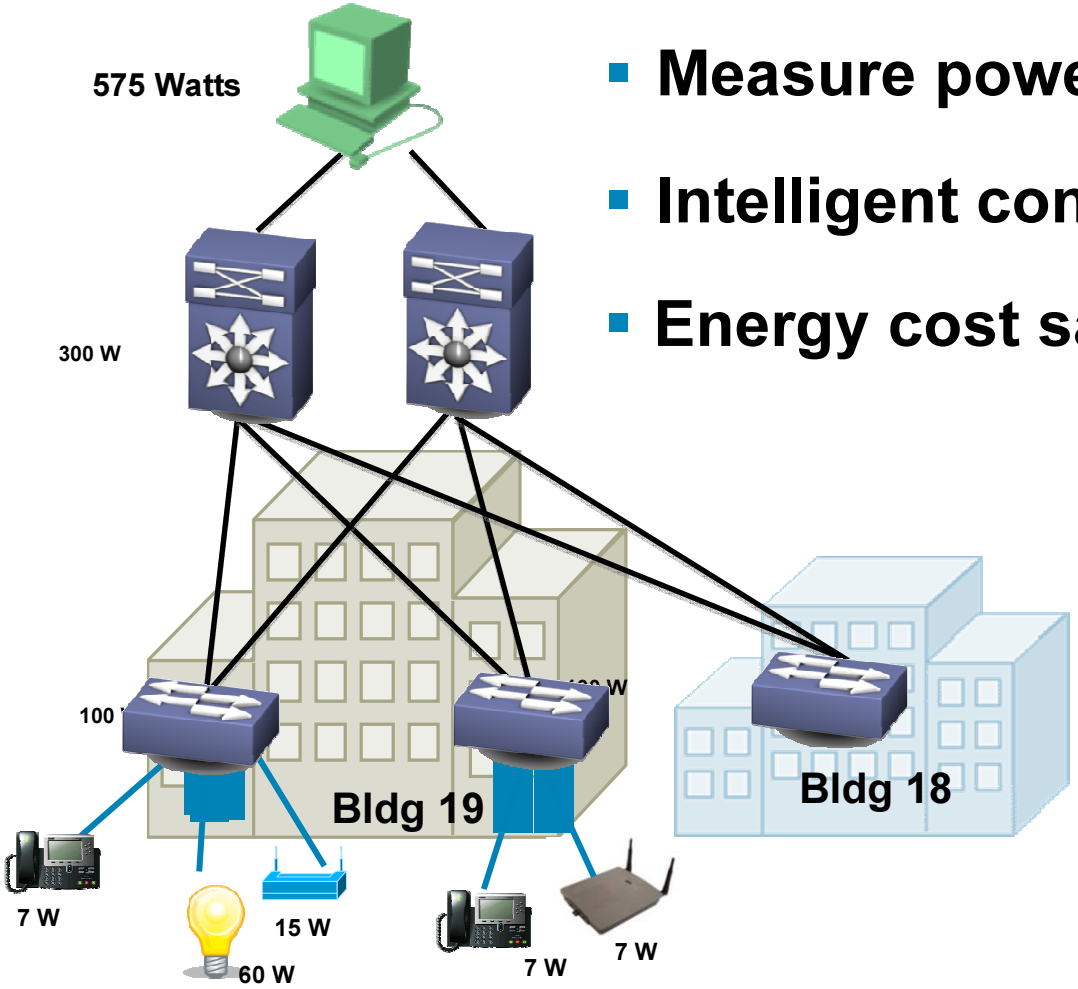
**Selbst-Konfigurierender Access-Layer**

- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

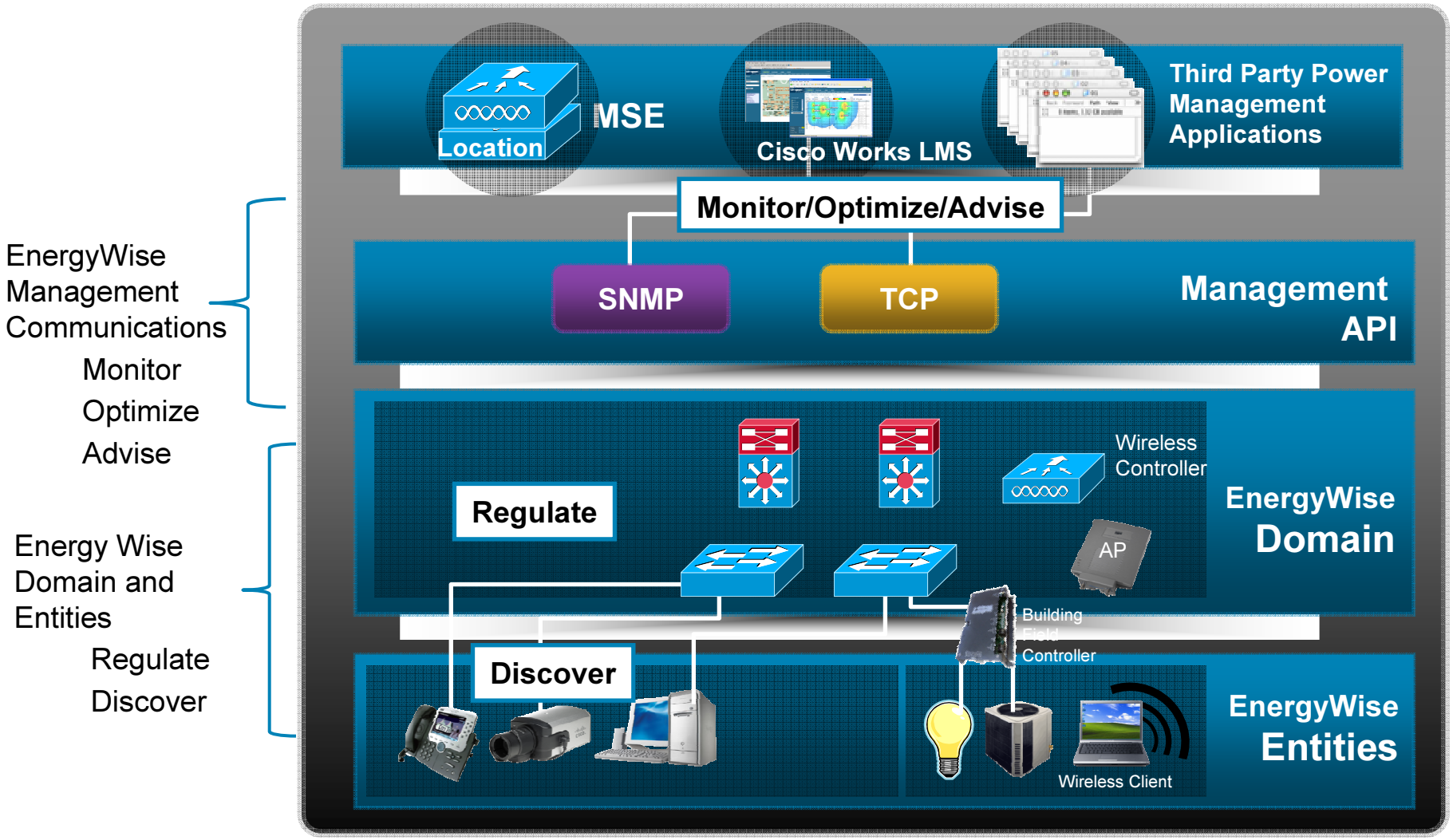


# Cisco EnergyWise




- Measure power of connected devices
- Intelligent control
- Energy cost saving

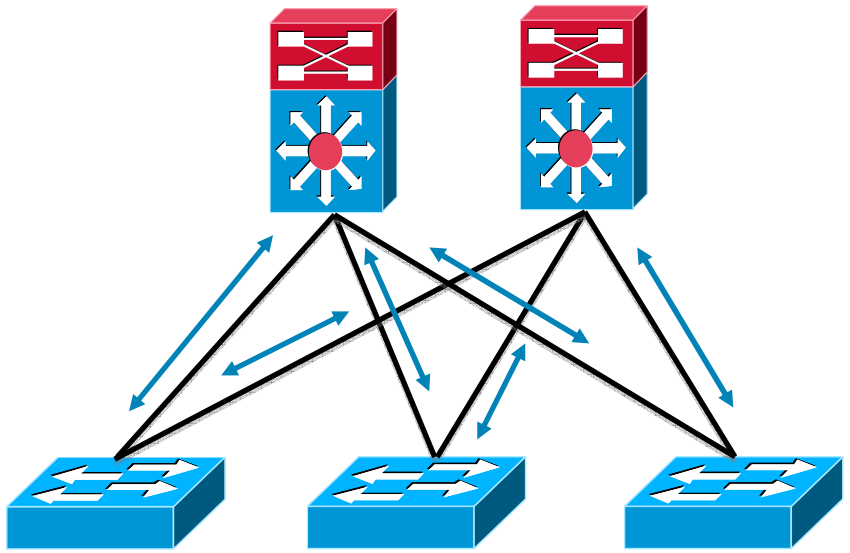
# EnergyWise Management



# Evolving Power Optimizations

## EnergyWise

- **EnergyWise -** enables the network as a platform for energy command and control
- Increase the **span of control** of the switch for power
- Provides a control framework for monitoring and managing power in both the network, attached devices along with building facilities
- Provide **time of day** controls
- Leverages CDP along with UDP to communicate power information and power control traffic



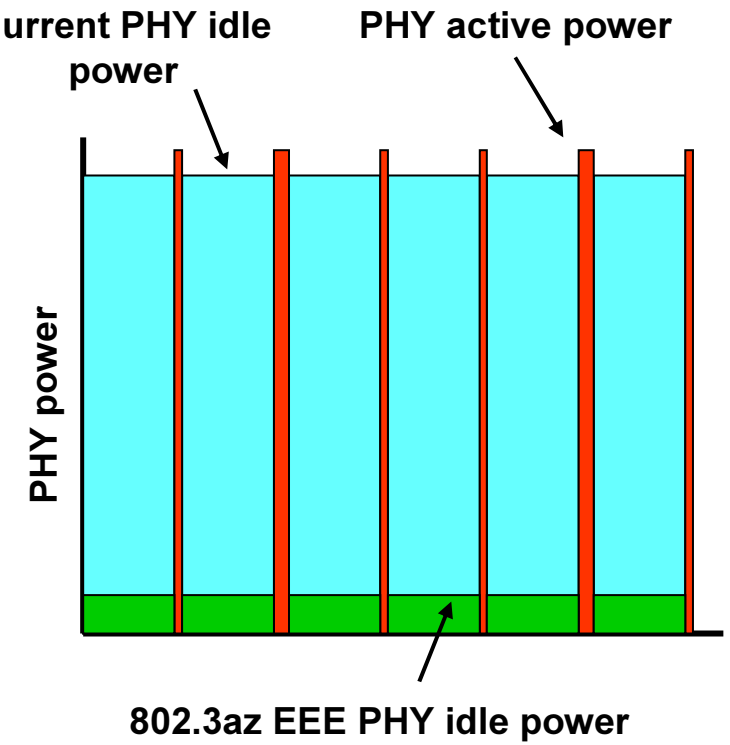
| CDP | EnergyWise TLV's |
|---|---|

```
interface FastEthernet1/0/17
 energywise level 7
 energywise importance 50
 energywise role role.lobbyaccess
 energywise name lobbyInterface.17
```

# Evolving Power Optimizations

## 802.3az – Energy Efficient Ethernet (EEE)

- IEEE Goal - Define a mechanism to reduce power consumption during periods of low link utilization
- Solutions chosen for 100 Mbps and 1Gbps: Low Power Idle (LPI)
  - PHY transmits when there's data, then sleeps
  - Significantly more efficient than constant Tx…
  - Periodic wake up to keep link fresh
- Nearly consensus for 10 Gbps: Low Power Idle (LPI) & Link Layer Discovery Protocol (LLDP)
- Projected mid 2011 for shipping implementations




Match the power of the PHY to the actual 'bursty' network traffic patterns

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

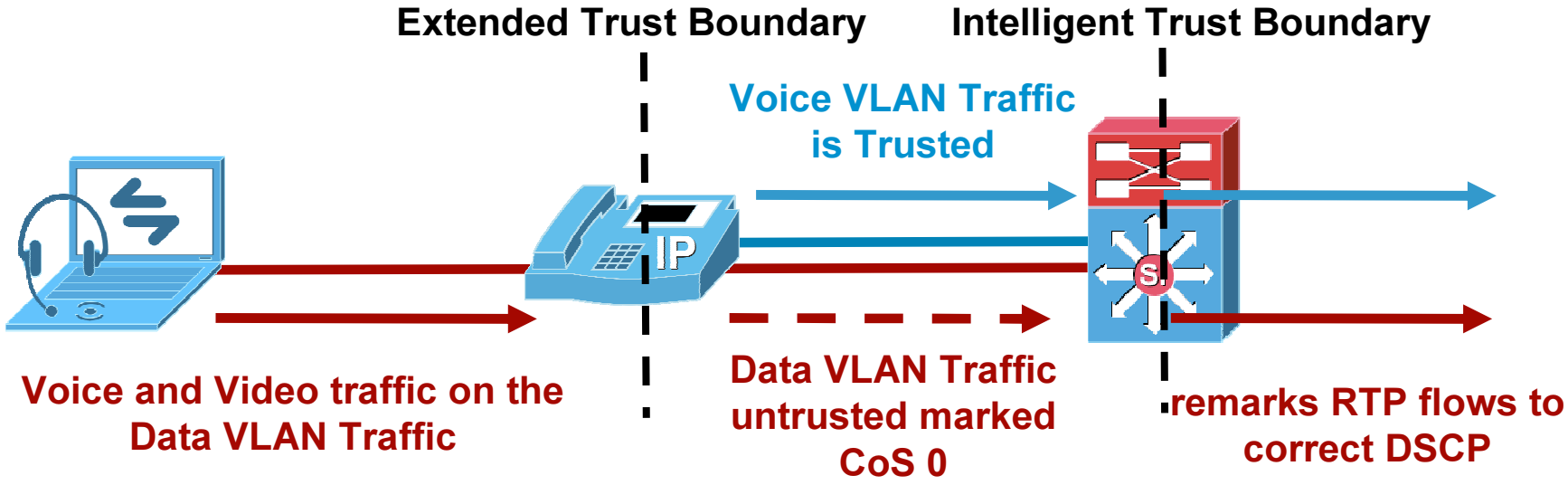
**Selbst-Konfigurierender Access-Layer**

- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

# Evolving UC Network Services

## UC applications migrating to the PC

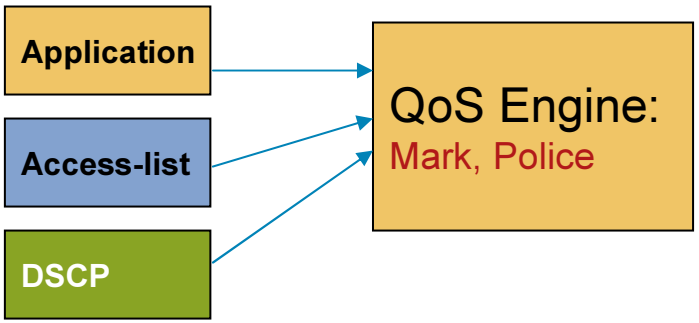


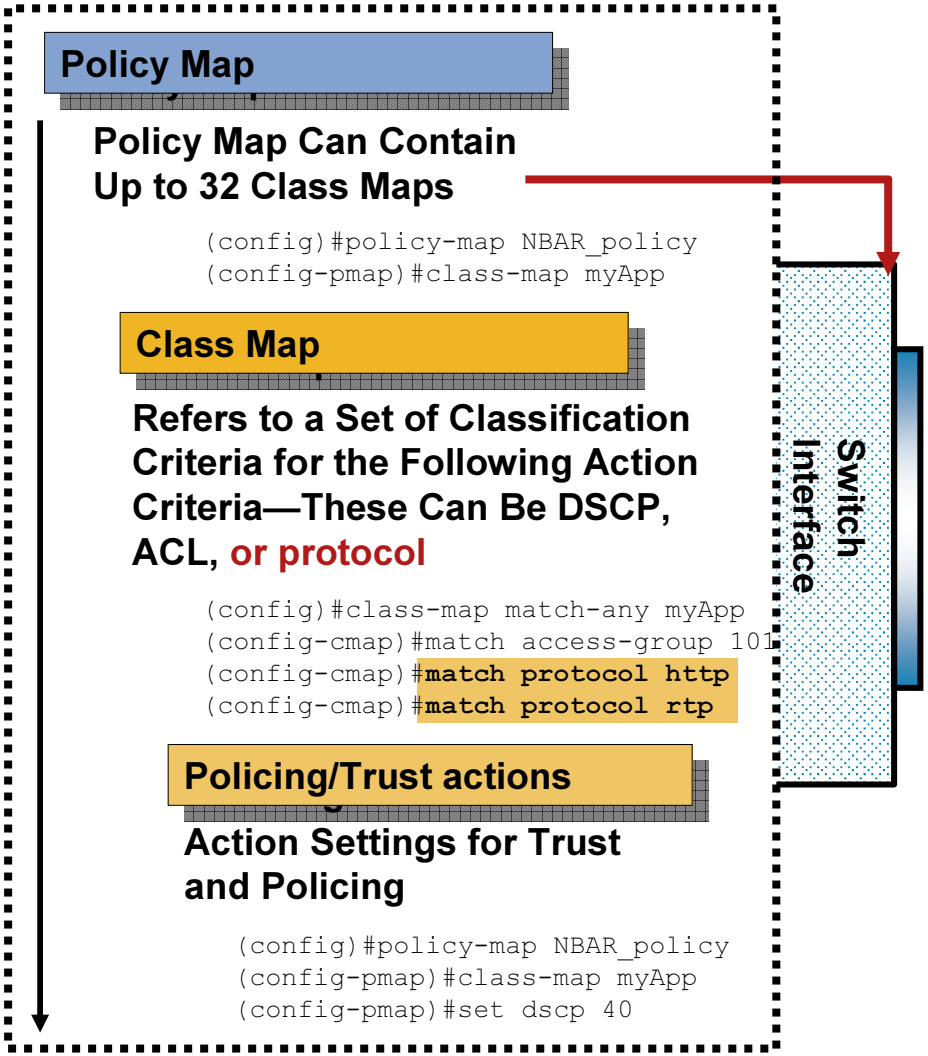

- With existing auto-qos configuration the default switch behaviour is to not trust edge ports and remark all traffic to configured CoS/DSCP
- When switch and phone exchange CDP the trust boundary is extended to IP phone
- Phone rewrites CoS from PC port to '0', switch rewrites DSCP
- Challenge is two-fold, PC based UC apps and increased end user mobility

# Evolving UC Network Services

## Enhanced Access Trust Boundary (Sup32 PISA et.al.)

- NBAR works together with QoS to assign QoS actions based on application classification
- Modular QoS traffic classification:
  - Define match criteria (class-map)
  - Associate actions for a given match criteria in a policy-map
  - Assign policy to an interface
- The ability to match L5-7 protocol information provides the basis for an enhanced trust boundary



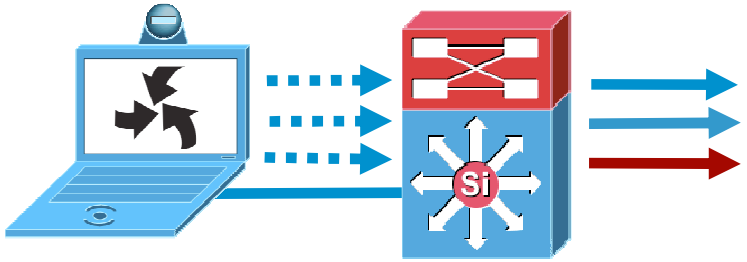



# Enhanced QoS Trust Boundary

## HTTP port overloading

- **Migration to common HTTP interface for multiple applications**
- **Challenge to distinguish priority based on port numbers**
- **NBAR deep packet inspection allows marking based on HTTP content**

**PISA identifies and remarks HTTP flows to desired DSCP**




```
cr32-6500-2(config-cmap)#match protocol http ?
  content-encoding  Encoding mechanism used to package entity body
  from              E-mail of human controlling the user-agent
  host              Host name of Origin Server containing resource
  location          Exact location of resource from request
  mime              Content-Type of entity body
  referer           Address the resource request was obtained from
  server            Software used by Origin Server handling request
  url               Uniform Resource Locator path
  user-agent        Software used by agent sending the request
  <cr>
```

```
class-map match-all Production-Web-Traffic
  match protocol http url "*.cisco.com"
class-map match-all Non-Production-Web-Traffic
  match protocol http url "*.youtube.com"
```

# Campus Quality of Service Updates

## Rational for the access port access port QoS updates

- The increase in end user mobility and UC evolution is moving us from a model based on fixed W2K desktop with phone to a laptop running XP/Vista/MacOS with integrated voice and video capabilities
- Corrections and improvements based on feedback from wide scale deployment
- Greater switch functionality (PISA, Sup6E, 3750E, …)
- Common policy applied to all ports on a switch except those with highly specific requirements (simply deployment and maintenance)
  - PC with no UC
  - Phone (7960, 7985, …)
  - PC running IP Communicator, CUPC, CVA
  - Legacy phone and untrusted PC
  - Phone and PC running IP Communicator, CUPC, CVA, …

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

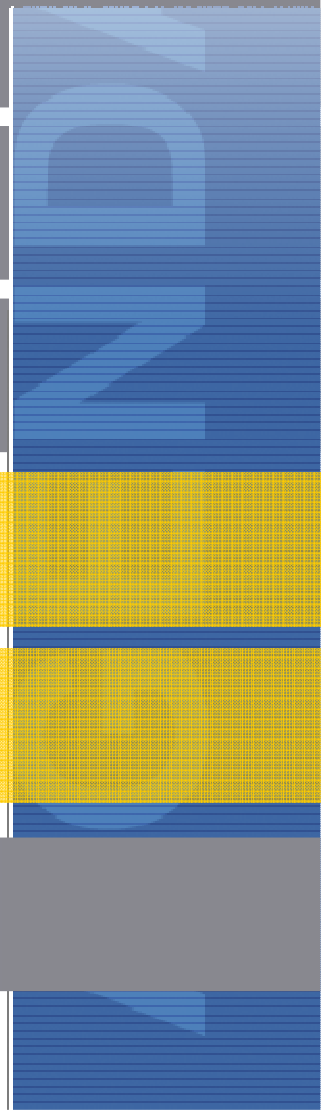
**Dynamisches QoS im Access-Layer**

- Intelligent Voice QoS

**Selbst-Konfigurierender Access-Layer**

- Auto-Smartports, IOS Shell, EEM

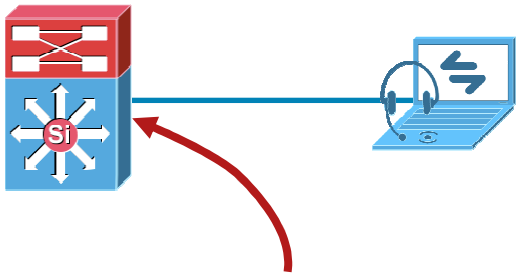
**Zusammenfassung, Q&A**



# Smartports

## Macro based port configuration

- Smartports first developed to ease the configuration for a variety of switch port types based on Cisco recommended best practice - 12.2(18)SE
- Existing macros include
  - cisco-desktop
  - cisco-phone
  - cisco-switch
  - cisco-router
  - cisco-wireless
- Manually configured on a per port basis

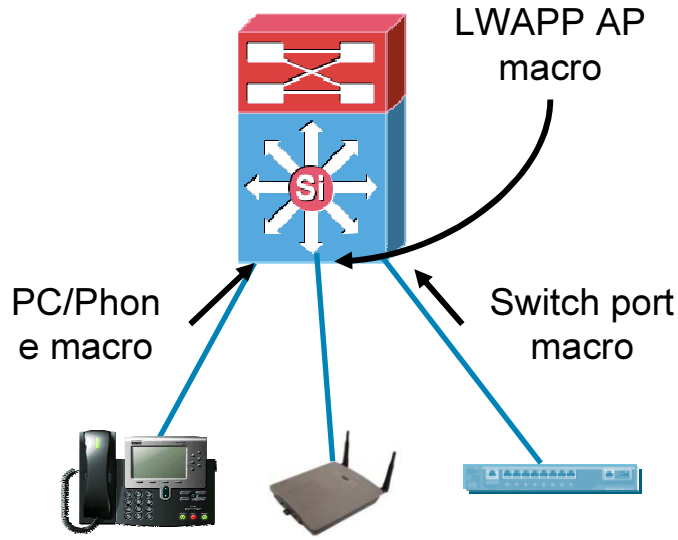


```
cr34-3560e-2#show parser macro name cisco-desktop
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $access_vlan
# Basic interface - Enable data VLAN only
# Recommended value for access vlan should not be 1
switchport access vlan $access_vlan
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one
minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

# Auto Smartports

## Automatic application of smartport macros

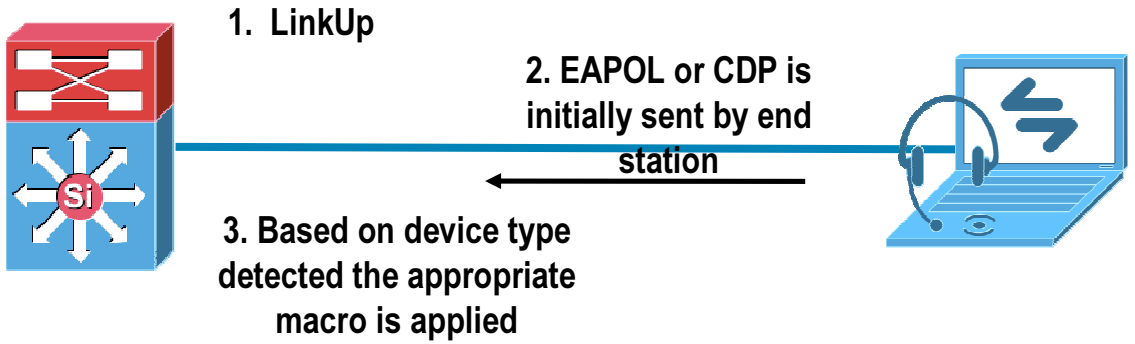
- Challenges with older version of smartports
  - Existing macros tended towards lowest common denominator behaviour in order to minimize the number of potential corner cases
  - New devices, e.g. LWAPP AP's, not supported
  - Initial implementation utilized the IOS parser to implement a macro capability which meant no "undo" capability
- Updating the implementation to address these issues plus add the ability to dynamically apply a macro based on detection of the device type
- 12.2(50)SE – 2970, 3560, 3750, 3560E, 3750E




Automatic configuration of the access port as devices connect

# Auto Smartports

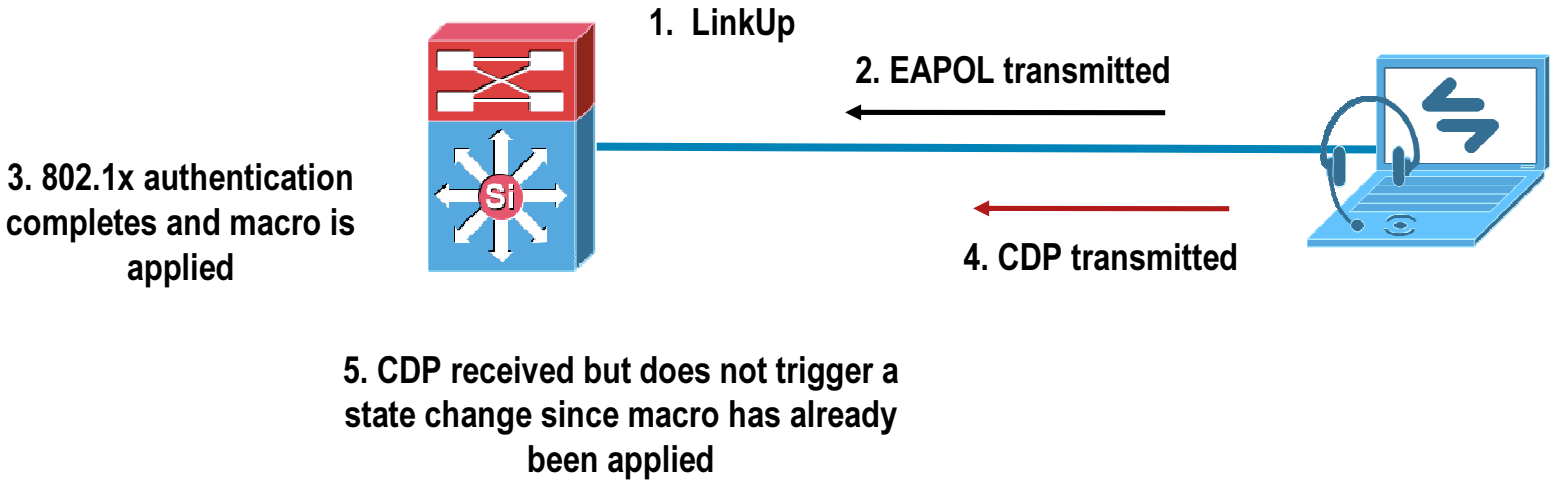
## Modes of operation




- Auto Smartports operates in one of two modes
  - Static – macro definition is applied manually (GUI or CLI) and does not change when the port/device state changes
  - Dynamic – smartport macro may change based on port/device state changes
- In dynamic mode the device identification is based on either CDP message or 802.1x/MAB attribute-value pair sent by the RADIUS upon successful authentication

# Auto Smartports

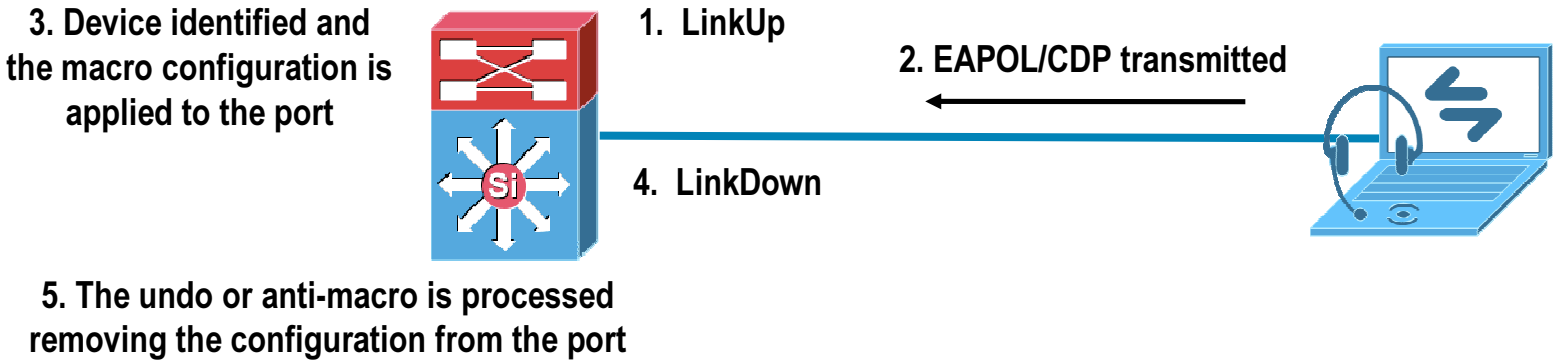
## Single State change occurs on link up




- Auto Smartports will only trigger *once* after a each link up event for that port
- In the case of multiple events per port (either multiple authentications or CDP messages) only the first message received will trigger the application of a port macro
- In cases with multiple devices (phone and PC, hub and multiple devices) the port configuration will be based on the *first* device detected

# Auto Smartports

## Undo macros




- Two macro types
  - macro – defines the configuration to apply to a specific port
  - anti-macro – defines the configuration changes required to remove the macro from a port
- On link up either CDP or 802.1x/MAB will trigger the application of the macro to the port
- On link down the anti-macro is processed and the configuration is removed from the port

# Auto Smartports

## Initial port configuration

- On switch initialization each port will be configured as a default type
- On switch reboot
  - If the switch port is marked as static the configuration stored in the startup-config will be applied to the interface
  - If the switch port is marked as dynamic it will either be configured based on the default port type (if the interface is down) or based on the device type as detected by 802.1x/MAB or CDP

```
cr34-3560-1#sh shell function brief
Built-in function names
CISCO_AP_AUTO_SMARTPORT
CISCO_DOT1X_AUTH_FAIL_AUTO_SMARTPORT
CISCO_DOT1X_CRITICAL_AUTO_SMARTPORT
CISCO_DOT1X_DESKTOP_AUTO_SMARTPORT
CISCO_DOT1X_EASY_AUTO_SMARTPORT
CISCO_DOT1X_MAB_GUEST_AUTO_SMARTPORT
CISCO_DOT1X_MAB_TIMEOUT_AUTO_SMARTPORT
CISCO_LWAP_AUTO_SMARTPORT
CISCO_PHONE_AUTO_SMARTPORT
CISCO_ROUTER_AUTO_SMARTPORT
CISCO_SWITCH_AUTO_SMARTPORT
```

**Pred-defined Smartport macros**

**802.1x**

**LWAPP and Legacy AP**

**End Station (user) macro is a superset of phone and desktop**

# Auto Smartports

## Enabling auto smartports

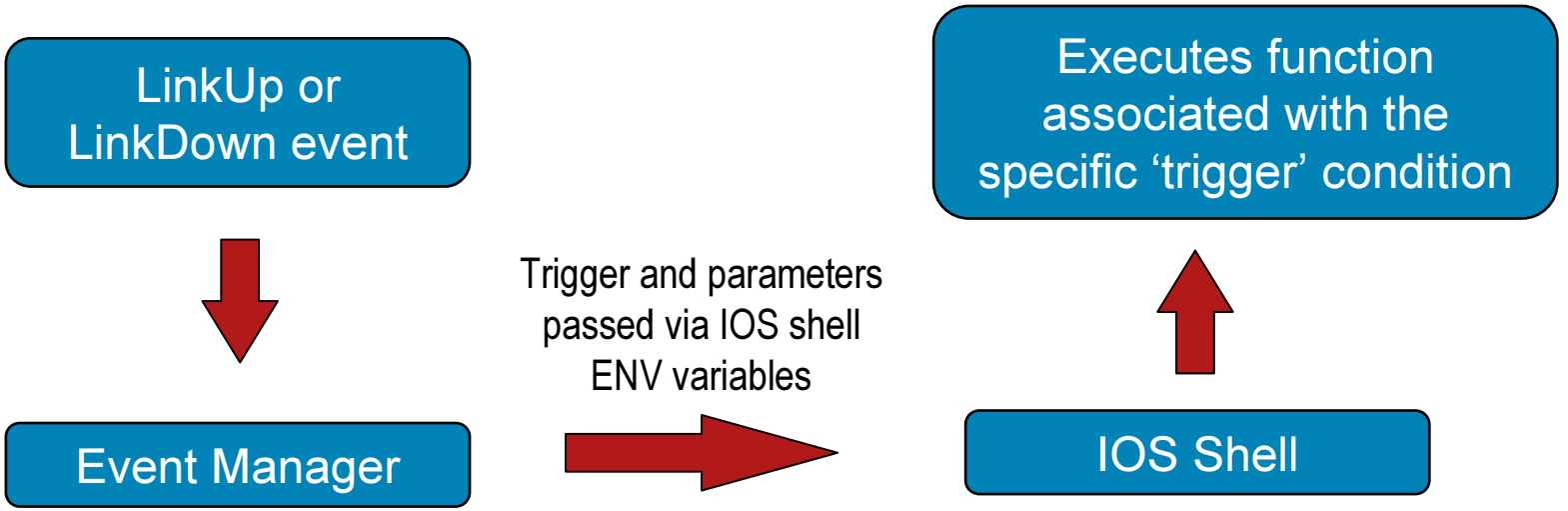
- Auto smartports can be enabled on a global or per interface basis
- By default auto smartports will utilize CDP as the device identification method
- If 802.1x is enabled then macro is controlled by 802.1x
- 802.1x allows for fallback to CDP trigger events

```
! Enabling auto smartports globally
!
cr34-3560-1(config)#macro auto global processing ?
  cdp-fallback  If the port is dot1x enabled and trigger is not sent by RADIUS,
                use CDP capability information as trigger
  <cr>
!
! Auto smartports can be enabled or disabled per interface
!
cr34-3560-1(config-if)#[no] macro auto processing ?
  cdp-fallback  Use CDP or Other Authentication Mechanism by default
  <cr>
```

# Auto Smartports

## Enabling the new auto smartports - IOS Shell

- The application and removal of the smartports configuration is accomplished via a new feature the IOS Shell
- IOS Shell is invoked by the switch Event Manager which will pass a trigger condition and a number of variables to the IOS shell
- IOS shell will execute the function associated with the trigger condition to apply the configuration changes required by the macro



# IOS Shell

## UNIX Shell like environment in IOS

- The shell is integrated into the existing IOS CLI environment
- Order of execution when a command is entered at the prompt
  - IOS command
  - Built-in ios.shell function
  - User defined ios.shell function

```
! Define a function in the IOS shell
switch#function config_port() {
>conf t
>int GigabitEthernet0/$1
>switchport mode access
>switchport access vlan $2
>switchport port-security
>switchport port-security maximum $3
>}
! This shell function can be invoked at the CLI
switch#config_port 22 100 3
!
```

# IOS Shell

## IOS Shell Triggers

- A shell function can not only be invoked from command line, it can also be invoked programmatically based on a trigger tag
- At FCS pre-defined triggers used by auto smartports will be available
- The network administrator can define their own triggers with associated self defined functions to be invoked in the case of that trigger

```
! Create a new trigger condition
cr34-3560-1(config)#shell trigger port_up Trigger for the config_port macro we created
!
cr34-3560-1#show shell triggers
User defined triggers
---------------------
Trigger Id: port_up
Trigger description: Trigger for the config_port macro we created
Trigger environment:
Trigger mapping function:

<snip>
```

# IOS Shell

## Auto Smartports

- Auto smartports uses the IOS shell capabilities
- CDP or 802.1x state changes invoke a trigger condition which in turn executes a built-in IOS shell function

```
cr34-3560-1#show shell triggers
---------------------
Built-in triggers
-----------------
Trigger Id: CISCO_PHONE_EVENT
Trigger description: This macro applies port configuration for ip-phone

Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1) and
$VOICE_VLAN=(2), The value in the parenthesis is a default value
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT
<snip>

cr34-3560-1#show shell functions CISCO_PHONE_AUTO_SMARTPORT
function CISCO_PHONE_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
                . . .
```

When this internal trigger occurs

Invoke this built-in function

# IOS Shell
## Auto Smartports

- The IOS Shell provides for simple programming logic, e.g. *'if'* constructs
- Undo capability is defined as the sequence of commands required to 'remove' everything the function configured initially
- Same logic just different 'variables' passed when the function is invoked

```
cr34-3560-1#show shell functions CISCO_PHONE_AUTO_SMARTPORT
function CISCO_PHONE_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface  $INTERFACE
                macro description $TRIGGER
                switchport access vlan $ACCESS_VLAN
                switchport mode access
                . . .
                ip dhcp snooping limit rate 15
            exit
        end
    fi
    if [[ $LINKUP -eq NO ]]; then
        conf t
            interface  $INTERFACE
                no macro description
                no switchport port-security
                no switchport access vlan $ACCESS_VLAN
                . . .
```

**When the interface changes state if it is 'linkup' then apply the configuration**

**When the interface changes state if it is 'linkdown' then remove all the configuration**

# Smartport Macros Update

## 3750/3560 Phone Auto Smartport macro

- Changes from the existing macros
  - DHCP Snooping, DAI and IP source Guard enabled
  - Port security configuration has been updated
  - Storm control is enabled
  - Enables blocking of unknown unicast flooding
- Similar to the changes being made to the access port QoS configuration it is designed for plug and play
- ***Not*** designed for Trade Floors, Data Center or other highly specialized network clients

```
! Global configuration
ip dhcp snooping vlan 4,200,404
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,404
ip arp inspection validate src-mac dst-mac ip allow zeros
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause arp-inspection
errdisable recovery interval 120
!
interface FastEthernet0/24
 switchport access vlan 4
 switchport mode access
 switchport block unicast
 switchport voice vlan 404
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security maximum 1 vlan voice
 switchport port-security
 switchport port-security aging time 5
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip verify source
 ip dhcp snooping limit rate 15
```

# Smartport Macro Updates

## What new features are in the macro

- DHCP Snooping

  Proxies all DHCP requests preventing accidentally (or intentionally) DHCP server spoofing

- Dynamic ARP Inspection

  Proxies all ARP packets preventing ARP masquerading

- IP Source Guard

  Prevents an endpoint from IP masquerading

- Storm Control

  Limits the rate of ingress broadcast and multicast traffic to reasonable levels

- Block Unicast

  Prevents flooding of unknown MAC addresses out this port

**Neue Entwicklungen fuer den Access-Layer**

- PoE, CDP, LLDP, 802.3az, EnergyWise

**Dynamisches QoS im Access-Layer**

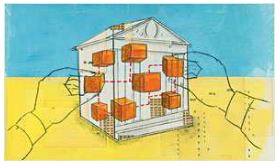
- Intelligent Voice QoS

**Selbst-Konfigurierender Access-Layer**

- Auto-Smartports, IOS Shell, EEM

**Zusammenfassung, Q&A**

# Key-Take-Aways:



- The Intelligent Access – unique for access switches
  - Best Practices configurations - Smartport and Auto-QoS
  - Dynamic application of the correct best practices configuration – Auto Smartports
  - The intelligence of application aware Deep Packet Inspection to both simplify and improve the QoS and security trust boundary
  - CDP, LLDP, LLDP-MED
  - PoE evolution (802.3at)

# Q and A