IOS 15.0(2)SE TDM

UAG Technical Marketing

© 2011 Cisco and/or its affiliates. All rights reserved.

Release Highlight IOS 15.0(2)SE for Cat 3K/2K/Compact

Now Shipping

- Innovative capabilities for Campus Networks by delivering Comprehensive Security Solutions, New IPv6 and Infrastructure capabilities, Green-IT and more….
- Feature Parity on Compact Switches (2960C & 3560C)
- Extended Maintenance (Long Lived) Release

Security

SGA (SGT/SGACL) on 3560-X & 3750-X for Simplified ACL Management, Uniform Policies & fine grained Access Control

Cisco SGT Exchange Protocol (SXP) support on Catalyst 2960S Series switches

IPv6

IPv6 First Hop Security to secure the network access from IPv6 enabled end devices

IPv6 Multicast Routing support

Compliance certifications for US FED/ SLED customers - USGv6, JITC & IPv6 Ready Logo certifications

Green

UPOE (60W PoE) powered 2960C/3560C for Reduced TCO

Energywise controlling devices with no Energywise Agent via SNMP

Others

Resilient Ethernet Protocol (REP) for faster convergence

Extending Support for **StackPower** in LAN Base (3750X)

SFP-10G-ER support on 3750-X/3560-X uplinks

Support for the new Cisco **Catalyst 2960-SF** Series Switch

Security Features

© 2010 Cisco and/or its affiliates. All rights reserved.

MACsec on 3560C

- From 15.0(2)SE, three 3560C GE models support MACsec on uplink and downlink ports:
- WS-C3560CG-8TC-S: 8 downlinks, 2 dual-purpose uplinks
- WS-C3560CG-8PC-S: 8 PoE downlinks, 2 dual-purpose uplinks
- WS-C3560CPD-8PT-S: 8 PoE downlinks, 2 PoE Input uplinks

Port Security on Etherchannel

- Available from 15.0(2)SE with minimum featuresetLanLite
- Supported in 2960 2960S 2918 2960C 3560C 3560 3750
- Port Channel Interface characteristics:
  - All etherchannel modes (pagp, lacp, on, cross-stack) supported
  - Access mode supported
  - Trunk mode supported
  - No support for L3 EC

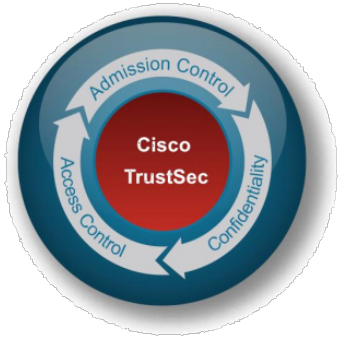
IP Source Guard on Etherchannel

- Available from 15.0(2)SE with minimum featuresetLan Base
- Supported in 2960 2960S 2960C 3560C 3750 3560
- Port Channel Interface characteristics:
  - All etherchannel modes (pagp, lacp, on, cross-stack) supported
  - Access mode supported
  - Trunk mode supported
  - No support for L3 EC
- IP Address Filtering:
  - Relies on DHCP snooping and static DHCP entries binding table
- IP and MAC address Filtering:
  - Also requires Port Security to be enabled

Cisco TrustSec
Enhancements in 15.0(2)SE

© 2011 Cisco and/or its affiliates. All rights reserved.

Secure Group Access Key Features



Security Group Based Access Control

- **Role-Based**, **Topology independent** access control
- Centralized Policy / Distributed Enforcement
- Scalable **ingress tagging (SGT) / egress filtering (SGACL)**

Authenticated Networking Environment

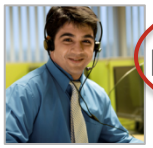
- Endpoint admission enforced via **802.1X authentication**
- **Network Device Admission** control based on 802.1X
- Only trusted network imposes Security Group TAG

Confidentiality and Integrity

- Encryption based on **IEEE802.1AE** (AES-GCM 128-Bit)
- **Wire rate** hop by hop layer 2 encryption
- Key management based on 802.11n (SAP), awaiting for standardization in 802.1X-REV

SGT Assignment for Roles

Doctor (SGT 7)



IT Admin (SGT 6)

Static
SGT Assignment
For
Servers

Users,
Endpoints

802.1X, MAB, LWA

Catalyst® 3750-X

Catalyst 6K
Core

Nexus® 7000
Distribution

STOP

Catalyst® 4948

ISE 1.1

IT Portal (SGT 4)
10.1.100.10

Dynamic
SGT Assignment
For
Endpoint

Public Portal (SGT 8)
10.1.200.10

Internal Portal (SGT 9)
10.1.200.200

Patient Record DB (SGT 10)
10.1.200.100

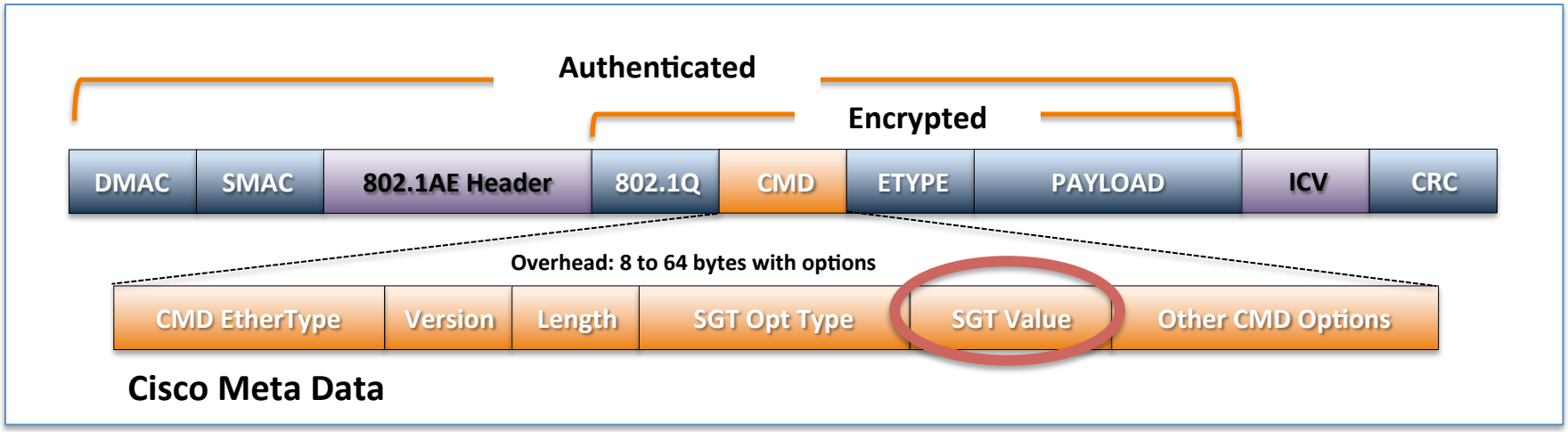
How To Create SGT Policy

Source SGT \ Destination SGT	Public Portal (SGT 8)	Internal Portal (SGT 9)	IT Portal (SGT 4)	Patient Record DB (SGT 10)
 Doctor (SGT 7)	Web	Web	No Access	Web File Share
 IT Admin (SGT 6)	We SS RD File S	Web SSH RDP File Share	Full Access	SSH RDP File Share

IT Maintenance ACL

```
permit tcpdst eq 443
permit tcpdst eq 80
permit tcpdst eq 22
permit tcp dst eq 3389
permit tcp dst eq 135
deny ip
```

Layer 2 SGT Frame Format



Ethernet Frame field

- 802.1AE Header | CMD | ICV e L2 802.1AE + TrustSec overhead
- Frame is always tagged at ingress port of SGT capable device
- Tagging process prior to other L2 service such as QoS
- No impact IP MTU/Fragmentation
- L2 Frame MTU Impact: ~ 40 bytes = less than baby giant frame (~1600 bytes with 1552 bytes MTU)

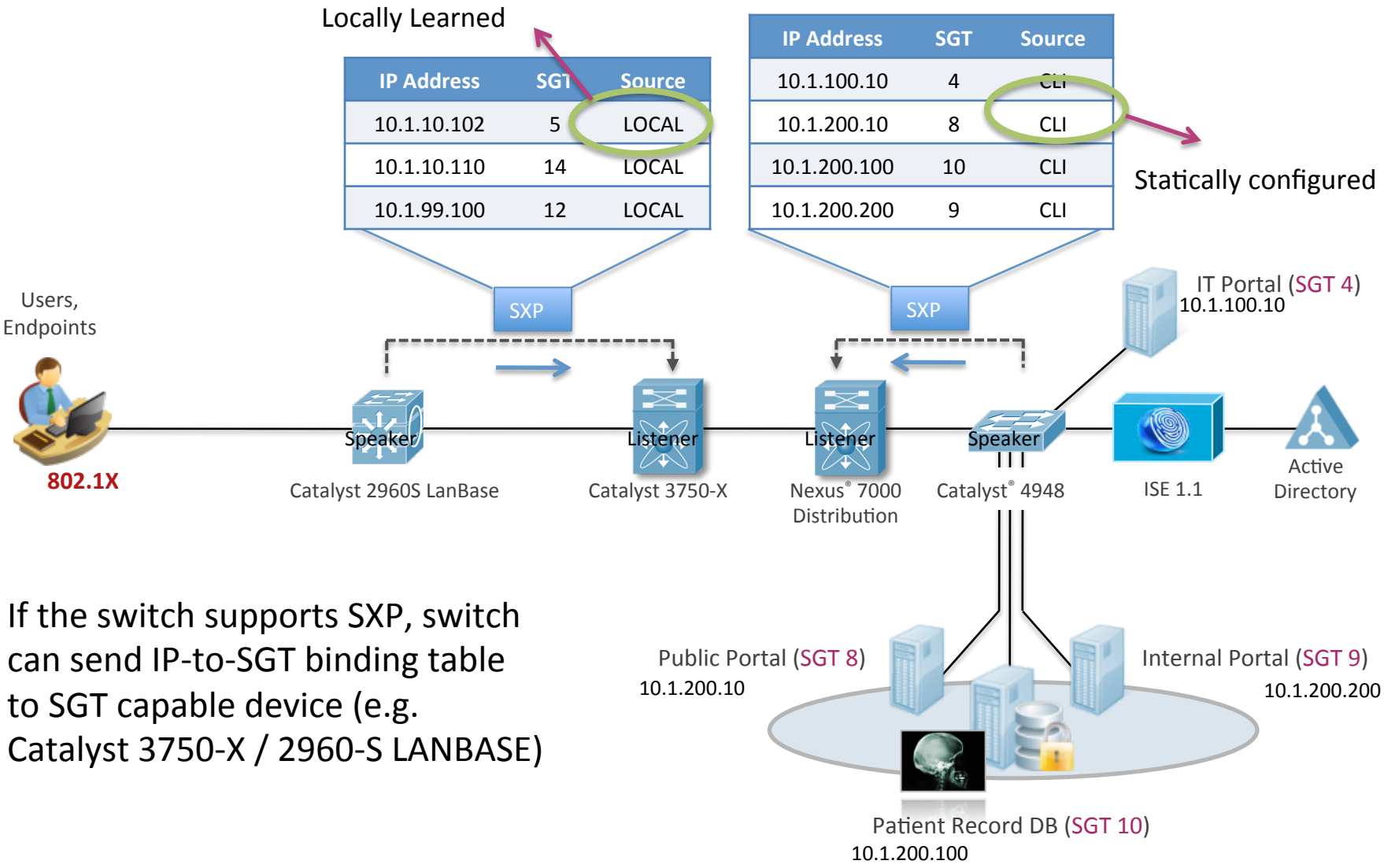
SGT Exchange Protocol (SXP)

© 2011 Cisco and/or its affiliates. All rights reserved.

SGT Exchange Protocol (SXP)

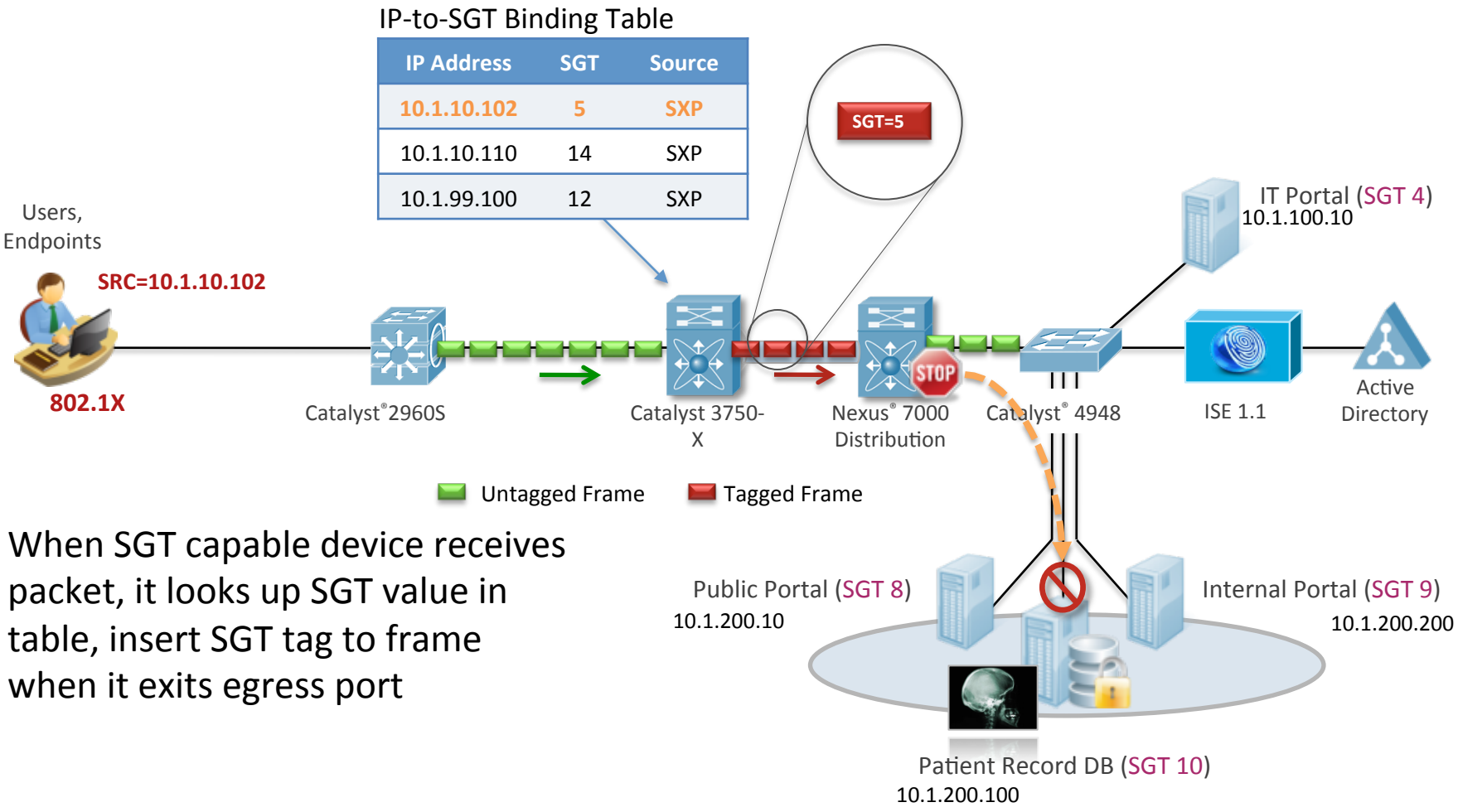
- SGT native tagging requires hardware (ASIC) support
- SGT eXchange Protocol (SXP) is used to exchange IP-to-SGT bindings between TrustSec capable and incapable device
- Currently supported on Catalyst 6500, 4500/4900, 3560/3750 and Nexus 7000 switch
- 15.0(2)SE IOS release extends SXP support to Catalyst 2960S LANBASE Series both as speaker and listener
  - No support for 2960 2960G
- Based on TCP with MD5 authentication
- Support single hop or multi-hop SXP
- SXP accelerates initial deployment of SGT/SGACL without immediate hardware upgrade

IP-to-SGT Binding Info Exchange using SXP



If the switch supports SXP, switch can send IP-to-SGT binding table to SGT capable device (e.g. Catalyst 3750-X / 2960-S LANBASE)

SGT Tagging



When SGT capable device receives packet, it looks up SGT value in table, insert SGT tag to frame when it exits egress port

SGA
Platform Support in 15.0(2)SE

© 2011 Cisco and/or its affiliates. All rights reserved.

SGT Platform Support in 15.0(2)SE

3560X 3750X

- SGT tagging is performed in the asic and it is available for downlink and uplink ports
  - Do not need a service module C3KX-SM-10G
- Aggregation platforms, including 3750X-12S and 3750X-24S, do not support SGT with IOS 15.0(2)SE

SGA – Platform Support for 15.0(2)SE

3K Platforms

3K-Legacy/3KG	3K-V2	3K-E	3K-X
SXP Only	SXP Only	SXP Only	✔☛

2K Platforms

2960	2960S
✖	SXP Only

Compact Switches

3560C	2960C
SXP Only	✖

***SGA is supported on IP Base and IP Services Images**

SXP is a software solution for SGT/SGACL deployments without immediate hardware upgrade

SGT Exchange Protocol (SXP)

IOS Software Image	3K-Legacy/ 3KG	3K-V2	3K-E	3K-X	2960/2960S
IP Services	✔	✔	✔	✔	✔
IP Base	✔	✔	✔	✔	✔
LAN Base	✘	✘	✘	✘	✘

Images supporting SXP

- Prior to 15.0(2)SE IOS release SXP is not supported in LANBASE Images
- 15.0(2)SE IOS release extends SXP support to LANBASE Images

SGA Feature Support Matrix

Components	Hardware	Available Features	Release
Nexus 7000 series Switch	**All Nexus 7K cards & chassis F-series don't support MACSec**	**SGT, SGACL, 802.1AE + SAP, NDAC, SXP v1, IPM,SGT**	**5.2.4**
Catalyst 6500E Switch (Sup 2T)	**WS-X6908-10G-2T & WS-X6908-10G-2TXL for MACSec**	**SGT, SGACL, 802.1AE + SAP, NDAC, SXPv2**	**15.0(1)SY1**
Catalyst 6500E Switch	**(Supervisor 32, 720)**	**SXP v2**	**12.2(33)SXJ2**
Catalyst 4500E switches	**Sup 7E, Sup7L-E (WS-X4712-SFP+E, WS-X4748-UPOE+E, WS-X4748-RJ45V+E, WS-X4748-RJ45-E for MACSec)**	**SXP v2, NDAC, 802.1AE + MKA (downlinks) or SAP (uplinks)**	**IOS-XE 3.3.0SG or 15.1.1(SG)**
Catalyst 4500E Switches	**Supervisor 6-E or 6L-E**	**SXPv2**	**IOS-XE 3.2.2SG or 15.0(1)SG2**
Catalyst 3560-X / 3750-X Switches	**Regular downlink ports or C3KX-SM-10G (MACSec10GE uplink)**	**SGT, SGACL, NDAC, SXPv2, 802.1AE + MKA or SAP**	**15.0(2)SE1**
Catalyst 3560(E) / 3750(E) Switches	**3560E, 3750E**	**SXPv2**	**15.0(1)SE2**
Cisco ASA	5505,5510,5520,5540,5550,5580,5585-X, ASA-SM and Saleen Platforms (5512-X, 5515-X, 5525-X, 5545-X, 5555-X)	**SXPv2, SGFW**	**9.0**
Cisco ASR 1000	**PR1/PR2, 1001, 1002, 1004, 1006, 1013,ESP10/20/40, SIP10/40**	**SXPv2, SGFW**	**XE3.5 or 15.2(1)S**
Cisco ISR	**88x, 89x, 19xx, 29xx, 39xx**	**SXPv2, SGFW**	**15.2(2)T**
Wireless LAN Controller	**5500,2500,WISM2, WLCM2**	**SXPv2 (Speaker Only)**	**7.2MR1**
Nexus 5K	**N5548P, N5548P and N5596UP. No support for N5010 or N5020**	**SXP (Speaker Only), SGT, SGACL**	**5.1(3)N1(1)**

SXP Platform Support Matrix

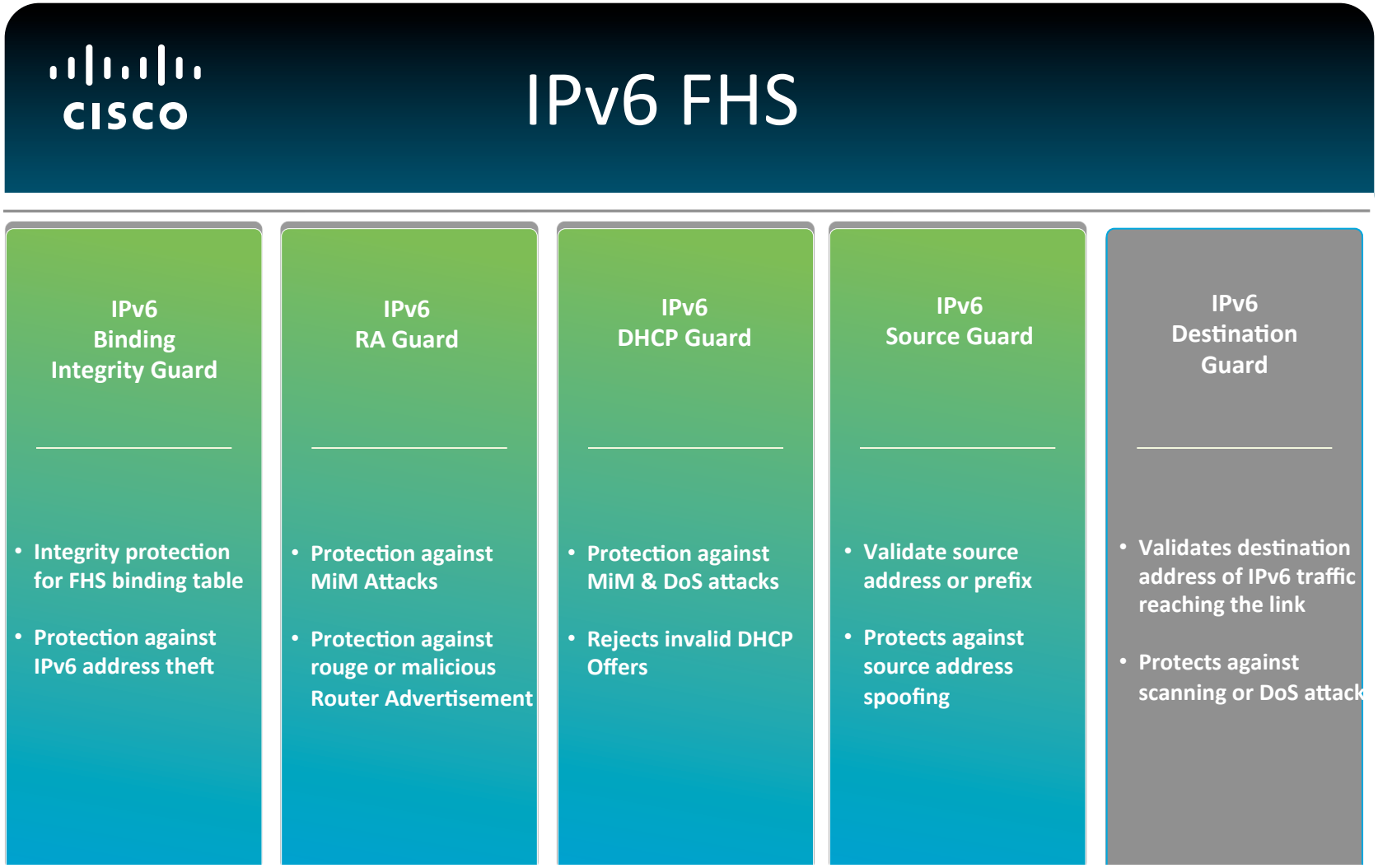
Platform	SXP v1	SXP v2	SXP MIBs	SXP Syslogs
Catalyst 2960	No	No	No	No
Catalyst 2690S	No	15.0(2)SE	15.0(2)SE	15.0(2)SE
Catalyst 3560E/ 3750E	12.2(53)SE2	15.0(1)SE	15.0(2)SE	15.0(2)SE
Catalyst 3560v2/3750v2	12.2(53)SE2	15.0(1)SE	15.0(2)SE	15.0(2)SE
Catalyst 3560X/ 3750X	12.2(53)SE2	15.0(1)SE	15.0(2)SE	15.0(2)SE
Catalyst 3560C	12.2(55)EX2	No	No	No
Catalyst 2960C	No	No	No	No
Catalyst 3750X-12S & 24S	12.2(55)SE	15.0(2)SE	15.0(2)SE	15.0(2)SE

IPv6 Features

© 2010 Cisco and/or its affiliates. All rights reserved.

IPv6 First Hop Security (FHS)

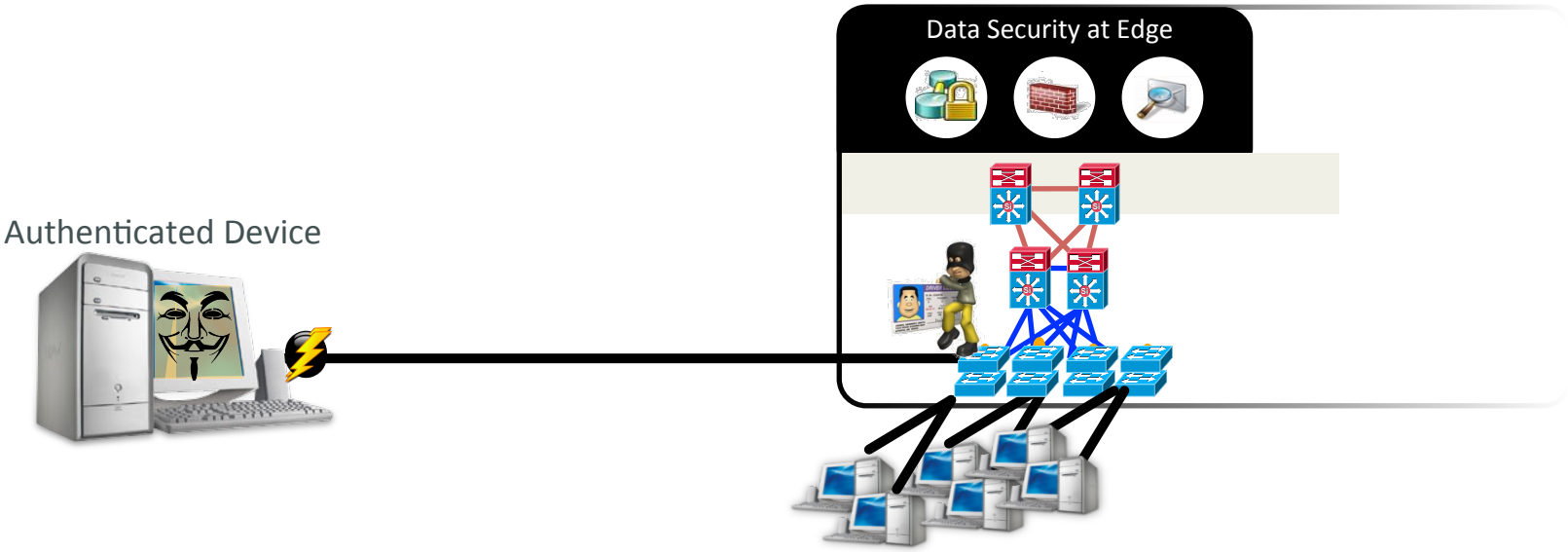
Securing Enterprise IPv6 Networks – Quick Intro



© 2010 Cisco and/or its affiliates. All rights reserved.

Attacks on an IPv6 Network

Example of Inside Attacks exploiting IPv6 Link Operations



The Challenge

IPv6 Link Operations can be easily attacked inside the local network

Attacks Inside the network

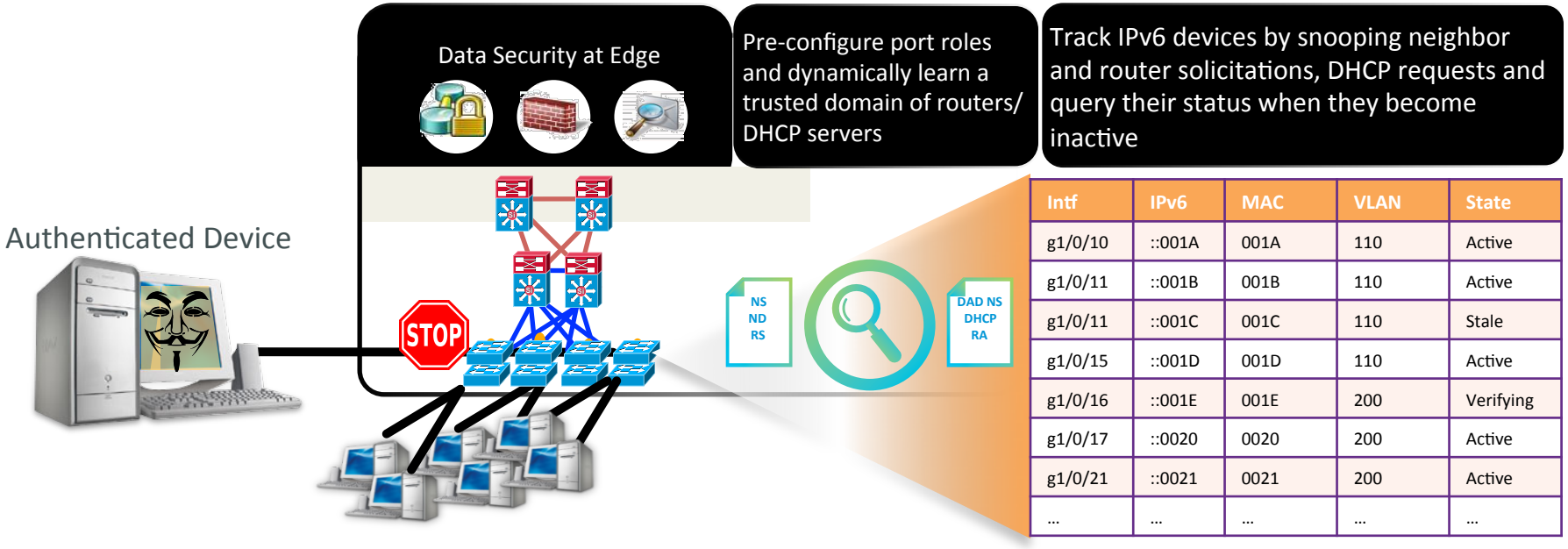
The attacker can spoof a user address by snooping Neighbor Solicitation and poisoning Neighbor Advertisement

The attacker can become the local default gateway by sending rogue Router Advertisements

The attacker can disable the local IPv6 network by poisoning Duplicate Address Detection

IPv6 First Hop Security

Intelligent Perimeter at the edge



Intf	IPv6	MAC	VLAN	State
g1/0/10	::001A	001A	110	Active
g1/0/11	::001B	001B	110	Active
g1/0/11	::001C	001C	110	Stale
g1/0/15	::001D	001D	110	Active
g1/0/16	::001E	001E	200	Verifying
g1/0/17	::0020	0020	200	Active
g1/0/21	::0021	0021	200	Active
…	…	…	…	…

The Solution

IPv6 First Hop Security in the access switch

IPv6 Snooping and Guard

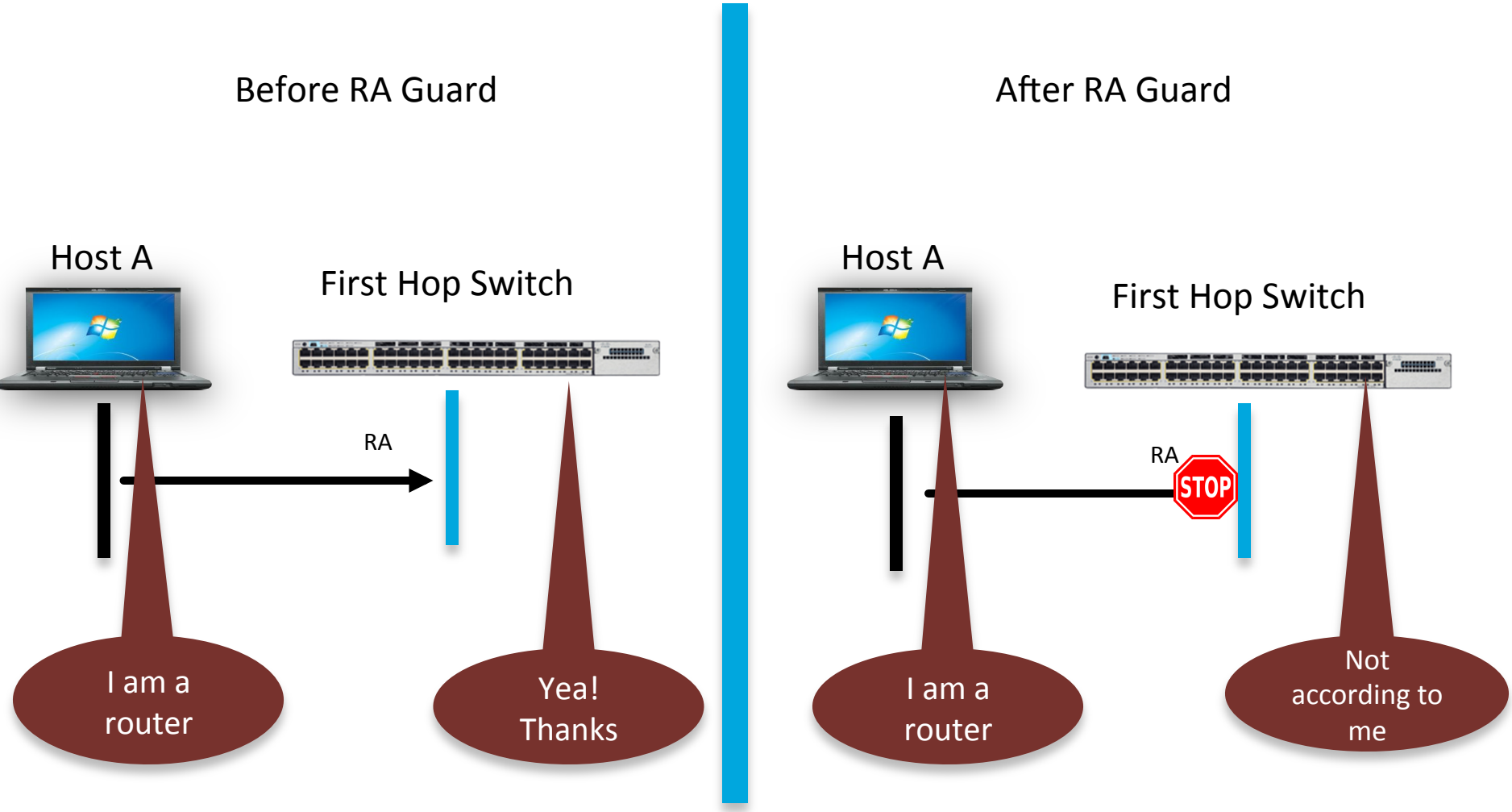
Block rogue advertisements from illegitimate routers and DHCP servers with **RA Guard and DHCPV6 Guard**

Monitor device address assignment with **Binding Integrity Guard**

Maintain a trustworthy database of IPv6 devices and block illegitimate IPv6 data traffic with **Source Guard**

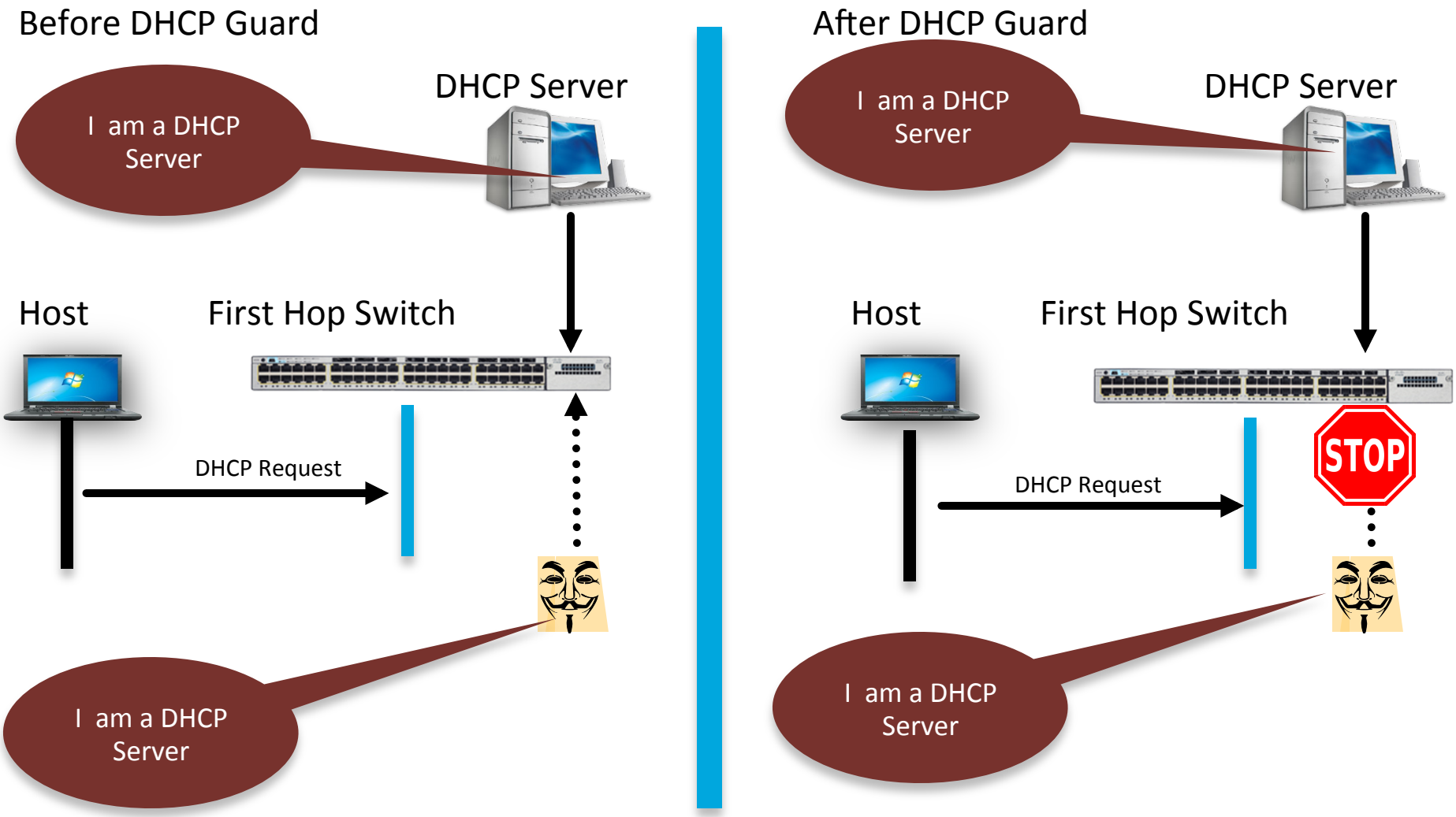
IPv6 FHS – RA Guard

Prevent Rogue Router Advertisements from taking down the network



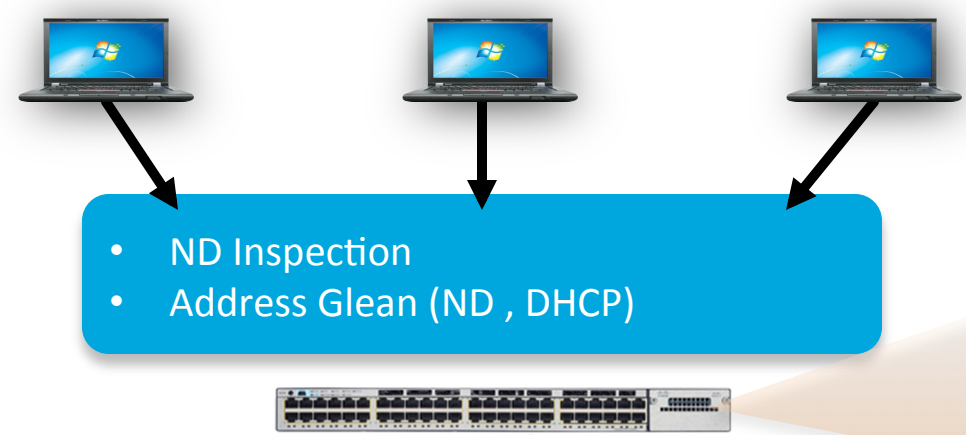
IPv6 FHS – DHCPv6 Guard

Prevent Rogue DHCP responses from misleading the client



IPv6 FHS – Binding Integrity Guard

Creates and maintains a v6 binding table to ensure rogue users cannot spoof or steal addresses



IPv6 Binding Table

Intf	IPv6	MAC	VLAN	State
g1/0/10	::001A	001A	110	Active
g1/0/11	::001C	001C	110	Stale
g1/0/16	::001E	001E	200	Verifying

IPv6 Source Guard

IPv6 Destination Guard

Device Tracking

IPv6 FHS – IPv6 Source Guard

Allow traffic only from sources that was present in the binding table

Before IPv6 Source Guard

Ok I'll update binding table

Intf	IPv6	MAC	VLAN	State
g1/0/10	::001A	001A	110	Active
g1/0/11	::001C	001C	110	Stale
g1/0/16	::001E	001E	200	Verifying
g1/0/21	::0021	0021	200	Active

Host A

First Hop Switch

::001A

NA(::001A,mac - 001A)

NA(::001A,mac - 002A)

I am Host A

After IPv6 Source Guard

No you are not!

Intf	IPv6	MAC	VLAN	State
g1/0/10	::001A	001A	110	Active
g1/0/11	::001C	001C	110	Stale
g1/0/16	::001E	001E	200	Verifying
g1/0/21	::0021	0021	200	Active

Host A

First Hop Switch

::001A

NA(::001A,mac - 001A)

STOP

NA(::001A,mac - 002A)

I am Host A

SysLogs for IPv6 FHS

Use SysLog messages to verify IPv6 FHS RA Violations on a switch.

RA Guard

If the client port is configured as host and receives any RA message the switch logs the messages as below

```
*Mar  1 00:23:37.449: %SISF-4-PAK_DROP: Message dropped A=FE80::F2F7:55FF:FEBF:F144 G=- V=22
I=Fa1/0/26 P=NDP::RA Reason=Message unauthorized on port
*Mar  1 00:24:03.197: %SISF-4-PAK_DROP: Message dropped A=FE80::F2F7:55FF:FEBF:F144 G=- V=22
I=Fa1/0/26 P=NDP::RA Reason=Message unauthorized on port
```

The port remains in forwarding state as violating packets are dropped

DHCPv6 Guard

SysLogson DHCPv6 guard intrusions not available (CSCub50593) . Enable debugging to monitor DHCPv6 violations

```
Switch# debug ipv6 snooping dhcp-guard
*Mar  1 01:18:29.212: SISF[DHG]: Fa1/0/25 vlan 22 DHCP Guard setting sec level to GUARD
*Mar  1 01:18:29.212: SISF[DHG]: Fa1/0/25 vlan 22 DHCP Server message for role dhcp client - Deny
```

The port remains in forwarding state as violating packets are dropped

IPv6 FHS – Platform Support in Compact Platforms

FEATURE	Legacy Compact	2960C	2960CG	3560C	3560CG
RA Guard	✖	✖	LANBASE	✖	IPBASE
DHCPv6 Guard	✖	✖	LANBASE	✖	IPBASE
BindingIntegrityGuard	✖	✖	LANBASE	✖	IPBASE
SourceGuard	✖	✖	✖	✖	IPBASE
DestinationGuard	✖	✖	✖	✖	✖
(DADProxy,RA throttling,ND MulticastSuppression, DHCPv6LDRA)	✖	✖	✖	✖	✖

Comments

- No IPv6 FHS support on LanLite switches
- 2960C 3560C switches HW not capable of IPv6 FHS
- No IPv6 Source Guard support in 2960CG LANBASE

SW Support:
✔- 15.0(2)SE

IPv6 FHS – Platform Support in 2K Platforms

FEATURE	2960- LanLite	2960-LanBase	2960S-LanLite	2960S-LanBase
RA Guard	✖	✖	✖	✔
DHCPv6 Guard	✖	✖	✖	✔
BindingIntegrityGuard	✖	✖	✖	✔
SourceGuard	✖	✖	✖	✖
DestinationGuard	✖	✖	✖	✖
(DADProxy,RAthrottling,NDMulticastSupression, DHCPv6LDRA)	✖	✖	✖	✖

Comments

- No IPv6 FHS support on LanLite switches
- 2960 switches HW not capable of IPv6 FHS
- No IPv6 Source Guard support in 2960S LANBASE

SW Support:
✔- 15.0(2)SE

IPv6 FHS – Platform Support in 3K Platforms

FEATURE	3K-Legacy/ 3KG	3K-V2	3K-E	3K-X
RA Guard	✖	✖	IPBASE	LANBASE
DHCPv6 Guard	✖	✖	IPBASE	LANBASE
BindingIntegrityGuard	✖	✖	IPBASE	LANBASE
SourceGuard	✖	✖	IPBASE	LANBASE
DestinationGuard	✖	✖	✖	✖
(DADProxy,RAthrottling,NDMulticastSupression, DHCPv6LDRA)	✖	✖	✖	✖

Comments

- 3K refers to both 3560 and 3750 series
- Legacy 3K and 3K-G, and 3K-V2 switches HW not capable of IPv6 FHS
- 3K-E will not support any new v6 FHS feature beyond 15.0(2)SE
- IPv6 Source Guard supported in 3K-X LANBASE

SW Support

✔- 15.0(2)SE

SDM Template Requirements for IPv6 FHS

- Need a IPv6 capable SDM template for the commands to be exposed
- For C3K, dual-IPv4-IPv6 SDM template significantly reduces TCAM resources

Resource	Default
Unicast MAC addresses	6 K
IGMP groups and multicast routes	1 K
Unicast routes	8 K
Directly connected hosts	6 K
Indirect routes	2 K
Policy-based routing ACEs	0
QoS classification ACEs	0.5 K
Security ACEs	1 K
VLANs	1 K

Resource	Dual IPv4-and IPv6 Templates Default
Unicast MAC addresses	2 K
IPv4 IGMP groups and multicast routes	1 K
Total IPv4 unicast routes:	3 K
Directly connected IPv4 hosts	2 K
Indirect IPv4 routes	1 K
IPv4 policy-based routing ACEs	0
IPv4 or MAC QoS ACEs (total)	0.5 K
IPv4 or MAC security ACEs (total)	1 K
IPv6 multicast groups	1 K
Directly connected IPv6 addresses	2 K
Indirect IPv6 unicast routes	1 K
IPv6 policy-based routing ACEs	0
IPv6 QoS ACEs	0.5 K
IPv6 security ACEs	0.5 K

Fig: Comparing v4 and v4-v6 Dual default SDM templates

- An IPv6 FHS capable SDM template will be available in later releases without requiring changing to dual-IPv4-Ipv6 template

Performance and Scalability
C3K-X and C3K-E

RA Guard

RA Rate	CPU utilization
240 pps	20%
1000 pps	48%

Assuming an average of 2 RA's per minute, this leads to theoretically 7200 clients supported with 20% CPU utilization

IPv6control plane packet Rate	CPU utilization
100 pps	13%
500 pps	74%
700 pps	98%

Testing is done by enabling IPv6 snooping, generating a mix of ICMPv6 and DHCPv6 synthetic traffic and monitoring CPU utilization.

IPv6 Multicast Routing

© 2011 Cisco and/or its affiliates. All rights reserved.

IPv6 Multicast Routing Requirements

- Minimum Requirements for IPv6 Multicast:

Products	3560X 3750X 3560E 3750E
Minimum Featureset	IPSERVICES
IOS Release	15.0(2)SE
SDM Template[2]	Dual IPv4/IPv6[1]

(1) Supports up to 1125 IPv6 multicast routes and 1000 IPv4 multicast routes concurrently in H/W

(2) Changing SDM template requires reload

IPv6 Multicast Routing in Mixed 3750 Stack

- IPv6 Multicast Routing can be supported only by X and E switches with an active IP Services license level
- No support for Mixed Stack with IPBASE and or V2 members

Supported Features and Comparison with IPv4

	IPv6	IPv4
PIM-SM	15.0(2)SE	Yes
PIM-DM	No	Yes
PIM-bidir	No	Yes
SSM	15.0(2)SE	Yes
SSM Mapping for MLDv1 hosts	15.0(2)SE	Yes (for IGMPv2 hosts)
Auto RP for RP mapping	No	Yes
BSR for RP mapping	15.0(2)SE	Yes
VRF Awareness	No	Yes
Scoped Boundary	15.0(2)SE	N/A
Embedded RP Special Multicast Address	15.0(2)SE	N/A

Green Features

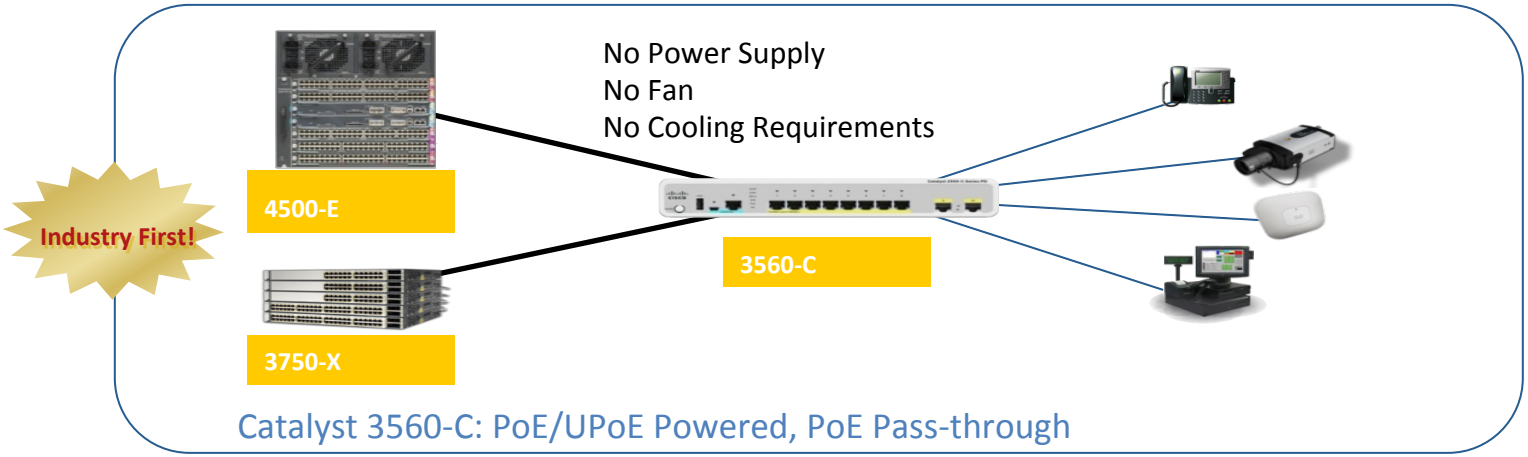
© 2010 Cisco and/or its affiliates. All rights reserved.

2960-C and 3560-C Series UPoE Support

Reduced Wiring Constraints and Costs with PoE pass-through

Eliminate the need for hundreds of meters of Ethernet cabling

- Support Up to 12 IP devices with just one Ethernet cable drop
- Save $100s to over $1000/drop depending on deployment scenario



Catalyst 3560-C: PoE/UPoE Powered, PoE Pass-through

Deploy applications in locations without access to power outlets

Power over Ethernet (PoE) pass-through:

- Compact Switch and PoE end devices powered by upstream PoE-capable switch/router
- First/only switch on the market to offer this unique feature

2960-C and 3560-C Series UPoE Support

IOS 15.0(2)SE (Nile) enables PD/PSE compact switches to be powered by 1 UPoE (60W) uplink

- PoE pass through does not require a second uplink
- Second UPoE uplink can be connected for high availability and redundancy
- Increase PoE Budget for downstream devices

Model	C3560CPD-8PT-S	C2960CPD-8PT-L	C2960CPD-8TT-L
Feature Set	IP Base	LAN Base	LAN Base
Ports	8 x 10/100/1000, PoE+	8 x 10/100, PoE	8 x 10/100
Uplinks	2 x 1G Copper or SFP		
Available PoE Power (1 UPoE uplink)	**23.8W**	**30.8W**	N/A
Available PoE Power (2 PoE+ uplinks)	15.4W	22.4W	N/A
Available PoE Power (1 PoE+ uplink)	0	7W	N/A
Auxillary Input	23.8W	30.8W	N/A

Whats New with EnergyWise 2.8

Features

- Wake On Lan Enhancements
- Agentless SNMP Translator (Printers)
- Support for PD/PSE switch

Upsell with EnergyWise

EnergyWise Fast-track 0$ SKU

- 0$ SKU with Joulex
- 0$ SKU with Verdiem
- 0$ SKU with CA

Sales Tools

- New Case Studies
- IVT Testing
- Solutions lab
- Deployment Guides *

Cisco End to End

- Cisco VXI
- LMS / Prime
- 4K / 6K / ISR

Wake-on-LAN Enhancement

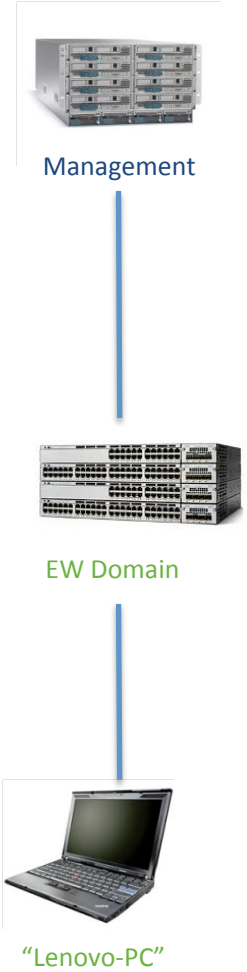
Same, Single Unified Method for Wake and Sleep

Before Enhancement

Wake up “Lenovo-PC”

energywise query importance 100
name * wol mac XXXX.XXXX.XXXX

WoL magic packet send on all ports, received by PC, now powered on.



After Enhancement

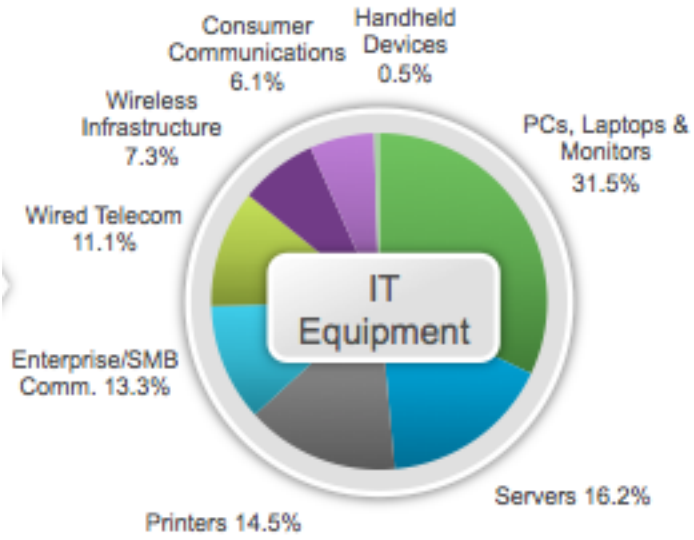
Wake up “Agent-PC”

energywise query importance 100
name Agent-PC set level 10

WoL magic packet send on the right port, received by PC, now powered on.

EnergyWise SNMP Translator (Agentless)

- Background: some devices, like printers, are not EnergyWise enabled, and are not PoE Powered.



Problem : Incomplete coverage of IT assets.

Solution : Translate other protocols to EnergyWise

How it Works – SNMP Translator

- Map EnergyWise and SNMP Data Models – Translation file – load in flash.
- SNMP endpoints become transparently managed as if they were native EW endpoints.
- Translation file stored in cisco.com

EnergyWise Value

Name (fn_get_name)

Unit (fn_get_units)

Power Level (fn_get_level)

Translation File

fn_get_name<->sysName

fn_get_units= WATTS

fn_get_level

SNMP OIDs

sysName (1.3.6.1.2.1.1.5.0)

1.3.6.1.4.1.253.8.53.13.2.1.6.1.111.6

Verification

- If everything has been configured properly, you should see:

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

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

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

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

joulex

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

Verdiem

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

ca technologies

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

Low TCO and other Access Features

© 2011 Cisco and/or its affiliates. All rights reserved.

Smart Install – Vlan 1 Enhancement

Behavior before 15.0(2)SE: Client to upstream switch connection

- New clients attempt to acquire IP address on vlan 1 interface by default
- Changing Vlan 1 behavior on client breaks zero touch deployment
  - No need for Smart Install if customer touches all clients
- Cisco best practices requests/requires no vlan 1 in L2 network
  - Aggregation/distribution layer will not have vlan 1 configured.
- Customers uncomfortable with vlan "hopping"
  - Willing to allow for short term – to get new client operational

15.0(2)SE onwards, Client connects on SMI start-up management vlan

- Director advertises start up management vlan to all clients
- Client will connect on advertised vlan interface
  - Creates start-up vlan interface
  - Does DHCP on start-up vlan interface
- New client learns startup mgmt vlan via CDP

Catalyst Clients will have 15.0(2)SE in manufacturing by 2HCY13

Resilient Ethernet Protocol (REP)
Benefits and Characteristics

- Fast and predictable convergence
  - Convergence time: 40ms to 450ms
  - Fast failure notification even in large rings with high number of nodes
  - Predictable failover behavior with configurable preemption and alternate port
- Co-existence with Spanning Tree
  - STP is deactivated on REP interfaces
  - Limit the scope of Spanning tree
  - Topology Changes Notification from REP to STP
- Optimal bandwidth utilization
  - VLAN Load balancing
- Easy to configure and troubleshoot

REP (Resilient Ethernet Protocol)

Support in 15.0(2)SE

- S/W and H/W support, scalability and performance information:

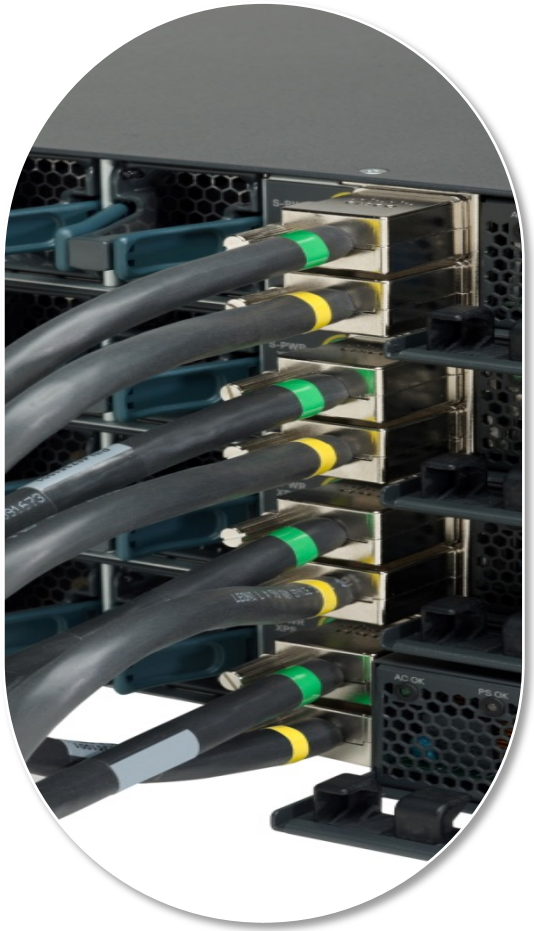
Minimum IOS	15.0(2)SE
H/W Platforms	3560X 3750X 3560E 3750E
Minimum feature set	IPBASE
# rings per node	64
# nodes per ring	Tested with 32
Unicast Convergence	40ms
Multicast Convergence	60ms
Cross-stack EC Unicast Convergence	250ms
Cross-stack EC Multicast Convergence	450ms

NOTE: Performance results may vary based on topology, configuration and traffic profile

StackPower coming to LAN Base

Start selling StackPower in LAN Base now!

- StackPower now available on all 3750-X LAN Base switches (-L)
- Release supported is 15.0(2)SE
- Existing 3750-X LAN Base customers will be able to upgrade for free*
- StackPower cable not included



* Existing customers will be able to get the software update for free but will be required to purchase the StackPower cable separately

Now Shipping

Introducing Catalyst 2960-SF

- 24 & 48 10/100 downlink ports
- 2 & 4 1G SFP uplink ports
- FlexStack (optional module)
- 2960-SF will stack with 2960-S
- PoE+ support & full-power model (740W)
- IPv6 support & First-hop security
- Enhanced Limited Lifetime Warranty

Catalyst 2960-S features at 10/100 speeds

© 2010 Cisco and/or its affiliates. All rights reserved.

2960-SF and 2960 feature comparison

2960	2960-SF
• Released 2006	• Available August 2012
• Does not stack	• FlexStack (20Gbps) • Optional module required

• Available with POE (15.4W)
  • 124 or 370W total budget
	• Available with POE+ (30W)
	  • 370W or 740W total budget

• Minimal IPv6 support	• IPv6 host capable • IPv6 first-hop security features

• Uplink options :
  • 2x 1000BASET
  • 2x “combo” (1000BASE-T or SFP)
	• SFP uplinks
	  • 2 or 4

• 64MB of DRAM • 32MB of flash	• 128MB of DRAM • 64MB of flash
• Serial console port	• USB & serial console

Thank You

© 2010 Cisco and/or its affiliates. All rights reserved.