cisco The bridge to possible

Cisco SD-Access Zero-Touch Provisioning Using LAN Automation

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

BRKENS-2800

cisco Live!

Cisco Webex App

Questions?

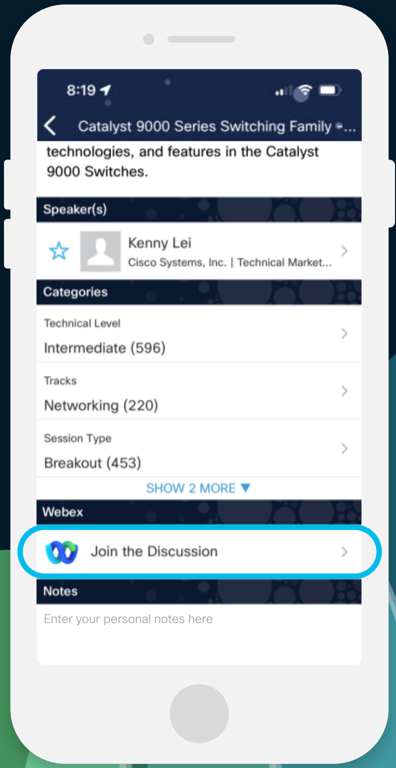
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKENS-2800



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Cisco Live US SD-Access/ISE Learning Map

Sunday–2nd

○ TECENS-2820 9AM
Cisco Software-Defined Access LISP: Architecture Overview

Monday–3rd

○ BRKENS-2810 8:30AM
Cisco Software-Defined Access LISP Solution Fundamentals

○ BRKENS-2800 9:30AM
Cisco SD-Access Zero-Touch Provisioning Using LAN Automation

○ BRKENS-2811 1PM
Connecting Cisco SD-Access LISP to the World: Use Cases and Segmentation

LTRENS-2419 1PM
○ SD-Access LISP Pub/Sub Wired Lab

BRKENS-2816 3PM
Cisco SD-Access Transit: Advanced Design Principles ○

○ BRKSEC-2100 10:30AM
ISE Your Meraki Network with Group Based Adaptive Policy

○ BRKENS-1802 2:30PM
SD-Access Success Stories: Concept to Reality by Petrobras and Ford Motor

○ BRKSEC-2091 3PM
Cisco ISE Performance, Scalability and Best Practices

○ BRKENS-1852 4PM
TrustSec Refresh Reinforced with Latest Segmentation Innovations

Tuesday–4th

○ BRKENS-2502 10:30AM
Cisco SD-Access LISP VXLAN Fabric Best Practices: Design and Deployment

○ BRKENS-1801 4PM
SD-Access Success Stories: Concept to Reality by Stanford Health and Yale University

Wednesday–5th

BRKENS-2833 10:30AM
○ LISP: Optimized Control Plane for Software-Defined Access

BRKENS-2819 2:30PM
○ Cisco SD-Access and Multi-Domain Segmentation

CIUG-1003 2:30PM
Zero Trust with Software-Defined Access Roadmap Update

○ BRKENS-2821 4:00PM
Cisco SD-Access LISP VXLAN Fabric for Manufacturing Verticals

Thursday–6th

BRKENS-2827 11:00AM
Cisco SD-Access Migration Tools and Strategies

○ BU-led sessions

Catalyst Center

Cisco SD-Access LISP

ISE

Cisco ISE

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

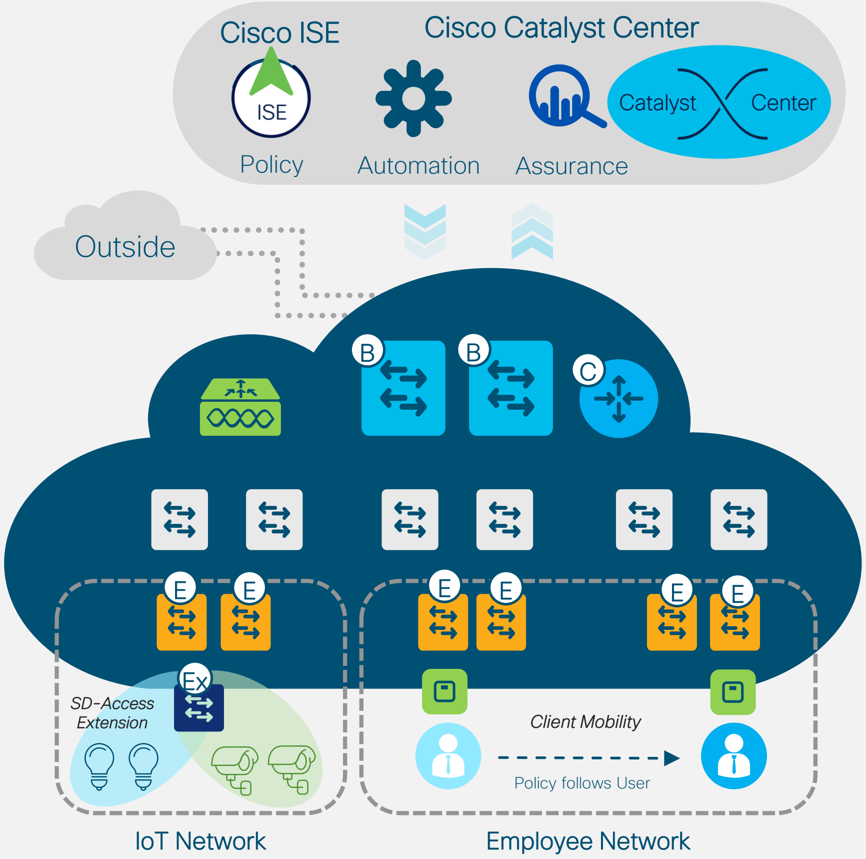
Cisco Catalyst Center (formerly Cisco DNA Center)

- Introduction
- Lan Automation Overview
- Lan Automation Planning
- Lan Automation Design
- Lan Automation Discovery
- Lan Automation Provision
- Conclusion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst Center
Device Onboarding options

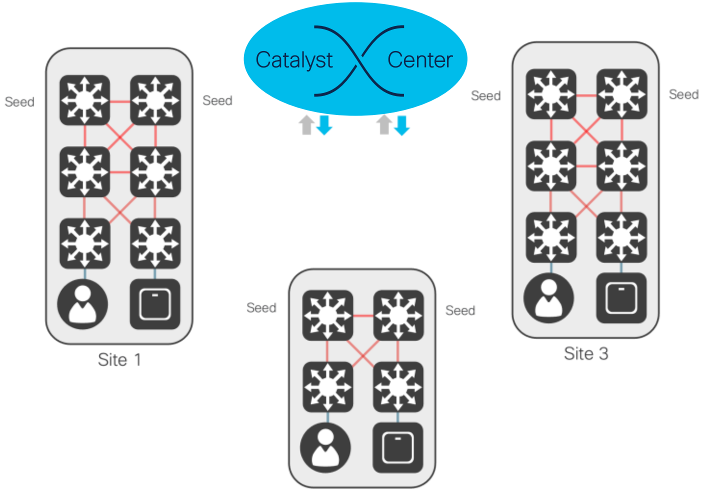
Manual | Semi-Automated Underlay

Device-by-Device onboarding and configuration either manually or through Cisco Plug-and-Play.

Automated Underlay(Lan Automation)

Turnkey solution to onboard multiple switches with image management and best-practices configuration.

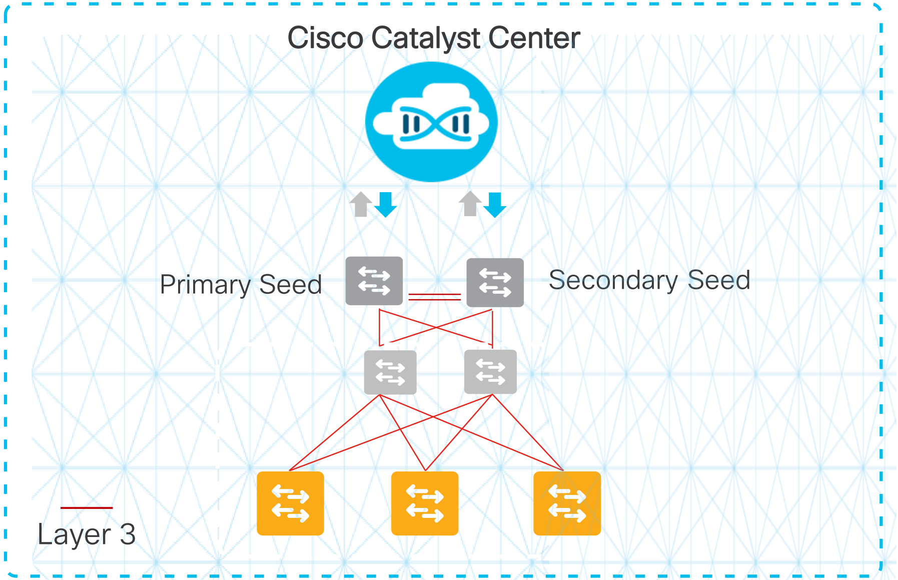
Underlay multicast to optimize overlay subnet multicast/broadcast distribution



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

LAN Automation for Error-Free Underlay

Adopted by 60% of SD-Access customers



- Automated Routed access Underlay for N-tier topology
- Inbuilt with best-practices

Accelerates organizations SD-Access overlay deployment

Lan Automation Overview

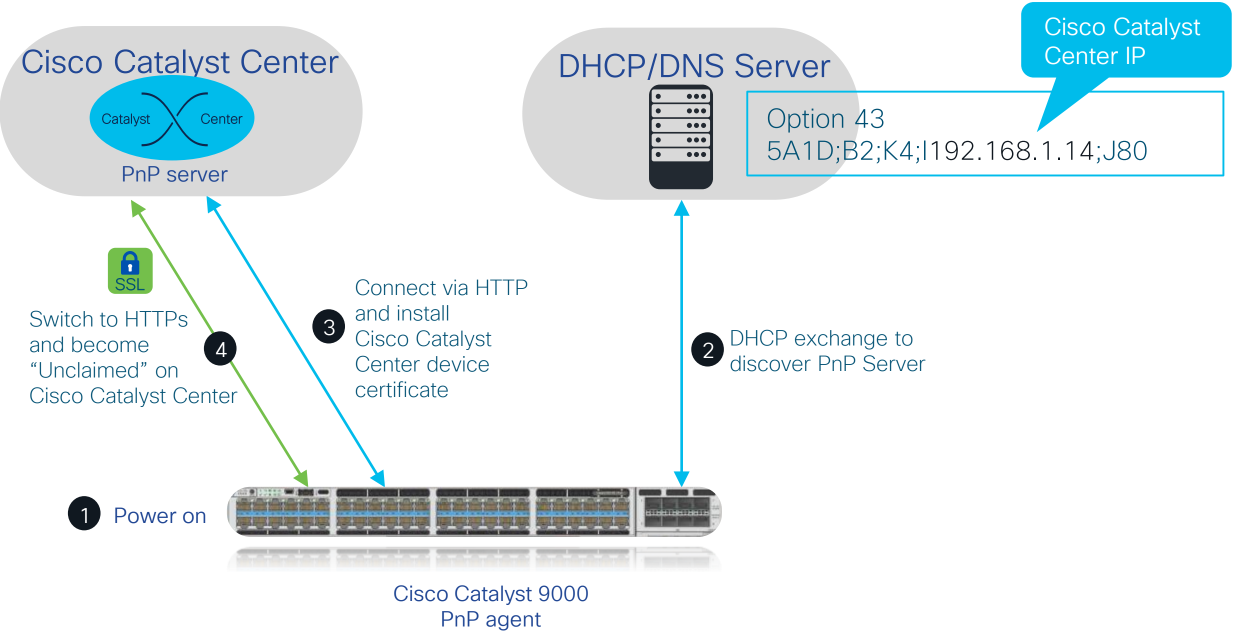
Cisco Plug and Play

5 Assign Site

6 Add CLI Template

7 Image upgrade

8 Claim Device



Cisco Catalyst Center

PnP server

DHCP/DNS Server

Cisco Catalyst Center IP

Option 43
5A1D;B2;K4;I192.168.1.14;J80

4 Switch to HTTPs and become "Unclaimed" on Cisco Catalyst Center

3 Connect via HTTP and install Cisco Catalyst Center device certificate

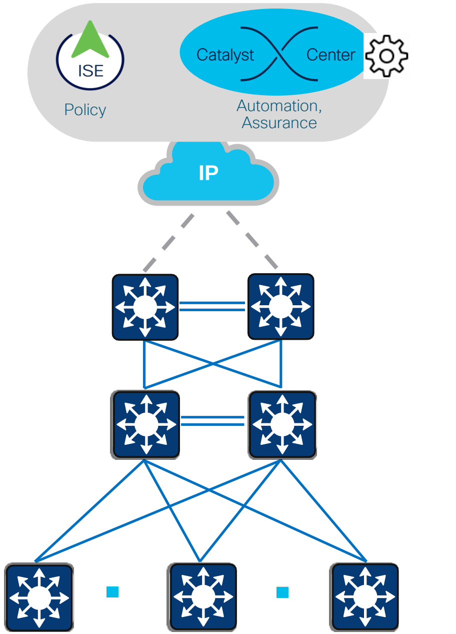
2 DHCP exchange to discover PnP Server

1 Power on

Cisco Catalyst 9000
PnP agent

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Lan Automation



Traditional Networks

Lan Automation

- Simplifies network operations
- Frees IT staff from time-consuming, repetitive network configuration tasks
- Creates a standard, error-free underlay network

Lan Automation Benefits

- Zero-touch provisioning
- End-to-end topology
- Resilience
- Security
- Compliance

▣	Managed Device
▣	PnP Agent
—	Layer 3
—	Layer 2
⬚	LAN Automation Boundary

Layer 3 —
Layer 2 —

Lan Automation Overview

Simplified Procedure

Cisco Lan Automation Workflow – 4 Step Process

Planning

- Network Design
- Supported Switches
- Site/IP Pool Planning

Design

- Sites across geographic
- Global network services
- Design IP Address Pools

Discover

- Discover Network devices
- Physical Topology
- Network Readiness

Provision

- Dynamic automation
- Optimized routing design
- Resilient underlay settings

SD-Access Ready Network

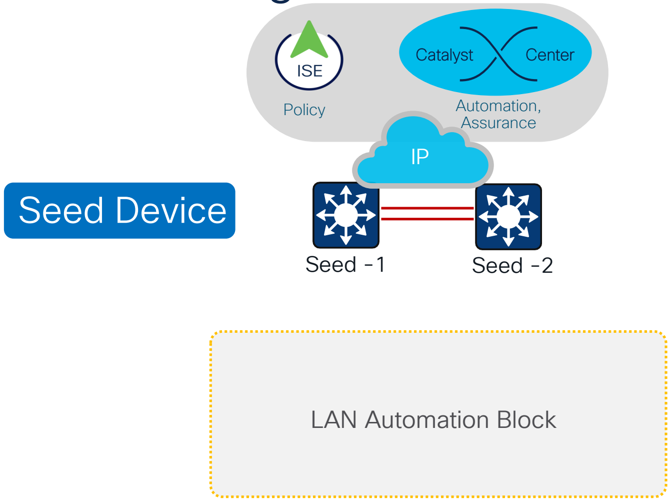
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

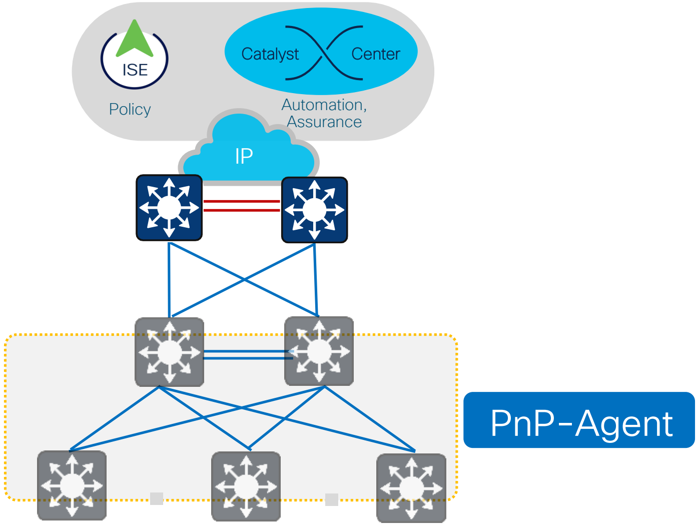
LAN Automation

Step1: Planning

Lan Automation – Planning

Understanding Device Roles





Seed Device

Intermediate system(s) between Core and new network block

Key system to discover, automate and on-board new Catalyst switches in network

Device can be automated using Cisco PnP or configured Manually

Only one Seed is required, Device discovery happens only on the primary seed device interfaces

Peer Seed(Seed-2) can be Lan automated.

PnP-Agent Device

Catalyst switch* with factory-default settings and waiting at startup-wizard state

Interconnect between Seed and another PnP-Agent device in the network

License Auto Upgrade – Catalyst Center release 2.3.5 onwards

■ Managed Device

▨ PnP Agent

🟥 Layer 3

🟦 Layer 2

⬚ LAN Automation Boundary

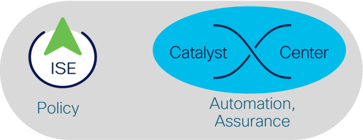
* - C9K or C3850

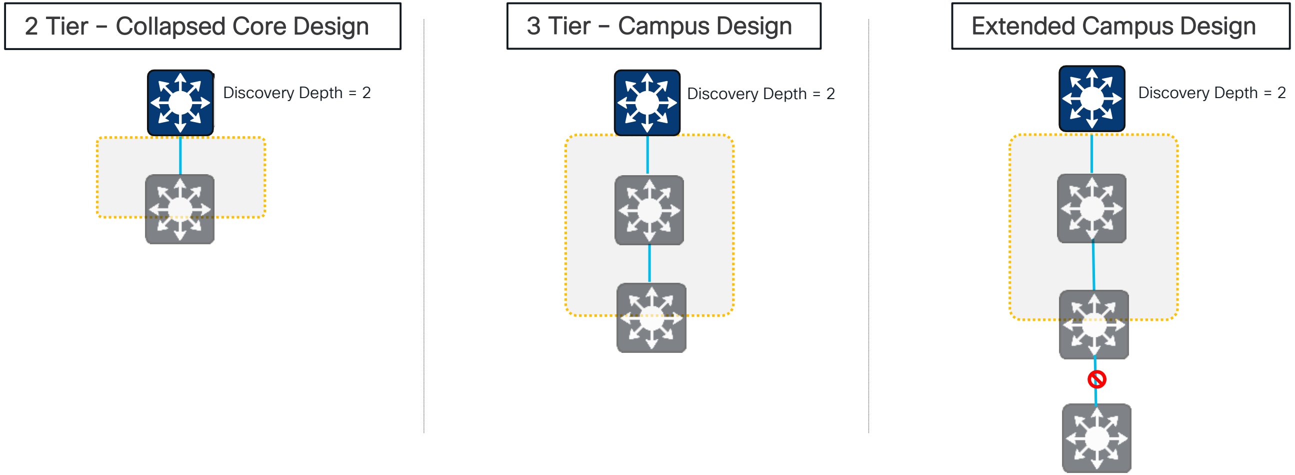
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

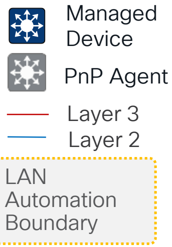
*Catalyst Center: 2.3.7.x

Lan Automation – Planning

Automation Boundary







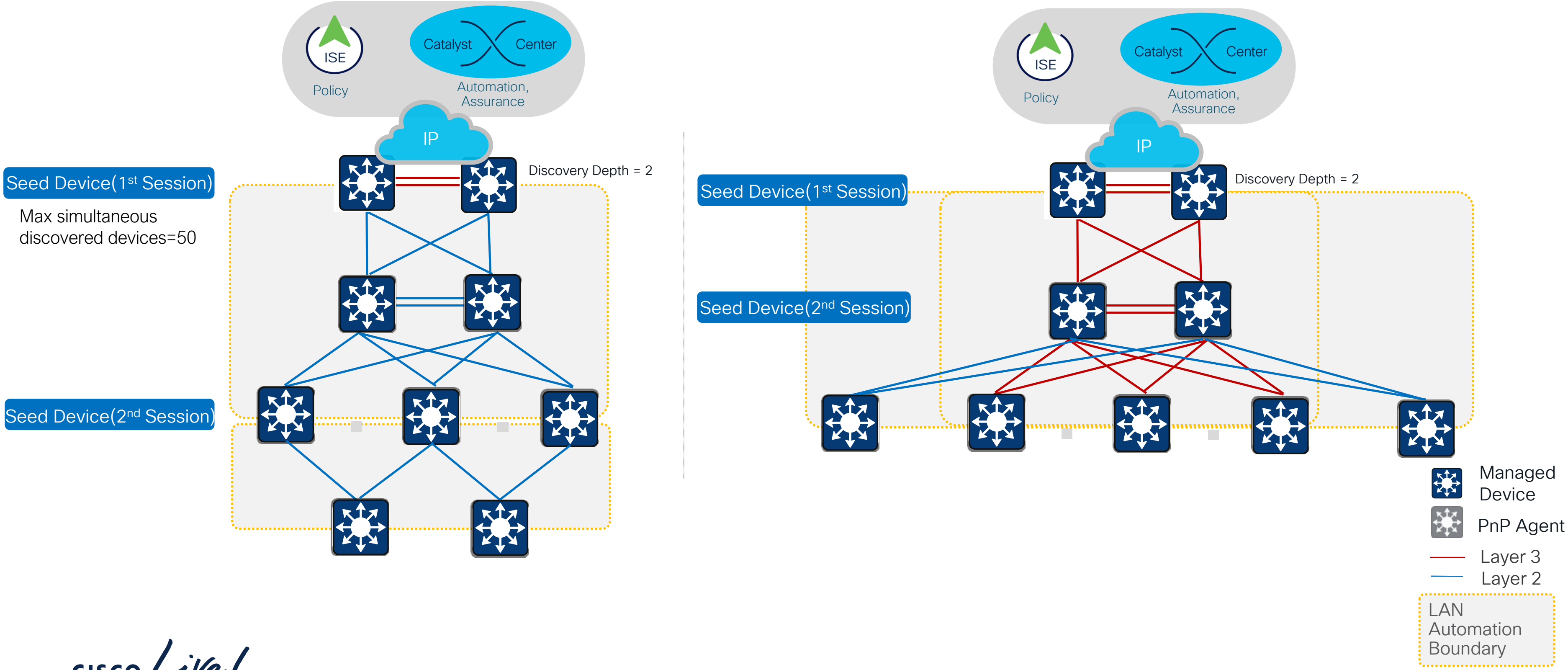
Underlay Automation Boundary

Maximum Automation boundary(**Discovery Depth**) from Seed Device: 1 to 5 (Default: 2)*

Supporting common hierarchical and structured Enterprise network designs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning
Multistep for Large Topologies



ISE

Policy

Catalyst Center

Automation, Assurance

IP

Discovery Depth = 2

Seed Device(1st Session)

Max simultaneous discovered devices=50

Seed Device(2nd Session)

ISE

Policy

Catalyst Center

Automation, Assurance

IP

Discovery Depth = 2

Seed Device(1st Session)

Seed Device(2nd Session)

Managed Device

PnP Agent

Layer 3

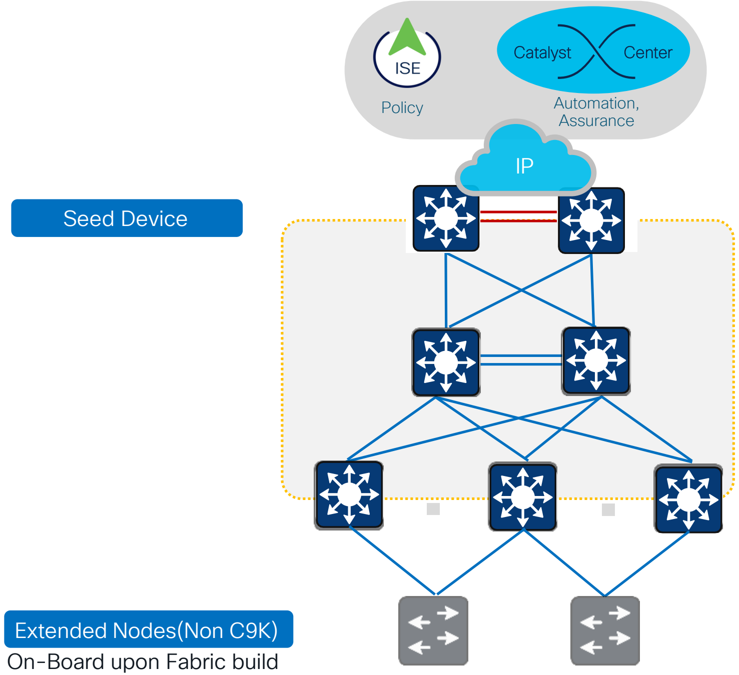
Layer 2

LAN Automation Boundary

Lan Automation – Provision

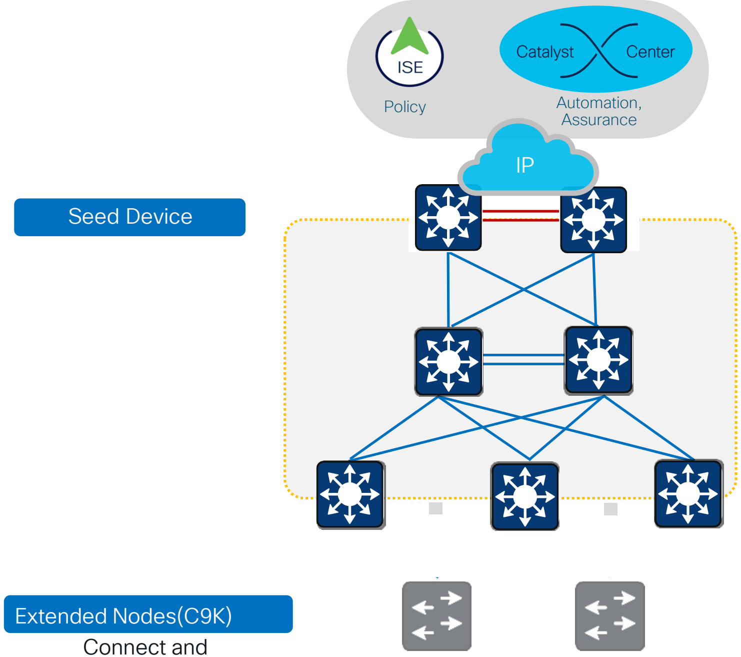
Network Expansion

Lan Automation with Non C9K as Extended Nodes



On-Board upon Fabric build

Lan Automation with C9K as Extended Nodes



Connect and
On-Board upon Fabric build

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning

Pre-Requisites

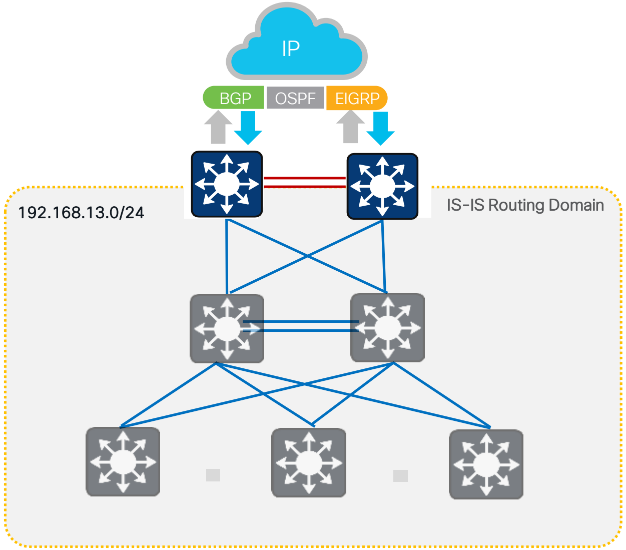
- MTU on the Seed device set to 9100
- **Seed Device:** Interface to PnP Agents should be defaulted
- Seed devices are reachable to Catalyst center, discovered and assigned to Site Hierarchy.
- PnP Agents are FACTORY DEFAULTED, running ADVANTAGE license and booted in INSTALL Mode
- Minimum Lan Automation IP Pool /29

Constraints

- No Automation of StackWise Virtual (SVL) switch via PnP. SVL switch can only be used as a seed device.
- No support for stack renumbering.
- For platform support, see Supported Switches for Each Role at Different Layers.
- Not supported on Switch dedicated management port

Lan Automation – Planning
Seed Switches IP Routing configuration

Seed Device
Manual Configuration for discovery
- Loopback IP
- Login Credentials
- SNMP Commands
- MTU
- Line VTY Commands
- IP Routing
- Northbound
  - Routing Protocol
  - Interface configs
- Netconf-yang
- Domain Name
- SSH



BGP

```
router isis
  redistribute BGP <as_number> route-map <name>
!
ip route 192.168.13.0 255.255.255.0 Null0 250
!
router bgp <as_number>
Network 192.168.13.0
```

OSPF

```
router isis
  redistribute ospf <id> metric <count>
!
router ospf <id>
  redistribute connected route-map <name>
  summary-address 192.168.13.0 255.255.255.0
```

EIGRP

```
router isis
  redistribute eigrp <id> metric <count>
!
interface <id>
  description CONNECTED TO CORE
  ip summary-address eigrp <AS> 192.168.13.0 255.255.255.0
```

Automated IS-IS Routing Configuration

Optional if IS-IS routing protocol in Core

Automates IS-IS routing process configurations on Seed and each PnP-Agent systems. No manual configuration required.

Programs default-route injection on selected Seed Device for global network reachability

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning

IP Pool Planning

IP Pool Type and Usage

Roles	Mandatory	Pool Type	Usage
Main/Principal IP Pool	Yes	LAN	Temp DHCP Pool* Loopback(/32) P2P L3 Links(/31)* Multicast
Link Overlapping IP Pool	No	LAN	Temp DHCP Pool P2P L3 Links(/31)

IP Pool Allocation Logic

Allocation Logic	TEMP Pool	Rest of the Pool
Less than /21	/23(512 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast
/24	/26(64 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast

IP Pool Usage Example

Allocated Pool	Total Devices to Automate	No of Uplinks	TEMP DHCP Range	Loopback Range	P2P Range	Total IP's
Main/Principal IP Pool 192.168.13.0/24	10	2 (one each to Primary and Secondary Seed)	First /26 (192.168.13.1 to 63)	Next /27 (192.168.13.65 to 94)	Remaining IPs (192.168.13.96 to 254)	10 – Temp DHCP(Released upon completion) 10 – Loopback 40 – P2P Uplinks

* – Link Overlapping IP Pool not provided

LAN Automation Step - 2: Design

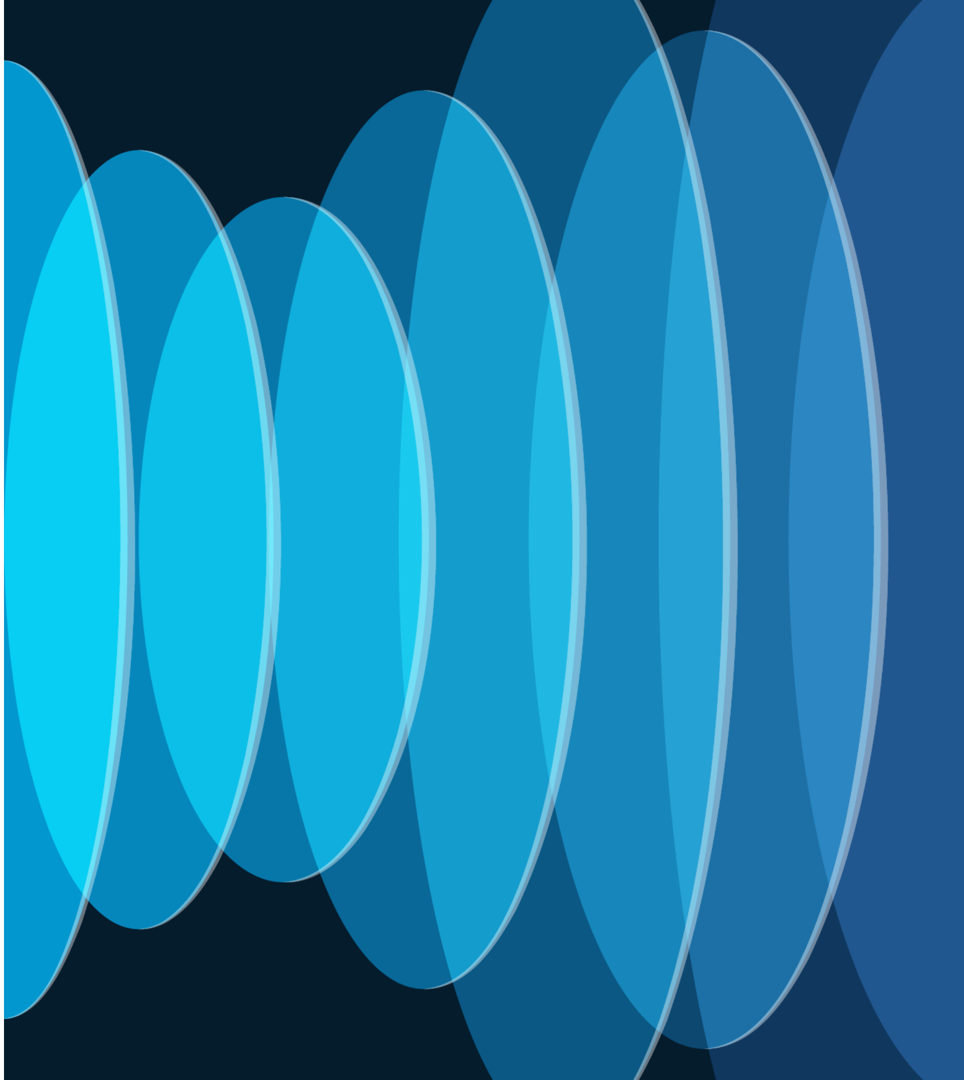
Lan Automation – Design

Configuration Summary

Optional	Integrate Cisco Catalyst Center and Cisco ISE
Step-1	Build Network Hierarchy based on geographic locations
Step-2	Configure Network Services – Global | Area | Site level
Step-3	Configure Network Address Range – Global | Area | Site level
Step-4	Configure LAN IP Pool from Parent – Global | Area | Site level

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design Demo



LAN Automation Step3: Discovery

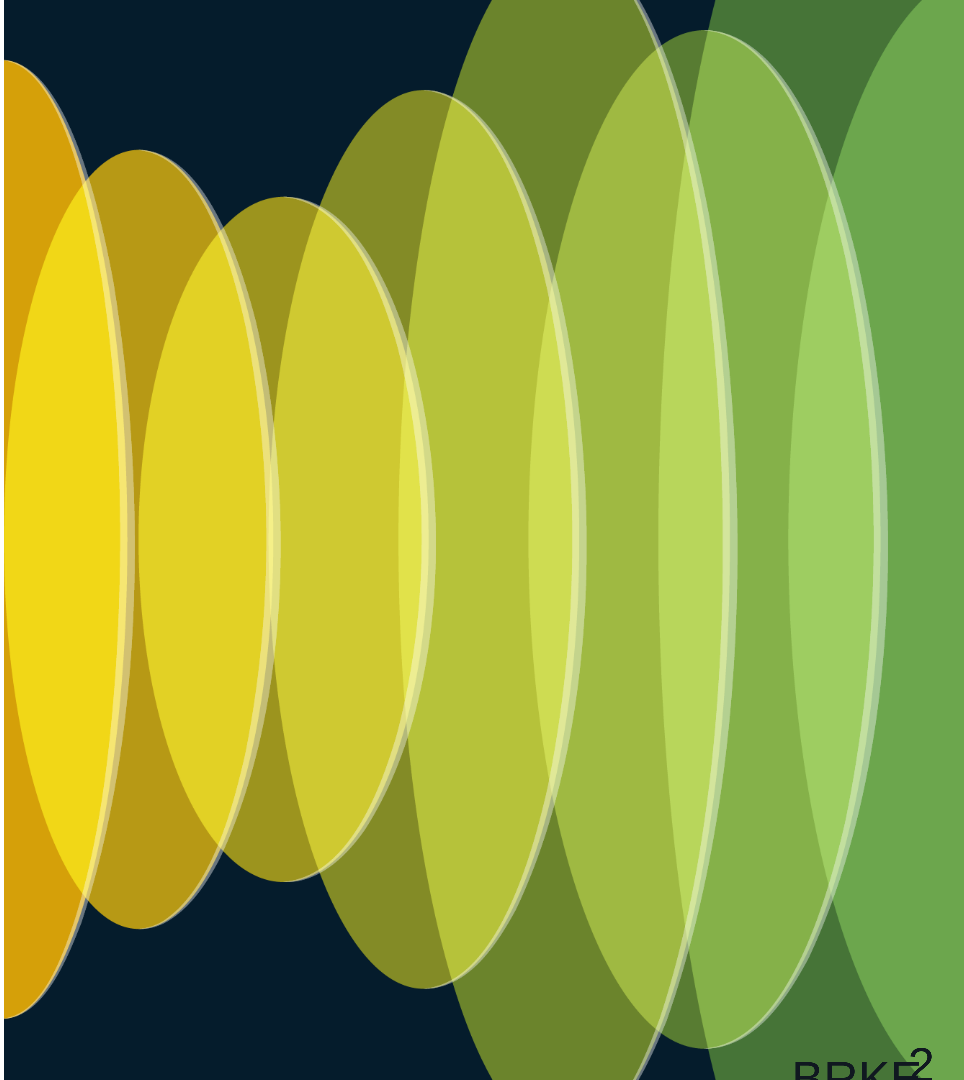
Lan Automation – Discovery

Configuration Summary

Step-1 Build Discovery Profile to discovery both Seed Devices

Step-2 Assign Discovered devices to Site

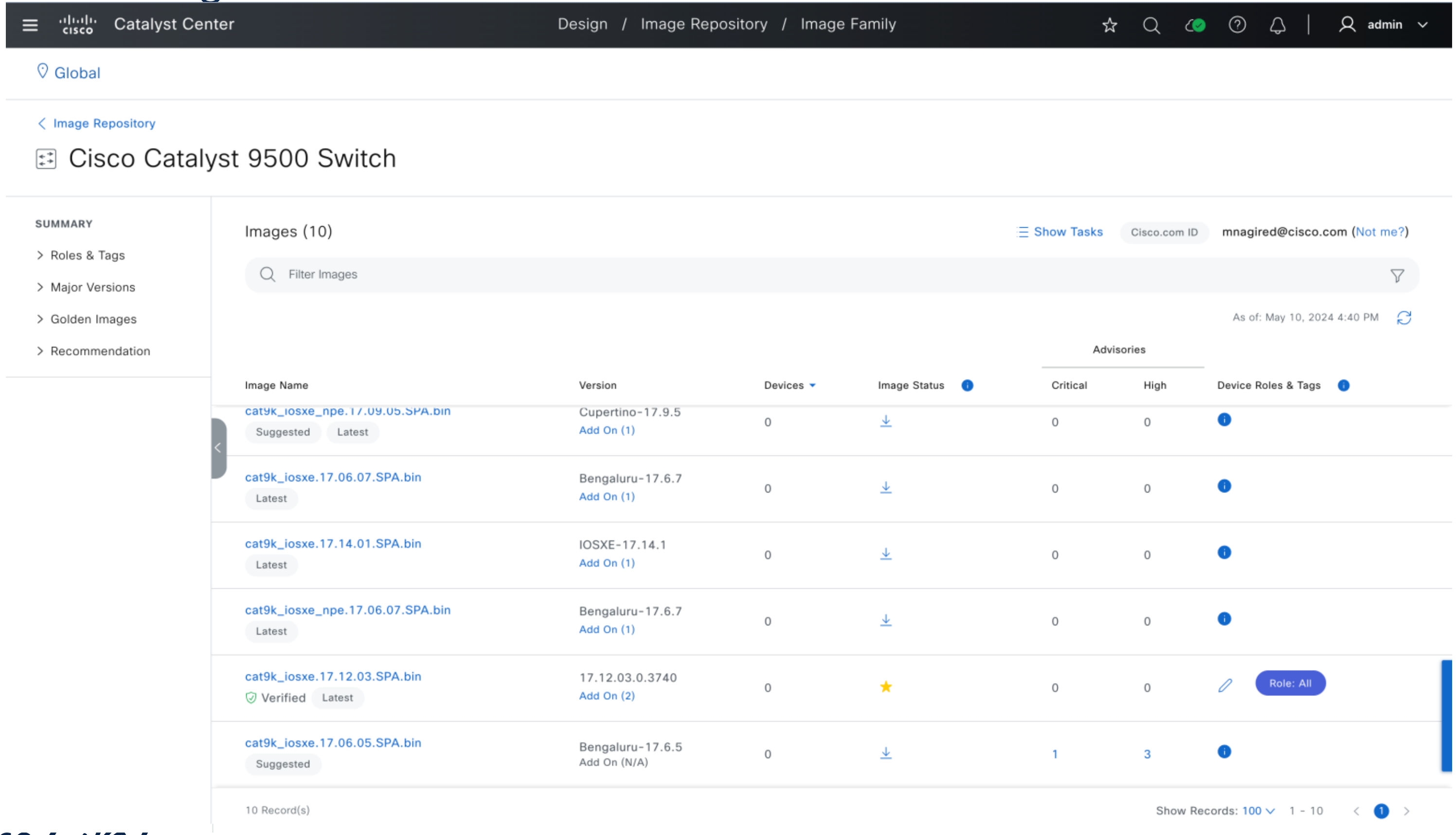
Discovery Demo



LAN Automation Step4 : Provision

Lan Automation – Provision

Golden Image Download



Cisco Catalyst 9500 Switch

Images (10)

mnagired@cisco.com (Not me?)

As of: May 10, 2024 4:40 PM

Image Name	Version	Devices	Image Status	Advisories Critical	Advisories High	Device Roles & Tags
cat9k_iosxe_npe.17.09.05.SPA.bin Suggested Latest	Cupertino-17.9.5 Add On (1)	0	↓	0	0	ⓘ
cat9k_iosxe.17.06.07.SPA.bin Latest	Bengaluru-17.6.7 Add On (1)	0	↓	0	0	ⓘ
cat9k_iosxe.17.14.01.SPA.bin Latest	IOSXE-17.14.1 Add On (1)	0	↓	0	0	ⓘ
cat9k_iosxe_npe.17.06.07.SPA.bin Latest	Bengaluru-17.6.7 Add On (1)	0	↓	0	0	ⓘ
cat9k_iosxe.17.12.03.SPA.bin Verified Latest	17.12.03.0.3740 Add On (2)	0	★	0	0	Role: All
cat9k_iosxe.17.06.05.SPA.bin Suggested	Bengaluru-17.6.5 Add On (N/A)	0	↓	1	3	ⓘ

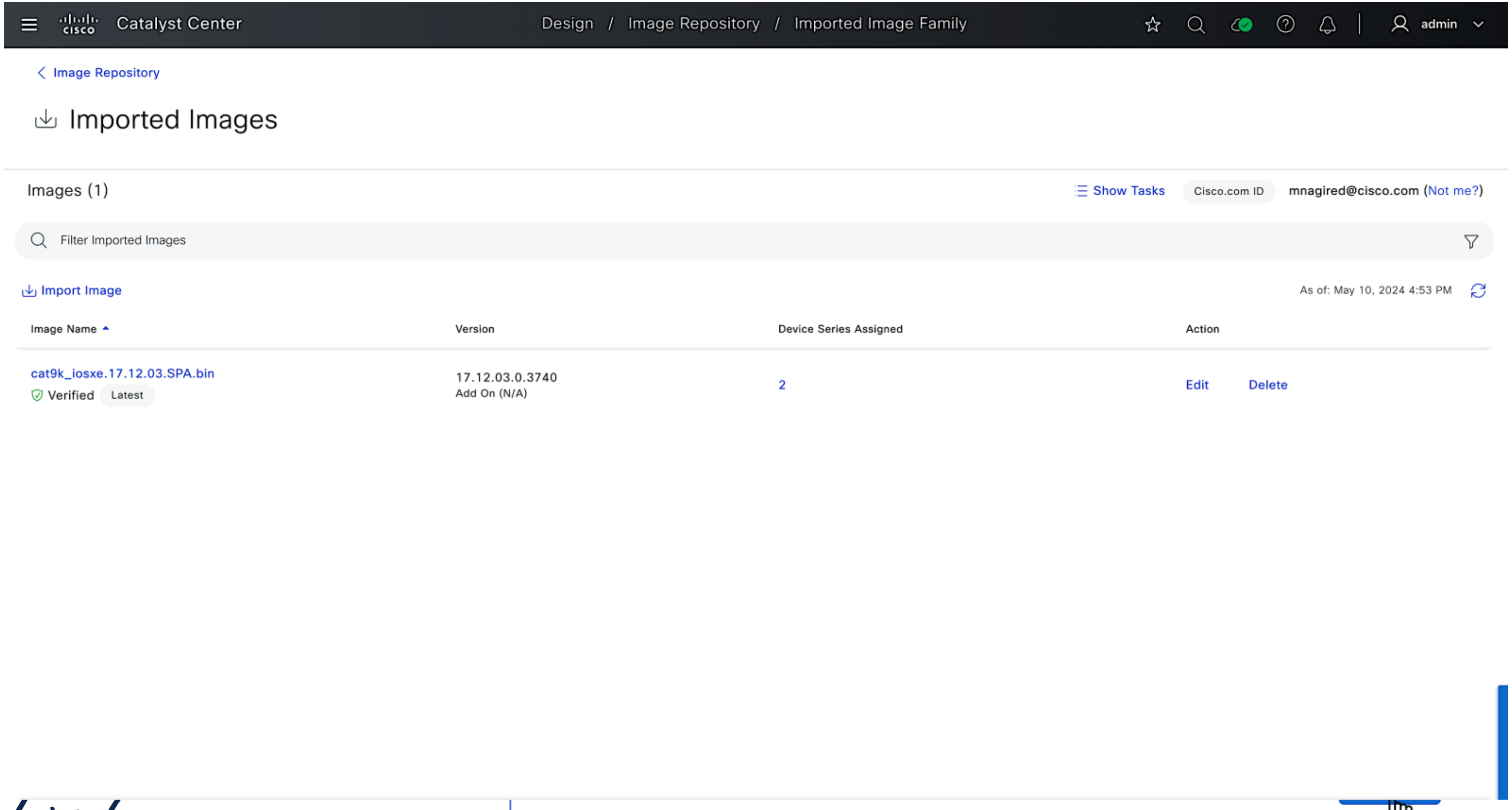
10 Record(s)

Show Records: 100 1 - 10 1

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Provision

Golden Image Selection for PnP Agent Devices



Imported Images

Images (1)

mnagired@cisco.com (Not me?)

As of: May 10, 2024 4:53 PM

Image Name	Version	Device Series Assigned	Action
cat9k_iosxe.17.12.03.SPA.bin Verified Latest	17.12.03.0.3740 Add On (N/A)	2	Edit Delete

Lan Automation – Provision

Switch Factory default

Restore the switch configurations to factory default using the following commands:

- **For Cisco IOS XE 16.11 and earlier, use:**

  [CLI config mode]

  ```
  no pnp profile pnp-zero-touch
  no crypto pki certificate pool
  crypto key zeroize  (remove any other crypto certs)
  config-register 0x2102 or 0x0102  (if not already)
  do write
  end
  ```

  [CLI exec mode]

  ```
  delete /force nvram:*.cer
  delete /force stby-nvram:*.cer (if a stack)
  delete /force flash:pnp-reset-config.cfg
  write erase
  reload (enter no if asked to save)
  ```

- **For Cisco IOS XE 16.12.x or later, use:**

  [CLI exec mode]

  ```
  pnp service reset no-prompt
  ```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Provision
Configuration Summary

Pre-Req

- IP Pool Subnet Reachability from Catalyst Center
- Unplug Management port
- Ensure Seed Ports are layer 2/defaulted
- Ensure PnP Devices are not present in the Inventory

Step-1 Start Underlay Network discovery and automation

Step-2 Stop Underlay Network discovery and automation

Step-3 Provision Global Network services

Step-4 Designate System role to build structure network topology

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

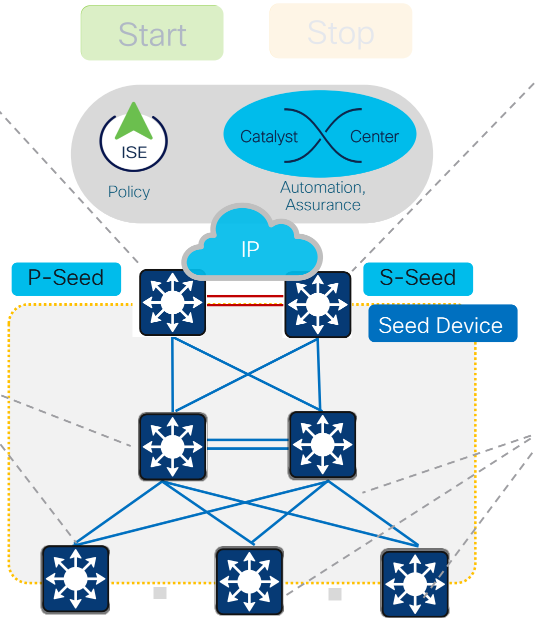
Lan Automation – Provision

- Loopback0
- Routing Protocol: ISIS
  ISIS Type: Level 2*
  Default Info Originate
- **BGP Advertisement**
- **DHCP Pool**
- Interface vlan 1
- Loopback 60000**
- RP_address**
- Multicast Routing**
- PIM**
- MSDP*

- **No DHCP Pool**
- No Interface vlan 1
- P2P Links
- Disable CTS
  Enforcement***

- Certificates
- Loopback0
- Routing Protocol: ISIS
  ISIS Type: Level 2*
- SSH
- IP Routing
- VTP- Transparent
- Rapid-pvst
- Error disable Recovery
  SNMP
- MTU 9100
- BFD
- Local Credentials
- Hostname
- RP_address**
- Multicast Routing**
- PIM**

- No Interface vlan 1
- P2P Links
- Disable CTS
  Enforcement***



- Loopback0
- Routing Protocol: ISIS
  ISIS Type: Level 2*
  Default Info Originate
- Loopback 60000**
- RP_address**
- Multicast Routing**
- PIM**
- MSDP**

- No DHCP Pool
- No Interface vlan 1
- P2P Links
- Disable CTS
  Enforcement***

- Certificates
- Loopback0
- Routing Protocol: ISIS
  ISIS Type: Level 2*
- SSH
- IP Routing
- VTP- Transparent
- Rapid-pvst
- Error disable Recovery
  SNMP
- MTU 9100
- BFD
- Local Credentials
- Hostname
- RP_address**
- Multicast Routing**
- PIM**

- No Interface vlan 1
- P2P Links
- Disable CTS
  Enforcement***

* Starting Catalyst Center 2.3.3
** With Underlay Multicast Enabled
*** Starting Catalyst Center 2.3.7.5

Provision Demo

Lan Automation Enhancements

LAN Automation Enhancements 2.3.5.0

- Dedicated LAN Automation landing page
- 5 Simultaneous LAN Automation sessions with one session per site
- Day N Add or Delete L3 links

LAN Automation Enhancements 2.3.7.0

- Workflow now support /27,/28 and /29 LAN pools
- Deterministic loopback IP addresses(Day 0 & Day N*)

LAN Automation Enhancements 2.3.7.5

- Discovery depth level for LAN automation(Default depth=2)
- Auto PnP reset for error devices
- Session Attributes
  - Session Timeout
  - Device Matching
    - Relaxed
    - Strict

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-Access **Customer Success**

	Healthcare	Education + Energy		Manufacturing
	Stanford HEALTH CARE	Yale	BR PETROBRAS	Ford
	Register - BRKENS-1801		Register - BRKENS-1802	
SCALE	6200 devices 10K+endpoints	6500 devices 66K+endpoints	5300 devices 57K+endpoints	4500 devices 10K+endpoints
REQUIREMENTS	Zero-Trust Access Endpoint Profiling	API Tooling Resilient Network & Security Visibility		EV Manufacturing Reliable Wall to Wall WIFI Connectivity

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you