# LAN Automation: Step-by-step deployment guide and Troubleshooting

# Contents

Introduction Planning Understanding system roles **Primary Device PnP-Agent Device** Automation Boundary Supported switches for each role at different layers Site Planning **IP Pool Planning** Site specific CLI/SNMP configuration Configuration on seed device(s) Additional recommended configuration on seed device(s) **PNP-agent initial state** Design Discover Steps to consider before starting LAN auto 1a) IP Pool Subnet reachability from DNAC 1b) Static Route addition for LAN Pool 2) PNP-agent initial state before starting Lan auto 1. Ensure the PNP-agent is at "System Configuration Dialog" state before starting Lan auto. 2. Stack considerations 3. Un-plug the management port 4. Seed ports must be Laver 2 5. Ensure port on primary seed connecting to the PNP-agent(s) is not STP blocking 6. Device being discovered (PNP-agent) should not be present in Inventory 7. Device being discovered should (PNP-agent) not be present in PnP database 8. Ensure the PNP-agent is running DNA ADVANTAGE license level 9. Ensure PNP-agent is in INSTALL mode for image upgarde to take place during Lan automation **Provision** 1. Start Lan Automation 2. Stop Lan Automation **Miscellaneous** 1. Adding a brand new switch or a switch never present in DNAC to a LAN automated stack 2. Adding a switch already present in DNAC to a LAN automated stack 3. Configuring additional links after Lan auto is stopped 4. Moving uplink to the newly added switch 5. Using 9500H as seed device or PNP agent 6. Using 40G interface on Catalyst 9400 **Known Issues** 

## What's new in DNA Center 1.3.0

## Troubleshooting

The customer facing document can be found here: <u>https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech\_notes/b\_dnac\_sda\_lan\_automation\_deployment.html?cachemode=refresh</u>

## Introduction

Cisco DNA Center's LAN Automation helps simplify network operations, free IT staff from time-consuming and repetitive network configurations tasks, and create a standard error-free underlay network. LAN Automation helps accelerating building SD-Access underlay networks without traditional network planning and implementation process.

Cisco LAN Automation provides following key benefits to Enterprise customers:

- Zero touch provisioning: Network devices can be dynamically discovered, on-boarded and automated from their factory default state to fully integrated system into the network.
- End-to-end topology: Dynamic discovery of new network devices and their physical connectivity can be modelled and programmed. These new network devices can be automated with layer 3 IP addressing and routing protocols to dynamically build end-to-end routing topologies.
- Resilient: Cisco LAN Automation integrates system and network configuration parameters that optimize forwarding topologies and redundancy. The intelligence within Cisco LAN Automation tool understands system-level reddundancy and automates best practices to enable best-in-class resiliency during planned or unplanned network outages.
- Secured: Cisco receommended network access and infrastructure protection parameters are automated providing uncompromised security from its initial deplyment stage.
- Compliance: LAN Automation helps eliminating human errors, mis-configurations, and inconsistent rules and settings that result in end-user experience and IT overheads. During new system on-boarding process, LAN Automation automates globally managed parameters from Cisco DNA Center providing compliance across the network infrastructure,

The Cisco LAN Automation workflow helps enterprise IT administrators to prepare, plan, and automate greenfield networks.

This guide will cover best practices, pre-requisites, steps to configure LAN Automation and how to troubleshoot issues

LAN Automation workflow: LAN Automation workflow consists of four main steps:

- 1. **Planning**: Understand different roles in the LAN Automation domain and list of supported devices. It also talks about the site and IP pool planning and pre-requisites needed on the primary device.
- 2. **Design**: Design and build global sites. Configure global network services and site local network services. Configure global device credentials. Design global IP address pool and reserve the LAN Automation pool in the specific site.
- 3. Discover: Discover primary device.
- 4. **Provision**: This steps consists of two sub-steps: Start LAN Automation: Push temporary configuration to the primary device, discover new network devices, upgrade the IOS- image and push initial config to the new discovered device, Stop LAN Automation: Convert all point-to-point links to Layer 3 routed interfaces.

## Planning

LAN Automation planning is the initial step in four step workflow to sucessfully build underlay network. There are multiple aspects that must be considered during the initial planning phase to ensure LAN Automation support matrix aligns the targeted underlay network environment. Ensure all required planning steps are verified before proceeding to next step in the workflow

- 2. Supported switches.
- 3. Site Planning.
- 4. IP Pool Planning.
- **5.** Site specific CLI/SNMP credentials.
- 6. Configuration on primary device.
- 7. New Switch (PNP-agent) initial state

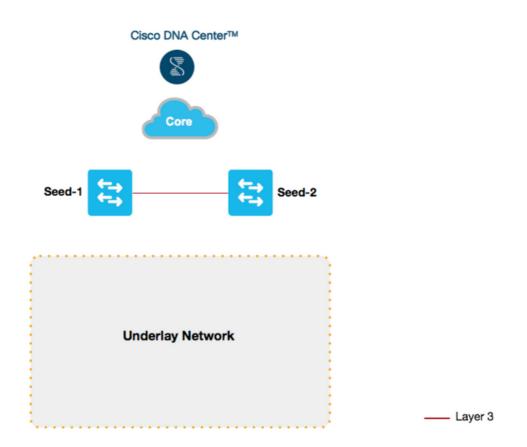
#### **Understanding system roles**

#### **Primary Device**

The primary device is a pre-deployed network device in the network and is the initial point through which Cisco LAN Automation can discover and on-board new switches downstream. The primary device can be automated via technologies such as Cisco Plug-n-Play (PnP) and zero-touch-provisioning or manual configuration. Figure below shows the primary device network boundaries between Cisco DNA Center connection in IP core and the to be discovered underlay network using LAN Automation.

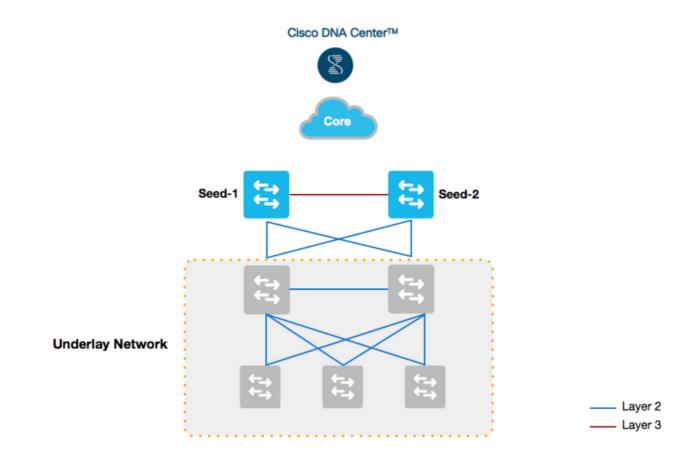
**Note**: The peer device can be automated via LAN Automation as well. Only one seed device is necessary.

Figure 1 - Seed device role



#### **PnP-Agent Device**

The PnP-Agent is a Cisco Catalyst switch with factory-default settings. The switch leverages builtin day-0 mechanism to communicate with Cisco DNA Center that supports integrated PnP server function. Cisco DNA Center dynamically builds PnP profile and configuration sets that enables complete day-0 automation. Figure below shows PnP-Agent physical connection to the primary device.



#### Automation Boundary

In genereal, Cisco recommends building structured and hierarchial network designs in enterprise networks providing scalability and redundancy at every network tier. While the 3-tier architecture is proven in large scale enterprise campus networks, the network design in enterprise may vary broadly based on overall network size, physical connection, and more. The network admin must determine the physical topology that needs to be automated using Cisco LAN Automation as part of initial planning.

The Cisco LAN Automation in Cisco DNA Center supports maximim of two hop-count from initial automation boundary point device. In other words, to build the underlay network using Cisco LAN Automation up to access layer the network administrator must start the automation boundary from core or distribution layer. Any additional network devices beyond two hop counts may get discovered but cannot be automated using LAN Automation.

LAN Automation will initiate only on directly connected neighbors. Consider two scenarios:

- User has a three tier network and wants to Lan automate distribution and access layer switches. Since distibution layer switches, which are directly conneted to seed are participating in Lan automation, both distribution and access layer switches will be discovered and Lan automated
- 2. User has a three tier network and wants to Lan automate distribution and access layer switches. User has already lan automated distribution layer and later adds access layer switches to network and wishes to Lan automate them. In this case, since distribution switches are already lan automated and links converted to Layer 3, Tier 1 switches cannot be used as seed. User has to select distribution as seed in this scenario.

Figure below shows the automation boundary supported by Cisco LAN Automation.

Figure 3 - LAN Automation boundary support

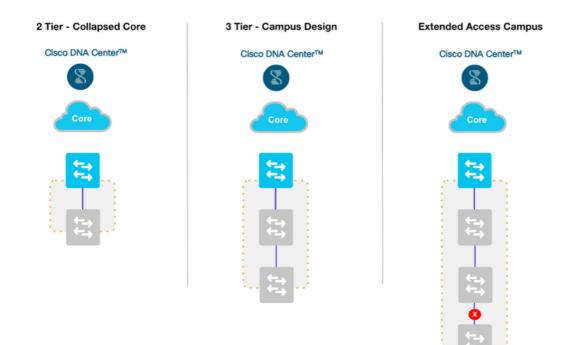
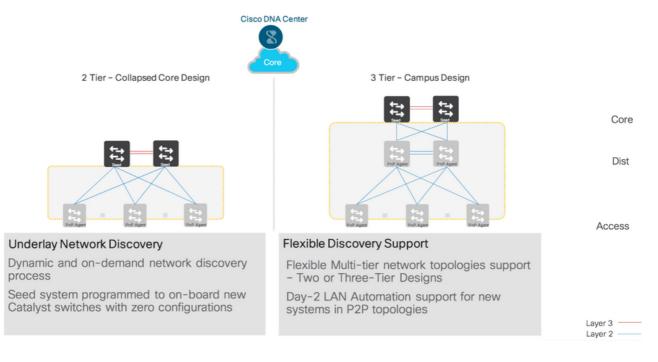
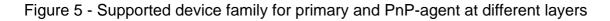
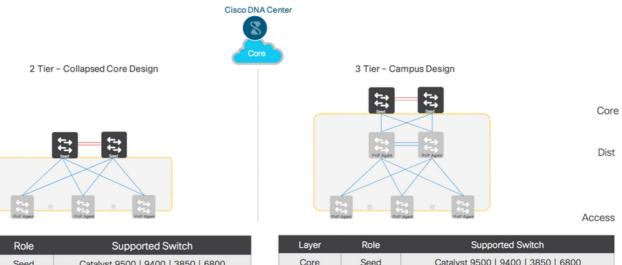


Figure 4 - Tier-2 and Tier-3 network design



### Supported switches for each role at different layers





	Layer	Role	Supported Switch
D	istribution	Seed	Catalyst 9500   9400   3850   6800
	Access	PnP Agent	Catalyst 9400   9300   4500E   3850   3650

Layer	Role	Supported Switch
Core	Seed	Catalyst 9500   9400   3850   6800
Distribution	PnP Agent	Catalyst 9000   4500E   3850   3650
Access	PnP Agent	Catalyst 9400   9300   4500E   3850   3650

#### Cisco LAN Automation product support matrix

Note: 9500H (high perfromance skus: C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C) as seed and PNP-Agent are currently not supported on 1.2.x release. Support is coming in DNA Center 1.3 and IOS 16.11.1.

Role	Product Model	Network Module <sup>1</sup>	IOS versi on	DNA Cente r
Seed PnP-Agent	C9500-32C C9500- 32QC C9500-24Y4C C9500- 48Y4C		16.11. x onwar ds	1.3 onwar ds
Seed PnP-Agent	C9500-12Q C9500-24Q C9500-40X C9500-16X	Any Front Panel Ports <sup>2</sup>		
Seed PnP-Agent	C9404R C9407R C9410R	Sup-1 <sup>3</sup> Sup-1XL <sup>3</sup> Sup-1XL-Y <sup>3</sup> Any Line Card		
Seed PnP-Agent	C9300-24T C9300-24P C9300-24U C9300-48T C9300-48P C9300-48P C9300-24UX C9300-24UX C9300-48UN C9300-48UN C9300-48UN	Any Uplinks and Modules Ports		
	C9200L-24P			1.2.8
Seed PnP-Agent	C9200L-48T	Any Uplinks and Modules Ports		onwar ds
	C9200L-48P			
		Sup6T		
Seed	C6807-XL	Any Uplinks and Modules Ports		
Seed	C6880-X C6880-X-LE	Any Uplink and Module Ports		
Seed	C6816-X-LE C6832-X-LE C6824-X-LE-40G C6840-X-LE-40G	Any Front Panel Ports		

Seed PnP-Agent	WS-C4503-E WS-C4506-E WS-C4507R+E WS-4510R+E	Sup9-E <sup>3</sup> Sup8-E Any Uplinks and Modules Ports
Seed PnP-Agent	WS-C3850-24T WS-C3850-24P WS-C3850-24P WS-C3850-24P WS-C3850-48F WS-C3850-24U WS-C3850-24U WS-C3850-24XU WS-C3850-12X48U WS-C3850-12X8 WS-C3850-24S WS-C3850-24XS WS-C3850-24XS	Any Uplinks and Modules Ports
Seed PnP-Agent	WS-C3650-24TS WS-C3650-24PS WS-C3650-24PS WS-C3650-24PS WS-C3650-24TD WS-C3650-24TD WS-C3650-24PD WS-C3650-24PD WS-C3650-24PD WS-C3650-24PD WS-C3650-24PD WS-C3650-248PD WS-C3650-248PQ WS-C3650-248PQ WS-C3650-248PQ WS-C3650-248PQ WS-C3650-248PQ WS-C3650-22X48UQ WS-C3650-12X48UR WS-C3650-12X48UR	Any Uplinks and Modules Ports

## <sup>1</sup>= Dedicated Management Port is unsupported in Cisco LAN Automation

## <sup>2</sup>= Breakout Cable is unsupported in Cisco LAN Automation

 $^{3}$ = 40G Uplink is supported from 16.11.1 onwards (Refer to miscellaneous section for more details on how to make 40G port work before and after 16.11.1)

#### Site Planning

Create the required building, floors and site using Design Application. Consider how the primary and peer device will be connected to the new devices.

e.g. whether they will all belong to same site or follow a hierarchy. Some other points to consider are how the IP pools will be shared across different sites/buildings or floors. One option is to have a pool specific to a site. Other option is to share a common LAN pool for all the sites in the hierarchy. Also if the devices are being on-boarded across multiple lan automation session, ensure that required IP pools will be available across the various sites in the hierarchy.

#### Note:

LAN Automation in 1.1.x release allows for only one site selection for primary, peer and pnp devices meaning all devices should belong to a single site.

LAN Automation in 1.2.8 release will allow selection of one site for primary device, one for peer device and one for PNP-agents.

The IP pool will be selected based on the site chosen for PNP-agents. Once devices are provisioned, site can not be changed. So its recommended to complete LAN Automation prior to provisioning them.

#### **IP Pool Planning**

IP pools for LAN Automation are created by first creating a global pool in Cisco DNA Center followed by site specific LAN IP Pool. LAN Automation takes site specific LAN IP pool. This pool is internally used for following allocations:

1. One part of the pool is reserved for a temporary DHCP server. The size of this pool depends on the size of the parent LAN pool. For example: If the

parent pool is 192.168.10.0/24 then a sub-pool of size /26 is allocated for dhcp server. If the pool size is bigger than /24 then algorithm keep increasing the size of DHCP pool upto a maximum of a /23 sub-pool (512 IPs). So /24 pool will reserve 64 IP addresses, /23 pool will reserve 128, /22 will reserve 256 and anything bigger will reserve 512 IPs for the DHCP server. The minimum pool size to start LAN automation is /25 that will reserve /27 or 32 IP addresses for DHCP pool. This IP pool is temporarily reserved only for the duration of LAN Automation discovery session. Once the LAN Automation discovery session is stopped and completed, the DHCP pool is released and these IP addresses are returned back to the LAN pool. Since the DHCP pool is usually the biggest contiguous chunk of IP addresses required, the pool should have at-least one such chunk available. If the pool is too fragmented then it may not be able to allocate DHCP pool and LAN automation session will terminate with IP Pool allocation error.

- 2. Second part of IP pool is used for link configuration between connected devices participating in discovery session. Participating devices are primary device, peer device and discovered devices in the discovery session. All links between these devices are configured with layer 3 configuration required for ISIS routing. Only exception are the links connected to primary seed device that are not selected while starting discovery. These could be links between the primary and peer devices or links between primary and discovered devices. For every LAN Automation configured link a /31 subnet is allocated. So for e.g. in the topology containing 4 links, LAN automation will allocate 8 IP addresses for the point to point layer 3 link configuration. Note: Before release 1.3.0, we were using /30 subnets for the point to point link between the networ devices LAN Automation configures.
- 3. Third part of IP Pool is used to allocate single Loopback IP per discovered device. If the primary or peer devices do not have Loopback IPs configured then they are also configured with the Loopback IP addresses. Internally the IP Address Manager (IPAM) library allocates /27 pool for allocation of single IP addresses. So for example, when first Loopback IP address for a device is requested from the LAN pool, IPAM library allocates /27 (32 IPs) pool and returns one IP from this pool. On subsequent requests it will continue to give IP addresses from previously allocated /27 pool untill it runs out of IP address. So for a /27 IP, same internal pool will be used for 30 IP allocation. Currently only 30 of the 32 IP addresses in the internal pool can be used for Loopbacks. If the internal pool can no longer be used for IP allocation then another /27 pool is allocated for further single IP allocation. So in this case Loopback allocation for 31st discovered device will result in a new /27 sub-pool allocation.

#### IP pool usage example:

- Say you want to LAN Automate 10 devices using the same pool with each device having one link to primary seed and another one going to secondary.
- Consider a 192.168.199.0/24 pool. When LAN Automation is intialted a /26 pool will be reserved for the DHCP addresses. So 192.168.199.1 to 192.168.199.63 is reserved and assigned to Vlan 1 for the 10 devices.
- Next, a /30 pool for each of the point to point link will be reseved and a /27 is reserved for Loopback addresses. Since there are 10 devices with two links each, a total of 2\*10\*4 = 80 IP addresses will be reseved for point to point link and 10 Loopback addresses will be reserved.
- So in total, 100 IP addresses will be reserved for these 10 devices: 10 for each vlan1, 10 for each Loopback, and 80 for the point to point link between devices and seeds
- Once LAN Automation is stopped, the VIan 1 IP addresses are released back to the pool and a total of 90 addresses are allocated for the LAN Automation session.

#### Note:

Same IP pool can be used for multiple discovery sessions. For example user can run one discovery session and discover first set of devices. After the completion of this discovery session user can again provide the same IP pool for subsequent LAN Automation session. Similarly, user can choose one LAN pool for one discovery session and another LAN pool for second discovery session.

Everytime you start Lan auto, it will check for 64 free IP addresses in the IP pool. So, if you decide to do Lan automation multiple times with the same pool, best practice is to use at least /24 pool. If you plan to Lan automate only once for the IP pool, /25 will suffice

Don't use address pool that is being used elsewhere in the network such as address pool belonging to loopback or other addresses configured on the device.

#### Site specific CLI/SNMP configuration

Site specific CLI and SNMP v2 read/write or SNMP v3 configuration is required for starting LAN Automation. This configuration is done in Design application. This configuration selection should be selected and saved for the site that is used for LAN Automation. Usually if the credentials are configured at global level

they are visible at the site level. It requires explicit selection in radio box for the specific site and subsequent save to make them available for LAN automation app.

#### Configuration on seed device(s)

- Ensure system mtu 9100
- IP routing should be turned on the seed devices
- Routing between the seed service and DNAC should be setup so that DNAC has IP reachability to the LAN IP Pool Subnet
- The seed-device interface which is connected to the PNP-agent must not have an IP address configured. In most cases they should have the default configuration. This can be achieved by issuing the "default interface <interface>" command and performing an inventory resync.
- LAN Automation will work only when ports are L2. For cat6k and 9500H, ports are L3 by default. Convert them to L2 and re-sync the device before starting LAN Automation
- · Device credentials and SNMP credentials should be configured on the seed devices
- If the seed devices has L3 interfaces configured, it should not clash with any of the ip pools provided in DNAC
- Seed device should not have any other interfaces connected to some other DHCP server running in VLAN 1
- If loopback is not configured on the seed devices, then lan automation will configure it on the seed
- If any configuration changes are done on seed device prior to running LAN automation it should be synced in inventory service
- Seed device should be assigned a site. It's not required to provision the seed device for LAN automation.

#### Additional recommended configuration on seed device(s)

• <u>Running multiple discovery sessions for devices across sites connected to same seed</u>: In the scenario where the user plans to run multiple discovery sessions to on-board devices across different building and floors connected to same seed devices, it's recommend to block the ports for PNP-agents that are not participating in the upcoming discovery session.

Example: Seed devices(s) are in building-23 and are connected to PNP-agents on Floor-1 and Floor-2. Floor-1 devices are connected on interfaces Gig 1/0/10 through Gig 1/0/15 and Floor-2 devices are connected to interfaces Gig 1/0/16 through Gig 1/0/20. For the discovery session on Floor-1 its recommended to shutdown ports connected to Gig 1/0/16 to Gig 1/0/20. Otherwise the PNP-agents connected to Floor-2 may also get DHCP IPs from server running on primary seed device. Since these interfaces will not be chosen for discovery session, they will remain as stale entries in PNP database. Now when the discovery session is run for Floor-2 later, the discovery wont work properly until these devices are deleted from PNP app and write erase/reloaded. So shutting down other discovery interfaces help in avoiding these unnecessary steps

 <u>Endpoint/client integration</u>: Similarly, if there are clients connected to a switch that is being discovered, those clients will also contend for DHCP IP and may exahust the pool causinglan auto to fail. Its recemmended to connect client after Lan automation is completed.
 Note: Starting 1.2.10, above endpoint/client integration restriction is removed. Clients can be left connected while switch is undergoing Lan Automation

#### **PNP-agent initial state**

- Ensure the device to be lan automated is running DNA ADVANTAGE license level. Else some of the commands will not get pushed
- PNP-agents fresh out of the box will have factory defaults and will be ready to start Lan automation
- If reusing network device(s) that were already in use for testing and/or in the network, please ensure the following:
   PNP-agents should have the required license that can push the LISP, ISIS routing, and CTS related CLIs. Use "show license" command to see the current license level and upgrade the license if needed.
  - PNP-agents should be in clean state meaning that they should not have stale certificate, keys etc. from previous runs.
  - Bring the device to factory defaults by clearing the following from the swicth console

[CLI config mode] pnpa service reset or alternatively (if above CLI is not supported): [CLI config mode] no pnp profile pnp-zero-touch no crypto pki certificate pool Also remove any other crypto certs shown by "show run I inc crypto" crypto key zeroize config-register 0x2102 or 0x0102 (if not already)

no system ignore startupconfig switch all

no boot manual

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 delete flash:vlan.dat write erase reload (enter no if asked to save)

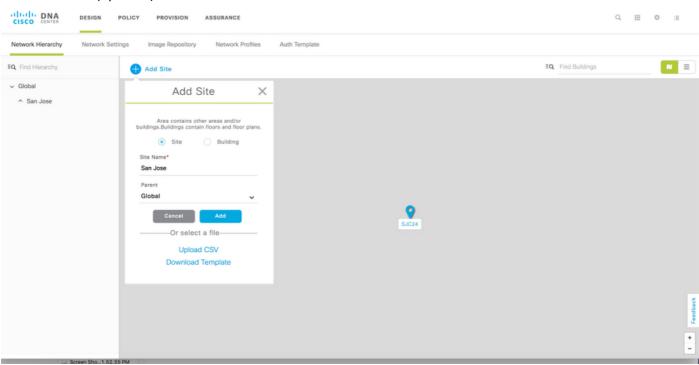
## <u>Design</u>

- **1.** Design and build global sites.
- 2. Configure global network services and site local network services.
- **3.** Configure global device credentials.
- 4. Design global IP address pool and assign Lan automation pool for the required site from the global pool

CISCO CENTER ⊿22 Q III ¢ III What can DNA Center do? Take a Tour Need to add functionality to DNA Center? Add applic Want to learn more about DNA Center? Watch video Policy Design Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud. ate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced · Add site locations on the network ork as Virtual Net te golden images for dev roups to describe your crit less profiles of SSIDs in policies to meet your policy goals Provision Assurance active monitoring and insights from the network, devices, and applications to predict problems faster and ensure that nd configuration changes achieve the business intent and the user experience you want. Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and on WLCs and APs to defin Set up Campus Fabric across switches

#### Navigate to Design -> Network Hierarchy

- Add Site
- · Add building
- Add floors (optional)



- Enter CLI credentials by clicking on ADD button on right hand side
- Enter SNMP credentials by first clicking on SNMPV2C Read and then clicking on SNMPV2C Write

Note: Click at the Global level if you want to have all sites to have same device credentials

#### Note: Do not use "cisco" as username

Note: Enable Password is mandatory for now. This is being addresed by CSCvm15743 after which enable password will not be mandatory

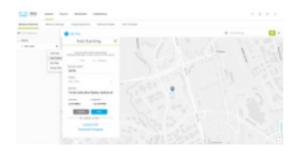
CISCO CENTER DESIGN	POLICY PROVISION ASSURANCE				Q Ⅲ ¢ Ⅲ
Network Hierarchy Network Set	ttings Image Repository Network Profil	es Auth Template			
EQ Find Hierarchy	Network Device Credentials IP	Address Pools SP Profiles	Wireless		
✓ Global					$\frown$
✓ San Jose	CLI Credentials				( 🕂 Add
∧ SJC24	Name / Description	Username	Password	Enable Password	Actions
	0	admindna	*****		Edit   Delete
	SNMP Credentials		SNMPV2C Read   SNMPV2C Write	I SNMPV3	🕂 Add
	Name / Description		Read Community		Actions
	O SNMPv2 RO				Edit   Delete
	HTTP(S) Credentials		HTTP(S) Read   HTTP(S) V	Nrite	🕂 Add
	Name / Description	Username	Password	Port	Actions
				Res	et Save

#### Navigate to Design -> Network Settings -> IP Address Pools

• Under Global create a dedicated IP Address Pool that will be used for Underlay Infrastructure

Note: Don't use address pool that is being used elsewhere in the network such as address pool belonging to loopback or other addresses configured on the device.

CISCO CENTER DESIGN P	POLICY PROVISION ASSU		Add IP Pool	×			Q Ⅲ Φ	
Network Hierarchy Network Settin	ngs Image Repository N	IP Pool Name *						
EQ. Find Hierarchy	Network Device Creden	Underlay_Automation						
<ul> <li>Global</li> <li>San Jose</li> </ul>		IP Subnet * 192.168.199.0						
A Sen Jose	IP Address Pools	CIDR Prefix /24 (255.255.255.0)		~	Last Updated: 15:35:27	📿 Refresh  🖄 Im	port 🛛 😁 Add IP	Pool
	Y Filter Name • IP S	Gateway IP Address * 192.168.199.1			Free Count	Overlapping	Actions	
	LAN_Automation 192	DHCP Server(s)		÷	0 of 256	No	Edit   Delete	
		DNS Server(s)		~				
		Overlapping						
			Cancel Save					
								Eaethack



#### Next Navigate to DNAC $\rightarrow$ Design $\rightarrow$ Network Settings $\rightarrow$ Site $\rightarrow$ Click the Reserve IP Pool

CISCO CENTER DESIGN	POLICY PROVISION ASSU	Reserve IP Pool ×	Q Ⅲ ♥ Ⅲ
		IP Pool Name * LAN_pool_SJC24  Type LAN	Lest Updated: 15:59:04 C Refresh Reserve IP Pool Overlapping Inherited from Actions I
100			

#### • Reserve IP pool at site level. Ensure to select LAN under "type" field

## **Discover**

Before creating a Discovery profile and running it, please take a moment to look at the underlay configuration of the seed device. Refer to pre-requisites for seed configuration

Navigate to Discovery by selecting the "boxes matrix" icon in top right corner of DNAC, and select the Discovery tool. Alternatively, scroll to the bottom of DNA Center home page and click on Discovery under Tools section

- Click on New Discovery and fill in the following details
  - Discovery Name

- IP Address (The IP address could be any L3 interface or Loopback on any switch that DNA Center can access. You can provide a range of IP

address as well especially if you are discovering primary and peer seed together)

- Credentials (Enable the CLI and SNMP credentials that you created in Step1)
- Advanced Choose SSH and/or Telnet (ensure the seed is configured for ssh)
- Click on Start. Once the discovery starts, the page will present the discovery settings and details.

CISCO DNA	Discovery	_@ Q ∐ 0 ≡
Eq. + Search by Decovered Device	Test test a report	Add Credentials xxxxx xxxxx xxxxx xxxxx xxxxx xxxxx xxxx
<ul> <li>E00_E00 ( reason term or no exect</li></ul>	V # Alexand Mage Market States Market States Mar	Confron Presservit Confron Presservit Confron Charlos Presservit Confron Ch
	SMEV2 Meeters to distry	
Device Controllability is Enabled. Les	n Nov	Reset

• Discovery will take some time. Once done, it will show completed. Ensure there are no failures

CISCO CENTER					Discovery							<b>22</b> Q	L 111	¢		
EQ - Search by Discovered Device	9500_Border	⊘ Completed	4 Reachable Device	es 00h:00r	n:21s									Hist	tory 🗸	
O Seed_Discovery   3 Reachable D CDP 192.168.210.1				DEVICE STATU	is v			Filter	Device Name	Status	ICMP .	SAMP	CLI H	(TTP(S)	NETCONF	
O 9500_Border   4 Reschable Devices CDP 192.158.210.1								192.168.210.1	AEAA barder ele					•	•	
9300_Edge   4 Reachable Devices			4		Success(4)			192.168.199.9	9500_border- 6.cisco.com					0		
CDP 192.168.199.97			Devices		Discarded(0)			192.168.199.9	9300_Edge- 5.cisco.com					0		
								192.168.199.90	3850_Edge_3.cl sco.com					•		7
	Discovery D	etails														Make a Wish
	CDP Level	5				LLDP Level	None									Make
	Protocol Order	ssh telnet				Retry Count	3									Ì
	Timeout	5 second(s)				IP Range	192.168.210.1									
	IP Filter List	None				Preferred Management IP	Use LoopBack	Show 25		Showing 1	to 4 of 4	4	Page	1 -	of 1	
	CLI Credentials	admindna				SNMPv2c READ	SNMPv2 RO									
	SNMPv2c WRITE	SNMPv2 RW				SNMPv3	None	⊘ success	O UNREACHABLE	🛞 FAIL	une 🔘	) NOT THE	0 0	UNAVALAB	48	
	HTTP(S) READ	None				HTTP(S) WRITE	None									
	NETCONF	None														
Device Controllability is Enabled. Lea	rn More								Delet	e Clor	ne 🚺	Edit		St	tart	

• Next, navigate to inventory page and verify the discovered device was added. When you enter the Device Inventory page all the devices should have

the "Device Status" set as "Reachable" and "Last Inventory Collection Status" as "Managed

CISCO CENTER			Inve	ntory			Q Ⅲ Φ Ⅲ
				Last update	d: 6:00 pm 📿 Refresh	import 🖞 Export Credentials	🖞 Export Data 🕂 Add
<b>Filter</b> Actions ~							EQ Find
Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Resync Interval	Last Inventory Collection Status	Location :
3850_edge_2 C	192.168.199.98	Reachable	2 days, 2:47:30.96	9 minutes ago	00:25:00	Managed	SJC24-1
9300_Edge_1 2*	192.168.199.97	Reachable	5 days, 0:56:19.91	a minute ago	00:25:00	Managed	SJC24-1
9500_border.ciscodna C	192.168.210.1	Reachable	13 days, 0:29:03.29	6 minutes ago	00:25:00	Managed	SJC24-1
Show 10 entries			St	nowing 1 - 3 of 3			Previous 1 Next

• Once in Managed state, add the discovered seed to the same site. Navigate to Provision -> Devices -> Inventory. Select the device and under Actions, click on "Assign Device to Site"

Note: For DNA Center 1.2.6 and earlier, ensure that both the primary and peer seed are in the same site and same floor (although they can be physically on different floors)

aha) cisco	CENT	A DESIGN	POLICY	PROVISION	ASSURANCE							_@	Q Ⅲ ¢	≎ ∷
Inventor	y (4)	Unclaimed De	víces											
Select	device(s	i) to assign to a Si	te and Provisi	on network settings	from the Network Hie	rarchy.								$\times$
									Network Telem	etry 🖞 Upgr	ade Readiness	🖬 Update	e Status 📿 I	Refresh
7 Filter		actions ~	Selected	LAN Automation	·									
	Devic	Assign Device	to Site	IP Address	Site	Serial Number	Uptime	OS Version	OS Image \\	Last Sync Status	Credential Status ()	Last Provisioned Time	Provision Status	I
	3850_	Update OS Ima Resync	90 s S	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	46 days, 9:17:29.06	16.6.2	packages.conf Tag Golden	Managed	Not Provisioned	Oct 01 2018 13:20:02	Success See Details	
	9300_	Delete Device	5	192.168.199.97	SJC24/SJC24-1	FCW2214L053, FCW2224C122, FOC2224Q0UE, FCW2224C123	18 days, 18:06:07.33	16.6.4s	CAT9K[16.6.4s	Managed	Not Provisioned	Oct 01 2018 13:19:58	Success See Details	
	9500_b 6.cisco.		Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	4 days, 18:00:05.68	16.6.4s	packages.conf Tag Golden	Managed	Not Provisioned	Oct 05 2018 14:34:09	Success See Details	
	9500_b	order.cisco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FCW2205A33L	46 days, 9:22:42.01	16.6.4	cat9k_iosxe.1 Tag Golden	Managed	Not Provisioned	Oct 01 2018 13:16:25	Success See Details	

#### • On next page, select the site and click Apply

CISCO CENTER DE	ESIGN POLICY PROVISIO		Q Ⅲ Φ Ⅱ
Devices Fabric			
Assign Device to	o Site		
			Close
Serial Number FCW2205A33L	Devices 9500_border.ciscodna	Choose a site JC24/SJC24-1 × V	
		Global/San Jose	
		Global/San Jose/SJC24	
		an Jose/SJC24/SJC24-1	

CISCO CENTER ASSURANCE 🖉 Q 🏢 🔅 DESIGN POLICY PROVISIO Device Inventory Inventory (4) Unclaimed Devices O Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.

								Network Teleme	try 🖄 Upgra	de Readiness	🖬 Update	Status 📿	Refresh
7 Filte	r Actions - O LA	N Automation	~										
	Device Name 🔺	Device Family	IP Address	Site	Serial Number	Uptime	OS Version	OS Image 🕕	Last Sync Status	Credential Status	Last Provisioned Time	Provision Status	I
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	46 days, 9:17:29.06	16.6.2	packages.conf Tag Golden	Managed	Not Provisioned	Oct 01 2018 13:20:02	Success See Details	
	9300_Edge-5.cisco.com	Switches and Hubs	192.168.199.97	SJC24/SJC24-1	FCW2214L0S3, FCW2224C122, FOC2224Q0UE, FCW2224C123	18 days, 18:06:07.33	16.6.45	CAT9K[16.6.4s	Managed	Not Provisioned	Oct 01 2018 13:19:58	Success See Details	
	9500_border- 6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	4 days, 18:00:05.68	16.6.4s	packages.conf Tag Golden	Managed	Not Provisioned	Oct 05 2018 14:34:09	Success See Details	
	9500_border.clsco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FCW2205A33L	46 days, 9:22:42.01	16.6.4	cat9k_iosxe.1 Tag Golden	Managed	Not Provisioned	Oct 01 2018 13:16:25	Success See Details	

Make a Wish

• If you can't find the Site tab, click on the "three vertical dots" on right hand side, select Site and click Apply

evi	ce Inventory										
ento	vry (4) Unclaimed De	rvices									
lect	device(s) to assign to a Si	ite and Provisio	on network settings I	from the Network Hier	rarchy.						×
								Network Teler	metry ÖUpgra	de Readiness	s 📑 Update Status 📿 Refres
Filte	Actions V O LA	N Automation	~								
]	Device Name 🔺	Device Family	IP Address	Site	Serial Number	Uptime	OS Version	OS Image 0	Last Sync Status	Credential Status ()	Last Provision Provisioned Status
]	Device Name		IP Address 192.168.199.98	Site	Serial Number FCW2133F05W, FOC2052X0C9, FCW2020F0A0	<b>Uptime</b> 46 days, 9:17:29.06		OS Image  packages.comf Tag Golden	Status V Dev		Provisioned Provision
		Family			FCW2133F05W, F0C2052X0C9,	46 days,	Version	packages.conf	Status V Dev	Status () ice Name ice Family ddress form	Provisioned Provision II Time Status
	3850_Edge_3.clsco.com	Family Switches and Hubs Switches	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, FOC2052X0C9, FCW2020F0A0 FCW2214L0S3, FCW2224C122, FOC2224Q0UE,	46 days, 9:17:29.06 18 days,	Version 16.6.2	packages.conf Tag Golden	N Dev N Dev V IP A N Plat V Site	Status  Control Name Control Name Control Name Control Name Control Name Control Namber Control	Provisioned Provision : Time Credential Status Credential Status Last Provisioned Time Provision Status Device series

## Steps to consider before starting LAN auto

#### 1a) IP Pool Subnet reachability from DNAC

LAN automation discovery uses the LAN pool for reaching the PNP-agents. DNAC should be able to reach the IPs allocated from the LAN pool. For e.g. if the lan pool is 192.168.10.0, DNAC should have the correct route to reach this subnet. One way to test this is create a SVI on primary seed device and try ping test between DNAC and seed. For e.g.:

[On seed device] Switch(config)#interface vlan1 Switch(config-if)#ip address 192.168.99.1 255.255.255.0 Switch(config-if)#end [On DNAC CLI console] [Sat Jun 23 05:55:18 UTC] maglev@10.195.192.157 (maglev-master-1) ~ \$ ping 192.168.99.1 PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data. 64 bytes from 192.168.99.1: icmp\_seq=1 ttl=252 time=0.579 ms 64 bytes from 192.168.99.1: icmp\_seq=2 ttl=252 time=0.684 ms 64 bytes from 192.168.99.1: icmp\_seq=3 ttl=252 time=0.541 ms [On seed device] Switch(config)#default int vlan 1 Interface Vlan1 set to default configuration If the ping test doesn't succeed then it indicates that the route has not been setup correctly on DNAC.

#### **1b) Static Route addition for LAN Pool**

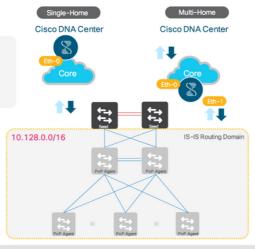
DNA Center hardware has multiple physical interfaces with each serving different categories of communication. Refer to 'Cisco Digital Network Architecture Center Appliance Installation Guide' for recommended interface connection, IP routing, and static assignment. In single-home design, DNA Center performs host function with default gateway providing IP routing. However, for multi-home design, the DNA Center must have static route to Lan automation network(s) via the enterrise facing interface.

Figure 6 - DNA Center IP addressing for single-home and multi-home designs

## DNA-C

Eth-0 Management Interface :

IP Address : <IP\_Address> Netmask : <Mask> Gateway : <Default\_Gateway>



#### DNA-C

Eth-0 Management Interface : IP Address : <IP\_Address\_1>

Gateway : <Default\_Gateway>

Eth-1 Interface :

Netmask : < Mask>

IP Address : <IP\_Address\_2> Netmask : <Mask> Gateway : <Skip> Static Route : <LAN\_Automation-Net>/<mask>/GW

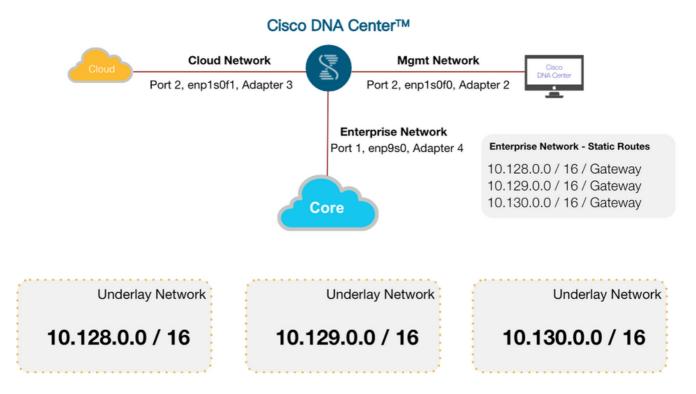
#### **DNA-CIP** Routing Configuration

DNA-C must have end-to-end IP reachability

In Single-Home design the DNA-C performs host function with Default Gateway providing IP routing.

In Multi-Home design, the DNA-C must have static route to LAN Automation network(s) via secondary interface.

## Figure 7 - DNA Center Static IP routing design



One way to fix the IP reachability issue is by adding a static route in DNAC in case of multi-home design. This can be done by network administrator during initial DNA Center configuration or later via maglev command (Don't use linux route command as maglev APIs don't pick the correct information if the route is modified using route command).

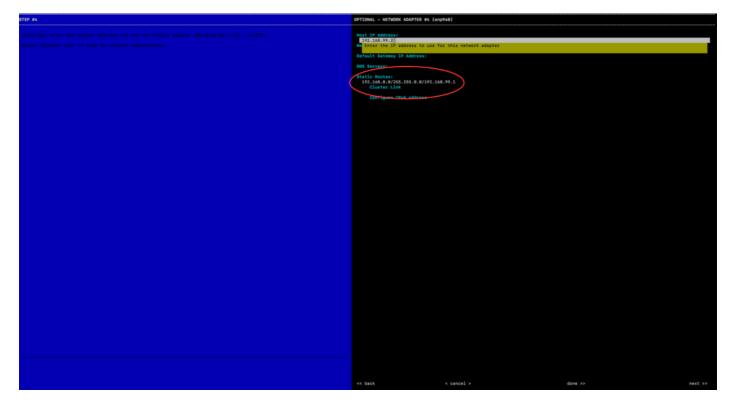
For single-home design, please check routing between the seed and DNAC.

Steps to add static route on DNAC:

1. Issue "sudo maglev-config update" from the DNAC console. The wizard will show up. 2. Enter the static route, then hit 'next' (Please ensure that correct interface is selected for adding the static route, otherwise use 'next' till it shows up the interface on which the route should be configured). 3. Wizard will validate and configure host networking 4. It will ask for Network Proxy where leave it blank. It will fail validating the proxy. Then it will have option to skip the proxy setting. 5. The wizard is ready. Hit 'proceed'

to apply the changed to controller. It may give some warning about starting services etc. This can be ignored. It takes about 5-6 minutes to add a static route.

Below is how the config wizard window looks like



#### 2) PNP-agent initial state before starting Lan auto

1. Ensure the PNP-agent is at "System Configuration Dialog" state before starting Lan auto.

Do not press yes or no. Leave the device at that state.

FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled cisco C9300-24T (X86) processor with 1418286K/6147K bytes of memory.
Processor board ID FCW2137G032
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address	: f8:7b:20:48:d8:80
Motherboard Assembly Num	ber : 73-17952-06
Motherboard Serial Number	: FOC21354B06
Model Revision Number	: A0
Motherboard Revision Numb	er : A0
Model Number	: C9300-24T
System Serial Number	: FCW2137G032

%INIT: waited 0 seconds for NVRAM to be available

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Note: If the device does not stop at this initial prompt and moves ahead, then check device config-register (use "show ver | inc register" cli). In some cases, the value might be 0x142. Change the config-register value to 0x102 or 0x2102 and save the config. Check the cli again and it will show "Configuration register is 0x142 (will be 0x102 at next reload)"

Note: If even after changing the value to 0x102 or 0x2102 and reloading the device, the device still comes up with older config-register, configure "no system ignore startupconfig switch all" on the device, save config and reload

#### 2. Stack considerations

- For a stack, follow the same, but in addition give extra time to ensure all memebrs in the stack are UP. Do not start Lan auto until all switches are UP
- Lan automation is always initiated on active switch. When all switches in a stack are booted together, the switch with lowest mac address (assuming no switch priority is configured) becomes the active, second lowest the standby and so on. Some customers have requirement that first switch should always be active. In this case if all switches are booted together and the first switch does not have the lowest mac addres, it will not become the active. To ensure first switch is the active, one should boot the switches in staggered manner i.e boot switch 1, after 120 seconds boot second switch, and so on. This will guarantee the order i.e switch 1 will be active, switch 2 will be standby and so on. However, upon reload this order will not be maintained and switches will get the role depending upon their mac address.
- If you want to ensure that switches maintian their order after reload, it's a good practice to assign switch priorities to ensure switches always come up
  in same order. Highest priority is 15. When priorities are assigned they take peference over the switch mac address. Assiging switch priorities doesn't
  change the NVRAM config. The values get written to ROMMON and will persist after reload/wr erase (Note: You may have to clean up the switch after
  configuring the priorities since some certificates will have been configured on the switch when they were booted. Refer to "PNP-agent initial state"
  section for the clean-up part)

3850\_edge\_2#switch 1 priority ? <1-15> Switch Priority 3850\_edge\_2#switch 1 priority 14 WARNING: Changing the switch priority may result in a configuration change for that switch. Do you want to continue?[y/n]? [yes]: y

Note: Starting Lan auto before the stack is fully up might cause problems

Note: If you are consoled into the standby/member switches, do not press enter there even though the screen says "console is now available, Press

RETURN to get started". Simply monitor the acrive switch which should be at the "System Configuration Dialog" state Note: If Lan auto is already running and you dont want to stop it, simply shut the seed link connecting to the PNP-agent, so no discovery will happen until you are ready and unshut the port

#### 3. Un-plug the management port

• PNP-agents should be directly connected to seed device(s). PNP-agent should not be connected to any other network (for e.g. Management Network) or any network that can provide DHCP through another server on VLAN 1

#### 4. Seed ports must be Layer 2

• Make sure the seed ports connected to the PNP-agents are layer 2 and defaulted. Example catalyst 6500 and 9500H ports are layer 3 by default

#### 5. Ensure port on primary seed connecting to the PNP-agent(s) is not STP blocking

#### 6. Device being discovered (PNP-agent) should not be present in Inventory

This step is applicable to devices that were at some point discovered or lan automated

- If the device(s) to be discovered in upcoming LAN automation session are already present in inventory, then they should be removed from invmtoery first
- Navigate to Inventory from the home page. Filter the device by the serial number and click on Actions->Delete. Note if the device was provisioned and added to fabric, then it first needs to be removed from fabric and unprovisioned before removing from inventory.

cits	ili. [	DNA ENTER			Inventory				∠20 Q Ⅲ	0 ::
								Last updated: 11:24 am 📿 Re	fresh 🖻 Import 📄 Export	🔂 Add
Y Filte	r	Actions ~ 1 Selected								
	Devic	Update Credentials	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status	Site	1
	3850,	Update Management IP	192.168.199.98	Reachable	47 days 10 hrs 22 mins	5 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
	9300,	Update Resync Interval Resync	192.168.199.97	Reachable	17 hrs 32 mins	23 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
	9500,	Delete	192.168.199.99	Reachable	5 days 18 hrs 59 mins	a few seconds ago	00:25:00	Managed	5J024/SJ024-1	
	9500,	Launch Command Runner	192.168.210.1	② Reachable	47 days 10 hrs 14 mins	17 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
Show 10	•	entries			Showing 1 -	4 of 4				on 1 10 1

#### 7. Device being discovered should (PNP-agent) not be present in PnP database

This step is applicable to devices that were at some point discovered or lan automated

- If the device(s) to be discovered in upcoming LAN automation session are already present in PNP application prior to running discovery, then they should be cleaned from PNP application. Otherwise the discovery for these devices will not work properly
- Navigate to Network Plug and Play at bottom of the home page. Click on Devices tab and then Unclaimed tab. Ensure the device (serial number) being discovered is not present under "Unclaimed"

CISCO CENTER			2	Q		¢ 🗉	
Dashboard Devices Workflows Settings							
All Devices Unclaimed Provisioned Errors							
Devices (0)			Last updated: 12:38 pm	⊖ Re	fresh	<b>•</b> A	bt
∑ Filter Claim Edit Delete				EQ Find			
Name A Serial Number	Product ID	Source	Last Contact			i	1
Devices will show up here	No data to display						Wieh

· If present, first console into the device and remove the pnp profile

[on PNP-agent] 3850\_edge\_2#show run | sec pnp-zero-touch pnp profile pnp-zero-touch transport https ipv4 192.168.99.2 port 443 3850\_edge\_2#conf t Enter configuration commands, one per line. End with CNTL/Z. 3850\_edge\_2(config)#no pnp profile pnp-zero-touch 3850\_edge\_2

• Next, delete that device from "Unclaimed" section shown above. To delete, check the box next to the device and click on "Delete"

#### 8. Ensure the PNP-agent is running DNA ADVANTAGE license level

#### 9. Ensure PNP-agent is in INSTALL mode for image upgarde to take place during Lan automation

- Image upgarde via Lan Automation happens in the background
- Once the device is disovered by PnP, DNA Center will first check whether any golden image is marked for the switch family (catalyst 9300 or 3850) of the discovered device. To check whether golden image is selected, go to Design -> Image repository
- If golden image is marked and the discovered device is not running the golden image, then Lan automation will first upgrade the discovered device to the golden image. If not, DNA Center will skip image upgrade and proceed to pushing initial device config.
- If intent is for Lan automation to upgarde the image on the discovered device, then ensure the device is running in **INSTALL mode**. Image upgrade via lan automation will not happen if the device is in BUNDLE mode.
- If device is in BUNDLE mode and user wants to still proceed with Lan automation, then remove the golden image for that particluar switch family under Design -> Image repository

## Provision

Provision is the final step in the lan automation process. It is divided into two stages

1. Device discovery and on-boarding (Starting Lan Automation):

Once Lan automation is initiated, it does three things

• Push loopback and isis configuration to primary and peer seed and temporary configuration such as DHCP and Vlan 1 to primary seed device that

enables it to discover and on-board the PNP-agent.

Discover new devices

• Upgrade image and push configuration to discovered devices

When user starts Lan automation, temporary configuration is pushed to primary seed device that enables it to discover and on-board the PNP-agent. Next, the PNP-agent image is upgraded and basic configuration such as loopback address, system MTU, ip routing etc. is pushed to the PNP-agent.

Note: The image on the PNP-agent is updated only if a golden image is marked for that switch type in SWIMS service

2. Interface configuration (Stopping Lan Automation):

Once Lan automation is stopped

- Discovery phase ends and all point-to-point links between the seed and discovered device and between the discovered device (max of two hops) are converted into Laver 3.
- All temporary DHCP and vlan 1 configuration on the seed and discovered device are removed and DHCP sub-pool is returned back to the lan auto pool

#### 1. Start Lan Automation

LAN automation asks for a selection of primary seed device, peer seed device, site selection for seed device, LAN IP pool selection and interface selection. There are some optional selection like device prefix, hostname CSV file, configurable ISIS password etc.

These are the interfaces on primary seed device that will participate in new device discovery and L3 configuration. The interfaces on seed devices provides a filter for directly connected PNPagents that can be on-boarded through LAN automation session. Let's take an example with four directly connected PNP-agents i.e. device-1 through Gig1/0/10, device-2 through Gig 1/0/11, device-3 through Gig 1/0/12 and device-4 through Gig 1/0/13. If the user selects Gig 1/0/11 and Gig 1/0/12 as part of discovery interfaces then LAN automation will only discover device-1 and device-2. If device-3 and device-4 also try to initiate PNP flow, they will be filtered out as they are connected through interfaces that are not selected during LAN automation session. This mechanism allows to restrict the discovery process.

The second usage for interface selection is for selecting interfaces between primary seed and peer seed that should be configured with L3 link configuration. If there are multiple interfaces between primary and peer seed, user can choose to configure any set of these interfaces for L3 link configuration. If no interfaces are chosen then they will not be configured with L3 link configuration.

There is no option for peer seed interface selection. The interfaces between peer seed and PNPagents are automatically inferred based on topology information gathered from the device. The topology information is built on CDP information available on device. site Selection:

Sites can be selected for seed devices and PNP-agents. Currently there is one site for seed device(s) and one site for PNP-agents. In future releases, primary and peer seed can be on different sites.

LAN Pool Selection:

Lan pool is selected based on PNP-agent site information. One LAN pool from the list of LAN pools available for a particular site can be chosen for starting LAN automation. Same LAN pool can be chosen for multiple LAN Automation sessions. For e.g. user can run one discovery session and discover first set of devices. After the completion of this discovery session user can again provide the same IP pool for subsequent LAN Automation session. Similarly user can choose one LAN pool for one discovery session and another LAN pool for second discovery session. It is important to choose a LAN pool with enough remaining capacity.

• If entering a value, user should enter the same password that is configured on the seed. If user enters a value that is different than the password

configured on primary and peer seed, then an error is thrown.

• If password on primary and peer seed don't match, an error is thrown

Case1: User enters value in the ISIS password field

1a. If primary seed has ISIS password configured, then LAN Automation will configure the primary seed's ISIS password on the PnP devices (and peer seed if it did not have the password already)

1b. If primary seed doesn't have ISIS password but the peer has, then LAN Automation will configure the peer seed's ISIS password on the PnP devices and the primary seed

1c. If primary and peer seed don't have ISIS password configured and user enters a value in the password field, then LAN automation will configure user entered password on the PnP devices as well as primary and peer seed

#### Case2: User leaves ISIS password field blank

2a. If primary seed has an ISIS password configured, then LAN Automation will configure primary seed's ISIS password on the PnP devices (and peer seed if it did not have the password already)

2b. If primary seed doesn't have an ISIS password but peer has, then LAN Automation will configure peer seed's ISIS password on the PnP devices as well as the primary seed

2c. If the primary and peer seed don't have an ISIS password configured, then LAN Automation will use the default value "cisco" for the PnP devices and both the seeds

#### **Hostname Mapping:**

- Default: If no value is entered, Lan automation will set hostname as Switch followed by loopback address. Example: Switch-192-168-199-100
- Device Name Prefix: Device prefix is used for generating the hostnames for discovered devices. LAN automation keeps site counter and generates the name using prefix and current site counter for e.g. if the device prefix is Building-23-First-Floor then LAN automation will generate device names like Building-23-First-Floor -1, Building-23-First-Floor-2 etc.
- Hostname Map file format: DNA Center expects a CSV file with the hostname and serial number (hostname,serial number) as shown in the following example. For stack LAN Automation, the CSV file allows you to enter one host name and multiple serial numbers per row. The serial numbers need to be separated by commas

A	В
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

Navigate to Provision  $\rightarrow$  Devices and click the 'Lan Automation' Icon

cisc	O CENTER DESIG	N POLICY	PROVISION	ASSURANCE							_22	୦. ⊞	¢	
Device	s Fabric													
Devi	ce Inventory													
Inventory (4) Unclaimed Devices														
Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.														
								Network Telem	etry ÖUpgr	ade Readiness	📰 Update	Status	C Refres	sh
Filte	er Actions ~ 0 L	AN Automation ~						Network Telem	etry ÖUpgra	ade Readiness	E Update	Status	C Refres	sh
7 Filte	Device Name A	AN Automation ~ LAN Automation LAN Auto Status	ddress	Site	Serial Number	Uptime	OS Version	Network Telem OS Image 0	etry ÖUpgr Last Sync Status	Credential Status	Last Provisioned Time	Provision Status		sh
Filte		LAN Automation	ddress 12.168.199.98	Site SJC24/SJC24-1	Serial Number FCW2133F05W, FCC2052X0C9, FCW2020F0A0	Uptime 46 days, 13:33:10.65			Last Sync	Credential	Last Provisioned	Provision	I	sh

Next, fill in the values explained above and click start

cisco	DNA DESIGN	POLICY PROV	ISION ASSURAN	CE								20 Q		0	
Devices	Fabric						L	LAN Automation							×
Devic	e Inventory (4) Unclaimed Devices						5	Seed Device Say* Global/San Jose/SJC24/SJC24-1				~			
Select d	evice(s) to assign to a Site and	d Provision network a	settings from the Netwo	ork Hierarchy.				Primary Device* 9500_border.cisco.com		Peer Dev ↓ 9500	ica _border-6.cisco.com				~
								Choose Primary Device Ports*							
₹ Filter	Actions v   LAN Act	tomation v	IP Address	Site	Serial Number	Upt		GI0/0 GI0/0 FortyGigabiEthemet1/0/2 FortyGigabiEthemet1/0/4		- Fort	GigabitEthemet1/0/1 GigabitEthemet1/0/3 GigabitEthemet1/0/5				
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FGW2133F05W, FDC2052X0C9, FGW2020F0A0	45 d 13:3	D	Discovered Device Configuration							
	9300_Edge-5.cisco.com	Switches and Hubs	192.168.199.97	SJC24/SJC24-1	FCW2214L053, FCW2224C122, F0C2224Q0UE, FCW2224C123	18 d 22.0	4	Globel/San Jose/SJC24/SJC24-1							
	9500_border-6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	4 da 22.0		P Pool* LAN_Auto   192.168.199.0/24							
	9500_border.clsco.com	Switches and Hubs	192.168.210.1	5JC24/5JC24-1	F0W2205A33L	46 d 13:3		5/S Password							
						1 to 4 of	1	Hostname Mapping Device Name Prefix 9300_Edget Hostname Map File					~	Upload I	File
									Clear All	Cancel	Start				

Once LAN automation is started, click on Lan Automation Status to see the progress

CISCO EXAMPLE DESIGN POLICY PROVISION ASSURANCE	∠30 q ⊞ ¢ ≋
Devices Fabric LAN Automation Status	×
Device Inventory	⊖ Refresh
Inventory (3) Unclaimed Devices Logs Devices	
Discovered Stree: SJC24-1 IP Pool: LAN_Auto   192	2.168.199.0/24
Device Prefix: 9300_Edge Primary Device: 9500_border.cis Peer Device: none	
Bierery Device Interfaces: Fonyotpestine Status: Initialized	emet//0/1
V Filter Actions V D LAN Automation V Discovered Devices:	
Device Name      Device Family     IP Address     Site     Serial Number     Uptime     //CV2133/GOW, /OC2052000,	<b>F</b>
3990_1008_3.0000.001     Switches and Hubs     192.196.193.08	
Stopp_border=6-cloco.com     Switches and Hubs     192.168.199.99    SUC24/SUC24-1     FCW2228A4LS     5 days, 0-	
9500_border.clsco.com     Switches and Hubs     192.168.210.1	
1 to 3 of	
Once LAN Automation is started, below sample configuration gets pushed to the seed device(s)     Primary Seed Configuration	Secondary Seed Configuration
lexec: enable	
!	
system mtu 9100	
	lexec: enable
ip multicast-routing	!
ip pim ssm default	system mtu 9100
Loopback IP and ISIS Configuration (If secondary seed is configured, it is also gets configured with loopback ip and isis config)	ip multicast-routing ip pim ssm default !
interfeces Leonhack0	interface Loopback0
interface Loopback0 ip address 10.4.210.123 255.255.255.255	ip address 10.4.210.124 255.255.2 description Fabric Node Router ID
description Fabric Node Router ID	
	router isis
router isis	net 49.0000.0100.0421.0124.00
net 49.0000.0100.0421.0123.00	domain-password *
domain-password *	ispf level-1-2
ispf level-1-2	metric-style wide
metric-style wide	nsf ietf
nsf ietf	log-adjacency-changes
log-adjacency-changes	bfd all-interfaces
bfd all-interfaces	passive-interface Loopback0
passive-interface Loopback0	default-information originate
default-information originate	!
!	interface Loopback0
interface Loopback0	ip router isis
ip router isis	clns mtu 4100
clns mtu 1400	ip pim sparse-mode
ip pim sparse-mode	exit
exit	!
!	
DHCP Pool Information	

ip dhcp pool nw\_orchestration\_pool network 10.4.218.0 255.255.255.192 option 43 ascii 5A1D;B2;K4;I10.4.249.241;J80; default-router 10.4.218.1 class ciscopnp address range 10.4.218.2 10.4.218.62 ip dhcp class ciscopnp option 60 hex 636973636f706e70 I ip dhcp excluded-address 10.4.218.1 Vlan1 Configuration vlan 1 interface Vlan1 ip address 10.4.218.1 255.255.255.192 no shutdown ip router isis clns mtu 4100 bfd interval 500 min rx 500 multiplier 3 no bfd echo exit I Switchport Configuration on interfaces used for discovery

(Each discovery interface on primary seed device gets this config) interface TenGigabitEthernet1/1/8 switchport

switchport mode access switchport access vlan 1 interface TenGigabitEthernet1/1/7 switchport switchport mode access switchport access vlan 1 exit Multicast Configuration (Optional: only configured if multicast checkbox is enabled) If Peer seed is configured, these multicast CLIs will be pushed on Peer seed as well. Pls. note that same rp-address will used to configure Loopback60000 on both Primary and Peer seed interface Loopback 60000 ip address 10.4.218.67 255.255.255.255 ip pim sparse-mode ip router isis ip pim register-source Loopback60000

ip pim rp-address 10.4.218.67

%INIT: waited 0 seconds for NVRAM to be available --- System Configuration Dialog --- Would you like to enter the initial configuration dialog? [yes/no]: Press RETURN to get started! \*Aug 2 23:13:50.440: %SMART\_LIC-5-COMM\_RESTORED: Communications with the Cisco Smart Software Manager or satellite restored \*Aug 2 23:13:51.314: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named TP-self-signed-1875844429 has been generated or imported \*Aug 2 23:13:51.315: %SSH-5-ENABLED: SSH 1.99 has been enabled \*Aug 2 23:13:51.355: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configuration \*Aug 2 23:13:51.418: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named TP-self-signed-1875844429.server has been generated or imported \*Aug 2 23:13:52.071: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down \*Aug 2 23:13:53.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down \*Aug 2 23:14:00.112: %HMANRP-6-EMP\_ELECTION\_INFO: EMP active switch 1 elected: EMP\_RELAY: Mgmt port status DOWN, reelecting EMP active switch \*Aug 2 23:14:00.112: %HMANRP-6-EMP\_NO\_ELECTION\_INFO: Could not elect active EMP switch, setting emp active switch to 0: EMP\_RELAY: Could not elect switch with mgmt port UP \*Aug 2 23:14:02.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:14:04 UTC Thu Aug 2 2018 to 23:14:02 UTC Thu Aug 2 2018, configured from console by vty0. Aug 2 23:14:02.000: %PKI-6-AUTHORITATIVE\_CLOCK: The system clock has been set. Aug 2 23:14:02.462: %PNP-6-PNP\_DISCOVERY\_DONE: PnP Discovery done successfully Aug 2 23:14:07.847: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configuration Aug 2 23:14:16.348: %AN-6-AN\_ABORTED\_BY\_CONSOLE\_INPUT: Autonomic disabled due to User intervention on console. configure 'autonomic' to enable it. %Error opening tftp://255.255.255.255/networkconfg (Timed out) Aug 2 23:14:25.263: AUTOINSTALL: Tftp script execution not successful for VI1.

• Once the device is disovered, DNA Center will first check whether any golden image is marked for the switch family of the discovered device. If golden image is marked and the discovered device is not running the golden image, then Lan automation will first upgrade the discovered device to the golden image. If not, DNA Center will skip image upgrade and proceed to pushing intial device config. Below logs are seen when image is upgraded

#### Oct 5 19:20:11.437: MCP\_INSTALLER\_NOTICE:

```
Installer: Source file flash:cat9k_iosxe.16.06.04s.SPA.bin is in flash, Install directly
Oct 5 19:20:12.450: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:20:12 provision.sh: %INSTALL-5-
OPERATION_START_INFO: Started install package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:20:22.778: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:20:22 packtool.sh: %INSTALL-5-
OPERATION_START_INFO: Started expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:21:26.034: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:21:26 packtool.sh: %INSTALL-5-
OPERATION_COMPLETED_INFO: Completed expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:22:09 provision.sh: %INSTALL-5-
OPERATION_COMPLETED_INFO: Completed install package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:22:09 provision.sh: %INSTALL-5-
OPERATION_COMPLETED_INFO: Completed install package flash:{cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:22:09 provision.sh: %INSTALL-5-
OPERATION_COMPLETED_INFO: Completed install package flash:{cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:22:09 provision.sh: %INSTALL-5-
OPERATION_COMPLETED_INFO: Completed install package flash:{cat9k_iosxe.16.06.04s.SPA.pkg,cat9k-
guestshell.16.06.04s.SPA.pkg,cat9k-espbase.16.06.04s.SPA.pkg,cat9k-
sipbase.16.06.04s.SPA.pkg,cat9k-sipspa.16.06.04s.SPA.pkg,cat9k-
sipbase.16.06.04s.SPA.pkg,cat9k-sipspa.16.06.04s.SPA.pkg,cat9k-
webui.16.06.04s.SPA.pkg,cat9k-wlc.16.06.04s.SPA.pkg}
```

\*\*\* \*\*\* --- SHUTDOWN NOW ---

Oct 5 19:22:20.950: %SYS-5-RELOAD: Reload requested by controller. Reload Reason: Image Install.

Chassis 1 reloading, reason - Reload command

Oct 5 19:22:30.501 FP0/0: %PMAN-5-EXITACTION: Process manager is exiting: reload fp action requested Oct 5 19:22:

Initializing Hardware...

 Next, DNA Center will push part of configuration allowing devices to get on-boarded and managed by DNAC. LAN Automation Status will show "In Progress", Discovered Devices status will show aggregate status of all devices being discovered, and "Devices" tab will show status of individual devices being discovered

cisi	DNA DESIGN	POLICY PR	OVISION ASSU	IRANCE				2 <b>0</b> Q	 • =
Devic	es Fabric						LAN Automation Status		×
Dev	ice Inventory								C Refresh
Invent	ory (3) Unclaimed Dev	rices					Summary Logs Devices		
<ol> <li>Selection</li> </ol>	t device(s) to assign to a Sit	e and Provision netwo	rk settings from the I	Network Hierarchy.			Discovend Site:         SJC24-1           IP Pool:         LAVL_Auto   192.108.199.0/24           Device Prefix:         0300_bridecisios.com           Pear Device:         9500_bridecisios.com           Pear Device:         Friggiblithernet1/0/1           Status:         In Progress		
Y Fil	Actions ~ O LA	N Automation ~					Discovered Devices:		
	Device Name -	Device Family	IP Address	Site	Serial Number	Uptime	⊘ Completed : 0		Б
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, F0C2052X0C9, FCW2020F0A0	46 days, 1			
	9500_border-6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	5 days, 0:			Ŀ
	9500_border.cisco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FCW2205A33L	46 days, 1			
						1 to 3 of			

• During this time, you will see logs like below on the PNP-agent. At this point it is safe to press return on the console if you wish to. When you press return, you will see that hostname has changed to the value entered at "Hostname Mapping" when starting LAN auto

Aug 2 23:14:50.682: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to up Aug 2 23:14:51.487: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up Aug 2 23:14:51.681: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up Aug 2 23:14:51.854: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/23, changed state to up 2 23:14:52.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, Aug changed state to up Aug 2 23:14:52.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to up 000123: Aug 2 23:16:17.345: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named dnac-sda has been generated or imported 000124: Aug 2 23:16:17.423: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait... 000125: Aug 2 23:16:17.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up 000126: Aug 2 23:16:17.479: %CLNS-6-DFT\_OPT: Protocol timers for fast convergence are Enabled. 000127: Aug 2 23:16:17.487: %PARSER-5-HIDDEN: Warning!!! ' ispf level-1-2 ' is a hidden command. Use of this command is not recommended/supported and will be removed in future. 000128: Aug 2 23:16:17.489: %BFD-6-BFD\_IF\_CONFIGURE: BFD-SYSLOG: bfd config apply, idb:Vlan1 000129: Aug 2 23:16:18.423: %CLNS-3-BADPACKET: ISIS: LAN L1 hello, packet (9097) or wire (8841) length invalid from f87b.2077.b147 (Vlan1) 000130: Aug 2 23:16:18.502: %BFD-6-BFD\_SESS\_CREATED: BFD-SYSLOG: bfd\_session\_created, neigh 204.1.183.1 proc:ISIS, idb:Vlan1 handle:1 act 000131: Aug 2 23:16:19.269: %BFDFSM-6-BFD\_SESS\_UP: BFD-SYSLOG: BFD session ld:1 handle:1 is going UP 000132: Aug 2 23:16:19.494: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 0100.1001.0001 (Vlan1) Up, new adjacency 000133: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: Op43 has 5A. It is for PnP 000134: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: After stripping extra characters in front of 5A, if any: 5A1D; B2; K4; I172.16.1.100; J80; op43\_len: 29 000135: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: \_pdoon.2.ina=[Vlan1] 000136: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: \_papdo.2.eRr.ena 000137: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: \_pdoon.2.eRr.pdo=-1 000138: Aug 2 23:16:30.010: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 9324-SN-BCP-1 (Vlan1) Up, new adjacency

Once all the device(s) are discovered, Discovered Devices status will change to "Completed" and the discovered device(s) will be added to inventory

	-	_						
Device	s Fabric						LAN Automation Status	×
Dev	ice Inventory						🔿 Refre	sh
Invento	ry (3) Unclaimed Dev	ices					Summary Logs Devices	
Select	device(s) to assign to a Sit	e and Provision networ	k settings from the I	Network Hierarchy.			Discovered Site:         SJC24-1           IP Pool:         LAN_Auto   192.168.199.0/24           Device Prefac:         9300_Ection           Premary Device:         9500_Ection           Peer Device:         970/GabitShement10/1           Status:         In Progres	
Y Fib	er Actions - O LA	Automation ~					Discourse) Bey/ces:	
	Device Name •	Device Family	IP Address	Site	Serial Number	Uptime	Completed : 1 O In Progress : 0 O Error : 0	5
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W; FOC2052X0C9; FCW2020F0A0	46 days,		ke a Wi
	9500_border-6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	5 days, 0		No
	9500_border.clisco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FCW2205A33L	46 daya,		
						1 to 3 of		

cisc	DNA DESIGN	POLICY PR	OVISION ASSU	IRANCE				_@ Q Ⅲ Ø Ⅲ
Device	es Fabric						LAN Automation Status	×
Dev	ice Inventory							⊖ Refresh
Invento	ory (4) Unclaimed Dev	ices					Summary Logs Devices	
Select	t device(s) to assign to a Site	e and Provision networ	rk settings from the I	Network Hierarchy.			Message Added device FCW2214L053 to inventory	Timestamp 2018-10-17 00:39:02.58
							Added device with Serial Number FCW2134D168 to Queue	2018-10-17 00:34:29.796
₹ Filt	er Actions - O LA	Automation ~					Received Ztd Device Provisioned Message for FCW2214L0S3	2018-10-17 00:33:16.936
	Device Name -	Device Family	IP Address	Site	Serial Number	Uptime	Claimed device FCW2214L0S3 and generated config file with hostname 9300_Edge-7	2018-10-17 00:31:41.674
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, FDC2052XDC9, FCW2020F0A0	45 days, 1	Started the Network Orchestration Session with primary device: 9500_border.clsco.com	2018-10-17 00:24:59.12
	9300_Edge-7	Switches and Hubs	192.168.199.97	SJC24/SJC24-1	FGW2214L053	0:11:56.80		1
	9500_border-6.cisco.com	Switches and Hubs	192,168,199,99		FOW2229A4US	5 days, 1:0		
	9500_border.cisco.com	Switches and Hube	192.168.210.1		FGW2205A33L	45 days, 1		
						1 to 4 of		

CISCO CENTER DI	SIGN POLICY PI	ROVISION ASS	URANCE						∠@ ⊂ ≡ ∘	=
Devices Fabric						LAN Autom	ation Status			×
	Device Inventory Inventory (4) Unclaimed Devices						Devices		4	Refresh
<ol> <li>Select device(s) to assign</li> </ol>	o a Site and Provision netwo	ork settings from the	Network Hierarchy.			Name	Address	Serial	Status	
						9300_Edge-7	192.168.199.97	FCW2214L053	Completed	
V Filter Actions - 0 Device Name -	LAN Automation v	IP Address	Site	Serial Number	Uptime					
3850_Edge_3.cisco.	om Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, F0C2052X0C9, FCW2020F0A0	46 days, 1					Make a Wish
9300_Edge-7	Switches and Hubs	192.168.199.97		FCW2214L053	0:11:56.85					Mak
9500_border-6.cisco	com Switches and Hubs	192.168.199.99	5J024/5J024-1	FCW2229A4L5	5 days, 1:					
9500_border.cisco.co	Switches and Hubs	192.168.210.1		FCW2205A33L	46 days, 1					
					1 to 4 of					

Navigate to Inventory and filter by the serial number. The newly discovered switches will show up

#### as 'Managed'

cis cis	CO CENTER			Inventory				∠20 Q III ©	
							ast updated: 5:40 pm 🛛 📿 Refresh	Import     DExport	🕂 Add
Y Fite	r Actions ~								
	Device Name .	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status	Site	:
	3850_Edge_3.clsco.com (2	192.168.199.98	Reachable	47 days 16 hrs 32 mins	12 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
	9300_Edge-7 (2*	192.168.199.97	Reachable	1 day 0 hrs 10 mins	a few seconds ago	00:25:00	Managed	SJC24/SJC24-1	
	9500_border-6.cisco.com \3	100 160 100 00	Reachable	6 days 1 hrs 14 mins	a minute ann	1110 W	Managed	SJC24/SJC24-1	
	9500_border.clsco.com [2*	192.168.210.1	Ø Reachable	47 days 16 hrs 40 mins	7 minutes ago	00:25:00	Managed	SJC24/SJC24-1	1
									_

Below sample config is pushed to Discovered Device(s)

```
!
archive
log config
logging enable
logging size 500
hidekeys
!
!
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
1
service password-encryption
1
service sequence-numbers
1
! Setup NTP Server
! Setup Timezone & Daylight Savings
!
ntp server 10.4.250.104
!
! ntp update-calendar
1
! clock timezone <timezoneName> <timezoneOffsetHours> <timezoneOffsetMinutes>
! clock summer-time <timezoneName> recurring
1
! Disable external HTTP(S) access
! Disable external Telnet access
! Enable external SSHv2 access
!
no ip http server
!
no ip http secure-server
1
ip ssh version 2
!
ip scp server enable
!
line vty 0 15
! maybe redundant
login local
transport input ssh
! maybe redundant
transport preferred none
! Set VTP mode to transparent (no auto VLAN propagation)
! Set STP mode to Rapid PVST+ (prefer for non-Fabric compatibility)
```

```
! Enable extended STP system ID
! Set Fabric Node to be STP Root for all local VLANs
! Enable STP Root Guard to prevent non-Fabric nodes from becoming Root
! Confirm whether vtp mode transparent below is needed
vtp mode transparent
1
spanning-tree mode rapid-pvst
spanning-tree extend system-id
! spanning-tree bridge priority 0
! spanning-tree rootguard
! spanning-tree portfast bpduguard default
no udld enable
errdisable recovery cause all
1
errdisable recovery interval 300
1
ip routing
!Config below applies only on underlay orchestration
1
! Setup a Loopback & IP for Underlay reachability (ID)
! Add Loopback to Underlay Routing (ISIS)
1
interface loopback 0
description Fabric Node Router ID
ip address 10.4.218.97 255.255.255.255
ip router isis
1
1
! Setup an ACL to only allow SNMP from Fabric Controller
! Enable SNMP and RW access based on ACL
1
snmp-server view DNAC-ACCESS iso in
1
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
!
snmp-server user admin DNACGROUPAuthPriv v3 auth MD5 C1sco123 priv AES 128 C1sco123
1
1
! Set MTU to be Jumbo (9100, some do not support 9216)
1
system mtu 9100
! FABRIC UNDERLAY ROUTING CONFIG:
1
! Enable ISIS for Underlay Routing
! Specify the ISIS Network ID (e.g. encoded Loop IP)
! Specific the ISIS domain password
! Enable ISPF & FRR Load-Sharing
! Enable BFD on all (Underlay) links
router isis
net 49.0000.0100.0421.8097.00
domain-password cisco
ispf level-1-2
metric-style wide
nsf ietf
! fast-reroute load-sharing level-1
log-adjacency-changes
bfd all-interfaces
! passive-interface loopback 0
!
1
!
```

```
interface vlan1
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
1
Ţ
!This config goes to subtended node
username lan-admin privilege 15 password 0 Clsco123
1
enable password C1sco123
1
1
hostname CL-9300_7
1
interface vlan1
ip router isis
1
1
end
```

- Once, Discovered devices status shows "Completed" and all the discovered device(s) show in Inventory as "Managed", Lan Auto can be Stopped
- As an additional step before stopping Lan Auto, check Topology page to ensure the links between the discovered device and primary and peer seed

\_\_\_\_\_ Q \_ \_ \_ Ø \_ \_

are displayed. Click on the physical link between seed and discovered device. Confirm that the interfaces are correct

cisco acate					
∀ Filter      O View Options		Q, Fi	d by device IP, o	device type, MAC	@
EQ, Find Hierarchy		Y Filter			×
v 🛞 Global		Device .	Interface	IP Address	Speed
√ 🖑 San Jose			Tenge		10
へ 回到 SJC24		2300_Edge-7	Tenge 1/1/5	192.168.199.97	Gbps
		9500_border.cisco.com	Fortyge 1/0/1	192.168.210.1	10 Gops
			showing 1 of 1		
	$\sim$				
	The Internet				
	8				Ē
	95006.csco.com 9500r.csco.com				
	9300_Edge-7 38503.cscc.com				

Note: If the physical link does not show up, re-sync that seed device where the physical link connects. After re-sync check the topology page again to ensure the links shows up before stopping Lan auto. There have been issues where after stopping Lan auto, the link to secondary seed does not get configured. This extra step will help avoid the issue. Fix is in 1.2.4 (CSCvk44711)

#### 2. Stop Lan Automation

This is second stage of the Provision step. Purpose of this stage is to finish discovering all devices that a user wishes to and to prevent inadvertent discovery of any additional devices

- Click Stop
- During this time, rest of the configuration gets pushed to network device(s) that includes converting the point-to-point links from Layer 2 to Layer 3
- Vlan 1 configuration is removed and vlan 1 ip addresses are returned to the Lan automation pool

• Device get on-boarded in DNAC and assigned to the site

CISCO CENTER DESIGN POLICY PROVISION ASSURANCE		Q Ⅲ Ø Ⅲ
Devices Fabric		
Device Name - Device Type IP Address Site Serial Number	Started the Network Orchestration Session with primary device: 4/357/ec4-4/05-4/91 0/3-1201ee/36/065	
State_Edge_3 Switches and Hube: 192.168.199.98	) Devices	
Stopping Underlay Ti 1990, Page, 1 Switches and Nuber 1992, 168, 199, 97 Schücks-Laure (Construction)	his may take few mins Devices	

#### Once stop in initiated, Lan Automation Status will show as "STOP In Progress

	CISCO CENTER DESIGN	POLICY PR	OVISION ASSU	RANCE				∠ <b>છ</b> વ	 0	
0	Devices Fabric						LAN Automation Status			×
C	evice Inventory								CRe	resh
li	wentory (4) Unclaimed Dev	ices					Summary Logs Devices			
0	Select device(s) to assign to a Sit	e and Provision netwo	ik settings from the P	Vetwork Hierarchy.			Discovered Site:         SJC24-1           IP Pool:         LAN_Leto   192.168.199.0/24           Device Prefax:         9300_Edge			
							Primary Device: 9500_border.clisco.com Peer Device: none Primary Device Interface: FortyGigabitEthernet1/0/1			
5	7 Filter Actions - O LA	Automation ~					Status: STOP In Progress			
	Device Name	Device Family	IP Address	She	Serial Number	Uptime	Discovered Devices:			
-	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98		FCW2133F05W, FCC2052X8C9, FCW2020F0A0	46 days, 1	Campleted : 1 In Progress : 0 In Progress : 0			a Wish
	9300_Edge-7	Switches and Hubs	192.168.199.97		FCW2214L053	0:11:56.80				Make
1	9600_border-6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW2229A4LS	5 days, 1:0				
	9500_border.cisco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FCW2205A33L	46 daya, 1				
						1 to 4 of				

#### Below sample config is pushed to the Discovered device after stopping Lan automation

Network orchestration service issues RESYNC for Seed and all PnP devices to retrieve state of all links. After initial Resync is complete, It pushes the L3 configuration on all L2 links. Finally it issues Resync again to re-synchronize the cluster's link state.

L3 link configuration pushed on stopping network orchestration (Each pair of interface gets its set of configuration):

interface GigabitEthernet1/0/13
description Fabric Physical Link
no switchport
dampening
ip address 192.168.2.97 255.255.255.252
ip router isis
ip lisp source-locator Loopback0
logging event link-status
load-interval 30
bfd interval 500 min\_rx 50 multiplier 3
no bfd echo
isis network point-to-point

Once all the point-to-point links between the seeds and discovered devices, including links

between peer seed and discovered devices, are configured, those devices are added to the site and synced to DNA Center.

• Lan Automation Status will show Completed and that completes Lan Automation process

cisco										
Devices	s Fabric					LAN Automation Status				
	ce Inventory ry (4) Unclaimed Dr	wices					Summany Logs Devices	⊖ Refr		
							Discovered Site: SJC24-1			
	device(s) to assign to a S		rtwork settings from t	he Network Hierarchy	κ.		IP Pool: LAN_Auto 192.168.199.0/24 Device Prefix: 9300_Edge Primary Device: 9300_Edge Peer Device: 0500_border.cisco.com Peer Device: none Primary Device Interfaces: ForgiGabiEthermet1/0/1 Status: Completed			
Filter	r Actions - O L	AN Automation 🖂					Discovered Devices: 1			
	Device Name •	Device Family	IP Address	Site	Serial Number	Upt	⊘ Completed : 1 ③ In Progress : 0 ⊗ Error : 0			
	3850_Edge_3.cisco.com	Switches and Hubs	192.168.199.98	SJC24/SJC24-1	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	47 i 175				
	9300_Edge-7	Switches and Hubs	192.168.199.97	SJC24/SJC24-1	FCW2214L0S3, FCW2224C122, FOC2224Q0UE, FCW2224C123	1 d				
	9500_border- 6.cisco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FOW2229A4LS	6 d				
	9500_border.clsco.com	Switches and Hubs	192.168.210.1	SJC24/SJC24-1	FOW2205A33L	47 1				
tisco	DNA DESIGN	POLICY	PROVISION AS	SURANCE		1 to 4 of		∠ <b>2</b> Q Ⅲ 0 1		
isco	CENTER	POLICY	PROVISION AS	SSURANCE		1 to 4 of	LAN Automation Status	∕20 ⊂ ⊞ ⊘		
evices	CENTER	POLICY	PROVISION AT	SSURANCE		1 to 4 of	LAN Automation Status			
evices	Fabric		PROVISION A1	SSURANCE		1 to 4 of	Summary Logs Devices	O Ref		
vices evices	Fabric Ce Inventory	víces				1 to 4 of	$\sim$	⊖ Ref		
evices	re Inventory y (4) Unclaimed De	víces				1 to 4 of	Summary Logs Devices	C Ref Timestam 2018-10-17 00:54:4:		
evices evices evices elect d	CE Inventory y (4) Unclaimed De device(s) to assign to a Si	vices te and Provision net				1 to 4 of	Summary Logs Devices Message Network Orchestration Queue has been cleared	C Ref Timestam 2018-10-17 00:54:40 2018-10-17 00:54:40		
elect d	CE Inventory y (4) Unclaimed De device(s) to assign to a Si	vices te and Provision net			Setal Humber	1 to 4 of	Summary Logs Devices Message Network Orchestration Queue has been cleared Ended Network Orchestration Session	C Ref Timestam 2018-10-17 00:54:4 2018-10-17 00:54:3		
evices evices entory elect d	Central     Fabric     Ce Inventory     y (4) Unclaimed De     device(s) to assign to a Si	vices te and Provision ner N Automation ~	twork settings from th				Summary Loss Devices Message Network Orchestration Queue has been cleared Ended Network Orchestration Session Configuring L3 interfaces for the session's Tier 2 Devices	© Ref Timestam 2018-10-17 00:54:4 2018-10-17 00:54:3 2018-10-17 00:54:3		
vices evice entory elect d	Fabric Fabric Fabric CCE Inventory y (4) Unclaimed De device(s) to assign to a Si	vices te and Provision ner N Automation ~ Device Family Switches and	twork settings from th	ne Network Hierarchy. Site	Serial Number	Upr	Summary Logs Devices Message Network Orchestration Queue has been cleared Ended Network Orchestration Session Configuring L3 interfaces for the session's Tier 2 Devices Ending device discovery	C Ref Timestam 2018-10-17 00:54:41 2018-10-17 00:54:3 2018-10-17 00:54:3 2018-10-17 00:54:3 2018-10-17 00:39:1		
evices evices evices rentory elect d	Contract     Fabric     Fabric     Ce Inventory     y (4) Unclaimed De     device(s) to assign to a Si      Accoss ~ 0 U  Device Name -  3809_Edge_3.cleos.com	vices te and Provision ner N Automation ~ Device Family Switches and Switches and	twork settings from th IP Address 192.168.199.98	he Network Hierarchy. Site SJ024/5J024-1	Serial Number FOX2133F09W, FOC2052X0C9, FOX2020F0A0 FOX2214L053, FOX2224C122, FOX2224C04E,	6.00 43 - 175	Summary Logs Devices Message Network Orchestration Queue has been cleared Ended Network Orchestration Session Configuring L3 interfaces for the session's Tier 2 Devices Ending device discovery Added device FCW2214L0S3 to inventory	© Ref Timestam 2018-10-17 00:54:4 2018-10-17 00:54:3 2018-10-17 00:54:3 2018-10-17 00:54:3 2018-10-17 00:34:2		
Pevices Pevic Ventory Filter	Contrain     Fabric     Fabric     Fabric     Ce Inventory     (4) Unclaimed De     device(s) to assign to a Si      / Actions ~ 0 U      Device Name -     3850_E6ge_3.claco.com     9000_E6ge-7     9000_boxter-	vices te and Provision ner N Automation ~ Device Family Switches and Hubs Switches and Switches and Switches and	P Address 192.168.199.97	Network Hierarchy. Site SJC24/SJC24-1 SJC24/SJC24-1	Berlal Number FCW2133F09W, FOC2052X009, FCW2020F9A0 FCW2214L655, FCW2224C122, FOC2224QULE, FCW2224C123	Орт 47- 12- 10	Summary Logs Devices Message Network Orchestration Queue has been cleared Ended Network Orchestration Session Configuring L3 interfaces for the session's Tier 2 Devices Ending device discovery Added device FCW2214LDS3 to Inventory Added device with Serial Number FCW2134D168 to Queue	<		

#### **Miscellaneous**

#### 1. Adding a brand new switch or a switch never present in DNAC to a LAN automated stack

Switches can be added to a stack that is already Lan automated and in provisioned state without having to Lan automate/discover the new switch. Follow below steps for a smooth addition

- 1. Ensure the switch was not part of DNAC earlier i.e it wasn't discovered and present in inventory
- 2. Ensure the switch being added has the same image and license version as the provisioned standalone/stack. Do "show ver" and "show license rightto-use"
- $\mathbf{3.}$  Ensure the switch is in same boot mode as the stack i.e either INSTALL (preferred) or BUNDLE

```
4.
```

-						
	9300_1	Edge	_1#show ver   i	nc INSTALL		
	* -	L 62	C9300-48U	16.6.3	CAT9K_IOSXE	INSTALL
	-	2 62	C9300-48U	16.6.3	CAT9K_IOSXE	INSTALL
		3 62	C9300-48U	16.6.3	CAT9K_IOSXE	INSTALL
	4	1 62	C9300-48U	16.6.3	CAT9K_IOSXE	INSTALL

5. Connect the new switch to the stack using the stack cable and THEN POWER IT ON

- 6. After 2-3 minutes this new switch will be added to the stack as a standby (if one switch was present before adding) or as a member (if 2 or more switches were already present in the stack)
- 7. Check output of "show ver" and "show switch" to ensure the new switch is added. "show ver" consists of serial number for all switches.
- ${f 8.}$  Once the switch is added to stack, go to Inventory service, select the original provisioned switch/stack, and do re-sync
- 9. After the sync, the new serial number will show up and that completes the addition

10. It is possible to add more than one switch at a time. Follow the procedure above and ensure cabling is correct Before addition:

ol) ci	SCO CENTER			Inventory	<b>∠</b> ● Q Ⅲ Φ					
						Last o	pdated: 4:14 pm	C Refresh 👜 Import	🖞 Export	🕂 Add
₹ Filt	er Actions ~									
	Device Name	IP Address	Reachability Status	Serial Number	Uptime	Last Updated	Resync Interval	Last Sync Status	Site	I
	3850_Edge_3 (2*	192.168.199.98	Reachable	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	8 days 6 hrs 22 mins	7 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
	9300_Edge_1 C*	192.168.199.97	Reachable	FCW2214L0S3, FCW2224C122	1 day 1 hrs 50 mins	6 minutes ago	00:25:00	Managed	SJC24/SJC24-1	1
	9500_border.clscodna 🛙	192.168.210.1	Reachable	FCW2205A33L	5 days 6 hrs 24 mins	13 minutes ago	00:25:00	Managed	SJC24/SJC24-1	Mich
Show 1	0 • entries			Showing 1 - 3	of 3					

ah cu	CO CENTER			Inventory				۷۵	Q Ⅲ Ø	
						Last update	ed: 4:45 pm	C Refresh 🖄 Import	🖞 Export	🕂 Ade
🝸 Filt	Actions ~									
	Device Name	IP Address	Reachability Status	Serial Number	Uptime	Last Updated	Resync Interval	Last Sync Status	Site	÷
	3850_Edge_3 🕑	192.168.199.98	Reachable	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	8 days 6 hrs 49 mins	10 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
	9300_Edge_1 2	192.168.199.97	Reachable	FGW2214L053, FGW2224C122, FOC2224Q0UE, FGW2224C123	1 day 2 hrs 13 mins	12 minutes ago	00:25:00	Managed	SJC24/SJC24-1	[
	9500_border.ciscodna 🕑	192.168.210.1	Reachable	FCW2205A33L	5 days 6 hrs 52 mins	17 minutes ago	00:25:00	Managed	SJC24/SJC24-1	
how 1	0 entries			Showing 1 - 3 of 3						1 No

#### 2. Adding a switch already present in DNAC to a LAN automated stack

- If the switch being added was previously Lan automated (i.e part of another stack/standalone) and/or was discovered by PNP, then in order to add it first remove the switch physically and then remove its entry from Inventory and PNP application/database.
- Removing from inventory:

- If the switch is a standalone, navigate to DNA->Inventory, select the switch to be removed and under "Actions", click on "Delete Device"- If the switch is part of a stack, after removing the switch physically, resync the original stack. Once sync is complete, the removed switch serial number should not show up under inventory

• Removing from PNP:

- If the switch is a standalone, first unconfigure "pnp profile pnp-zero-touch" from the switch and then delete the entry from PNP database under "Device"

- If the switch is part of a stack, after removing the switch physically, ensure the removed switch does not have "pnp profile pnp-zero-touch" and then delete the entry from PNP database under "Device"

#### 3. Configuring additional links after Lan auto is stopped

Use this method when you want to configure a) additional links between primary and peer seed devices or between distribution devices after lan auto was stopped b) uplinks from newly added switch to the stack to primary and peer seed

If you selected 'Enable Multicast' option the first time Lan auto was run on the device, do not select this option when using this method to configure additional links. Use the steps below and once Lan auto stops, go to the recently configured Layer 3 ports and manually configure "ip pim sparse-mode" under the interface

• Check output of "show cdp neighbor" to ensure the neighbor connected to the new link is displayed. Below, user is trying to configure new link connected to port Ten4/1/5 on switch 9300\_Edge-7. On other end the link is connected to switch 9500\_border-6 via port For1/0/1

```
9300_Edge-7#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
9500_border.cisco.com
Ten 1/1/5 173 R S I C9500-12Q For 1/0/1
9500_border-6.cisco.com
Ten 4/1/5 136 R S I C9500-12Q For 1/0/1
```

- Ensure the ports to whom link is connected (port Ten4/1/5 and For1/0/1 above), don't have any L3 config on them. If they do, default interfaces connected to the new uplink being added and resync both the devices.
- Next, go to provision page and click on Lan automation. Here, under "Primary Device" enter the switch (9500\_border-6 above) to whom the new link is connected to. Under "Peer Device", enter switch (9300\_Edge-7 above) where new link is to be configured.
- Next, select the port on the Primay device where the uplink will be connected i.e port where PNP device is connected (For1/0/1 above)
- Use same Lan auto pool that was used when provisioing the original stack.

CISCO CENTER DES	IGN POLICY	PROVISION AS	ISURANCE			∠® ⊂ ≡ ∽ ≡						
Devices Fabric						LAN Automation						
Device Inventory Inventory (4) Unclaimed Select device(s) to assign to	I Devices	work settings from t		her end of the link. Can be primary or seco	ndary seed	Seed Device Six* GibbalSan JoseSUC24:SUC24:1 Winany Doice* SECO_boter& Very Device where new link is to be configured Choose Primary Device Ports*						
Filter Actions	LAN Automation V Device Family Switches and	IP Address	Site	Serial Number	0;	G0.00     FortyGigabitEthernet1/0/1       FortyGigabitEthernet1/0/2     FortyGigabitEthernet1/0/3       FortyGigabitEthernet1/0/4     FortyGigabitEthernet1/0/5						
9300_Edge-7	Nubs Switches and Hubs	192.168.199.97	SJC24/SJC24-1	FOW2138105W, F0C20528005W, F0W20284080 FOW2214L053, F0W2224C122, F0C2224Q0UE, F0W2224C123	5	Discovered Device Configuration Six* Goba/San Jose/SJC24/6JC24-1						
9500_border- 6.cieco.com	Switches and Hubs	192.168.199.99	SJC24/SJC24-1	FCW222BA4LS	11	Use same pool when lan automation was run						
9500_border.cisco.com	Switches and Hubs	192.168.210.1	5J024/5J024-1	FCW2205A33L	52 16	SIS Password						
					1 to 4 o	Hostname Mapping Device Name Prefix Hostname Map File v Uplead File						
						Clear All Cancel Start						

- Start Lan auto. Wait for 2 minutes and then Stop Ian auto. Since, there is no new device discovery to be made, we don't have to go through entire Lan auto. Once you stop Lan auto, both the ports connected to uplink will be configured with IP address from the same Lan auto pool
- Once Lan auto is stopped and completed, you will see both the ports will be configured for Layer 3 from the Lan pool used

9300\_Edge-7#show run int t4/1/5 Building configuration... Current configuration : 325 bytes ! interface TenGigabitEthernet4/1/5 description Fabric Physical Link no switchport dampening ip address 192.168.199.85 255.255.255.252 ip lisp source-locator Loopback0 ip router isis logging event link-status loadinterval 30 bfd interval 100 min\_rx 100 multiplier 3 no bfd echo isis network point-to-point 9500\_border-6#show run int Fo1/0/1 Building configuration... Current configuration : 327 bytes ! interface FortyGigabitEthernet1/0/1 description Fabric Physical Link no switchport dampening ip address 192.168.199.86 255.255.255.255.255 ip lisp source-locator Loopback0 ip router isis logging event link-status load-interval 30 bfd interval 100 min\_rx 100 multiplier 3 no bfd echo isis network point-to-point end

Note: Above IP address addition can also be achieved manually via API. If you are familiar with API, you can try it out. However, doing via Lan auto is a much cleaner way since it will take care of updating all the table entries. Other advantage of lan auto is that when the device is removed from inventory, all assocaited IP addresses will be released. If IP addresses were configured manually via API, they will not be released. Refer to "Procedure to configure P-P" doc attached at bottom for API method

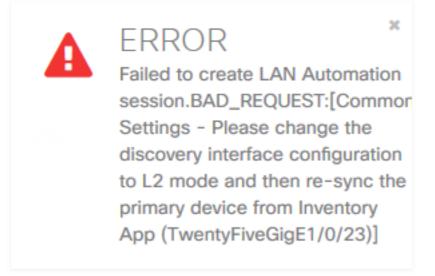
#### 4. Moving uplink to the newly added switch

Currently, it is not possible to move uplink from a stack that is already provisioned to the newly added switch to that stack. DDTS: <u>CSCvk40550</u>

#### 5. Using 9500H as seed device or PNP agent

Note: 9500H (high perfromance skus: C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C) as seed support started from DNAC 1.3.x release and IOS-XE 16.11 version onwards. DNAC 1.2.x and previous version doesn't support 9500H model for Seed and/or PNP devices. However, if you really need to make it work with DNAC 1.2.x release, follow below steps at your own risk. BU will not be repsonsible for fixing any issues arising out of using non-supported releases

- Prior to 16.11.x, 9500H ports will be layer 3 by default. Hence, if using as seed, first change the seed port to layer 2 and resync with DNAC
- If using skus C9500-32C or C9500-32QCas seed, use 16.9.x image. DO NOT use 16.10.x or 16.11.1 because of <u>CSCvo40879</u>. This DDTS is fixed in 16.11.1c and 16.11.2 and onwards
- If using 25G or 5G port on C9500-24YC or C9500-48YC skus and DNAC 1.2.10 or earlier, you will need to apply a patch. Without the patch, DNAC will
  not recgonize those port speeds and Lan auto will give following error when started Defect <u>CSCvo42419</u>.



• If using C9500-24YC or C9500-48YC as PNP agent, then you will need to run 16.11.x image because the ports need to be layer 2 and they cannot be manually changed to Layer 3 as in case of seed

## 6. Using 40G interface on Catalyst 9400

- Prior to 16.11.1, 40G interface on Catalyst 9400 supervisor is disabled by default and has to be manually enabled. If used as PNP-agent, PNP will fail since enabling the 40G port will break Day-0 functioanlity. To make 40G port work on a PNP-agent prior to 16.11.1, follow few manual steps below
- 1. Start LAN automation
- 2. Power up the 9400 and break out of the initial configuration wizard
- 3. Enable the 40G port on the supervisor. For example 3/0/9 and 3/0/10
- 4. Configure terminal -> interface vlan1 -> ip address dhcp -> no shut
- 5. Confirm vlan 1 ip address accquired via DHCP and default route present
- Configure pnp profile with the following pnp profile pnp-zero-touch transport http ipv4 <dnac-ip-address> port 80 (Use virtual IP if you have configured it)
- 7. Configuring the pnp profile will have the device call home and LAN automation picks up from there on
- From 16.11.1 on, IOS will enable 40G port on boot-up provided below two conditions are met

1. Switch should have Day 0/factory default config (Refer to section 'PNP-agent initial state if you want to know how to bring a device to day 0 config)

2. For Single supervisor: No 10G/1G SFP should be inserted on any of the SUP ports (1-8) and a 40G QSFP should be inserted on either port 9 or 10

3. For Dual supervisor: No 10G/1G SFP should be inserted on any of the SUP ports (1-8) and a 40G QSFP should be inserted in port 9 ONLY

• Note: this does not yet work for Dual Supervisor until a fix is available for CSCvs59282 .

# **Known Issues**

- If the hostname (hostname plus domain name) for the peer seed is greater than 40 characters then, the links connecing to peer/secondary seed will not get configured by Lan automation. Issue caused by cdp limitation <u>CSCvp73666</u>. Workaround is to reduce the hostname for peer/secondary seed to less than 40 characters and resync. Note this will not affect the primary seed. Even if primary seed hostname is greater than 40 characters, links connecting to the primary seed will still get configured
- Delete and re-add the lan automated device (Seed or edge) via inventory or discovery will complain ip address overlaps during subsequent Lan Automation. Workaround : Bring back the device into DNAC via Lan Automation. <u>CSCvr78668</u> <u>CSCvr77659</u>
- After upgrade to DNAC 1.3.1.3 Lan Automation will not work if any previous Lan automation had ISIS password configuration.<u>CSCvr89951</u>

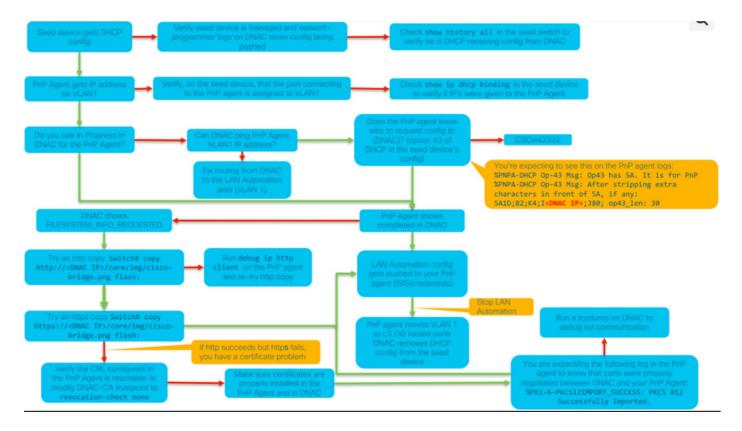
## What's new in DNA Center 1.3.0

- New device support
  - Support for 9400 40G port
  - Support for 9500 high performance as both seed and PnP agent
  - Support for 9600 as both seed and PnP agent
- Configuring /31 point to point link addresses rather than /30 thus saving on unused IP addresses
- Validation of LAN subnet reachability from DNA Center

 If DNA Center has no route to the LAN pool, error will be reported under LAN automation status field as "Error: Unreachable primary device on the LAN subnet" (To fix the LAN subnet reachability, refer to section 'Steps to consider before LAN auto' step 1a and 1b)

## Troubleshooting

Below is high level flow from the time Lan automation is started.



DNA Center 1.2 Ian automation relevant logs

- network-orchestration
- connection-manager-service
- onboarding-service (this is the old pnp-service equivalent from 1.1)