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

Contents

[What's new in DNA Center 1.3.0]
[Troubleshooting]
The customer facing document can be found here: 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

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 intial 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

1. Understanding system roles.

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

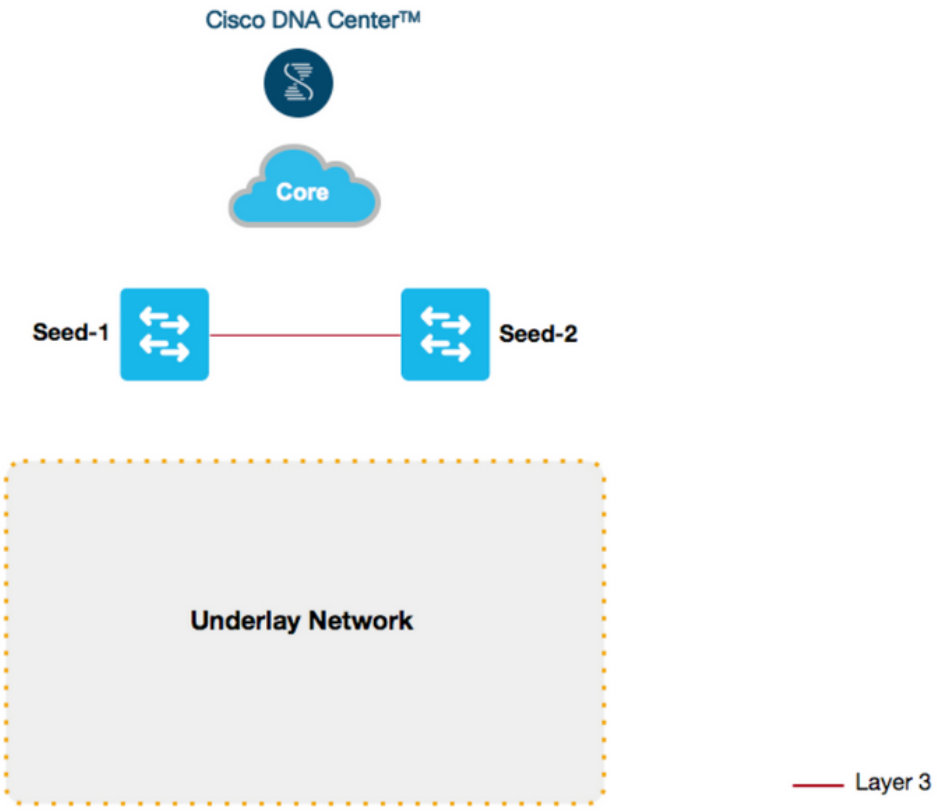
Understanding system roles

Primary Device

The primary device is a pre-deployed network device in the network and is the intial 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.

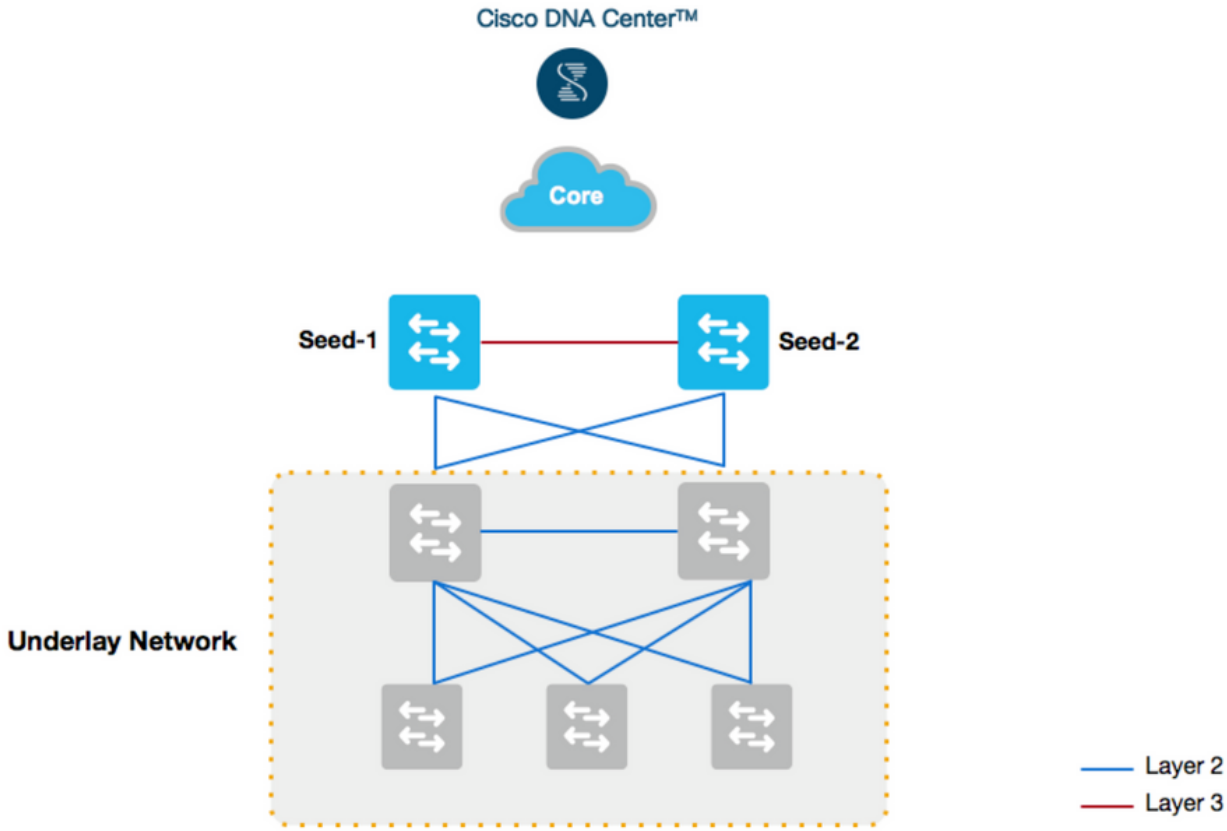
Figure 1 - Seed device role



PnP-Agent Device

The PnP-Agent is a Cisco Catalyst switch with factory-default settings. The switch leverages built-in 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.

Figure 2 - PnP agent device role



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:

1. 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

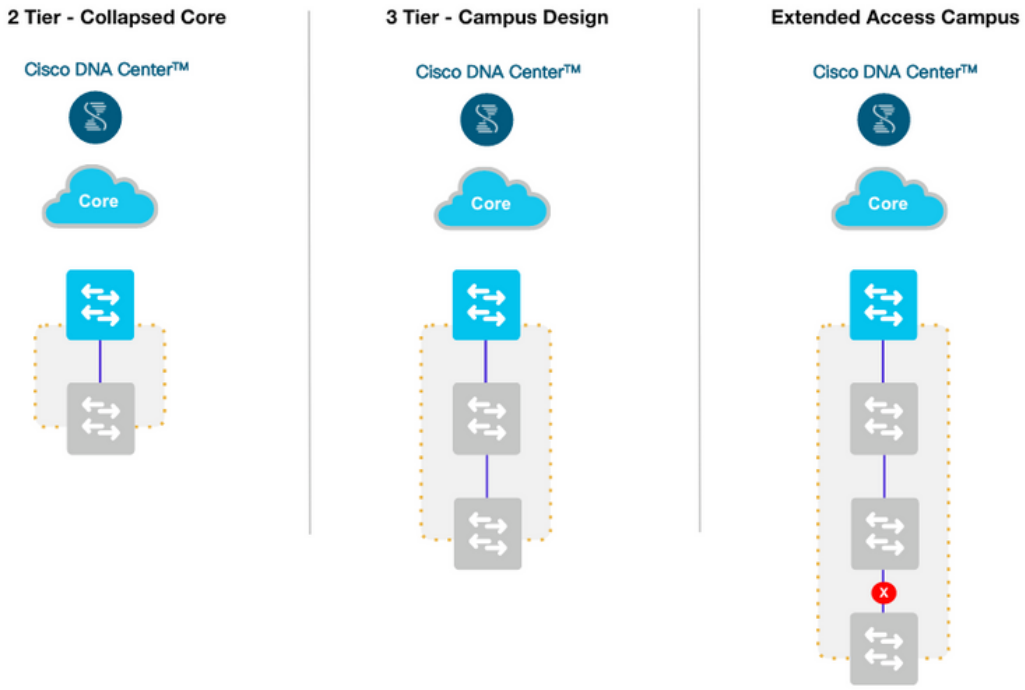
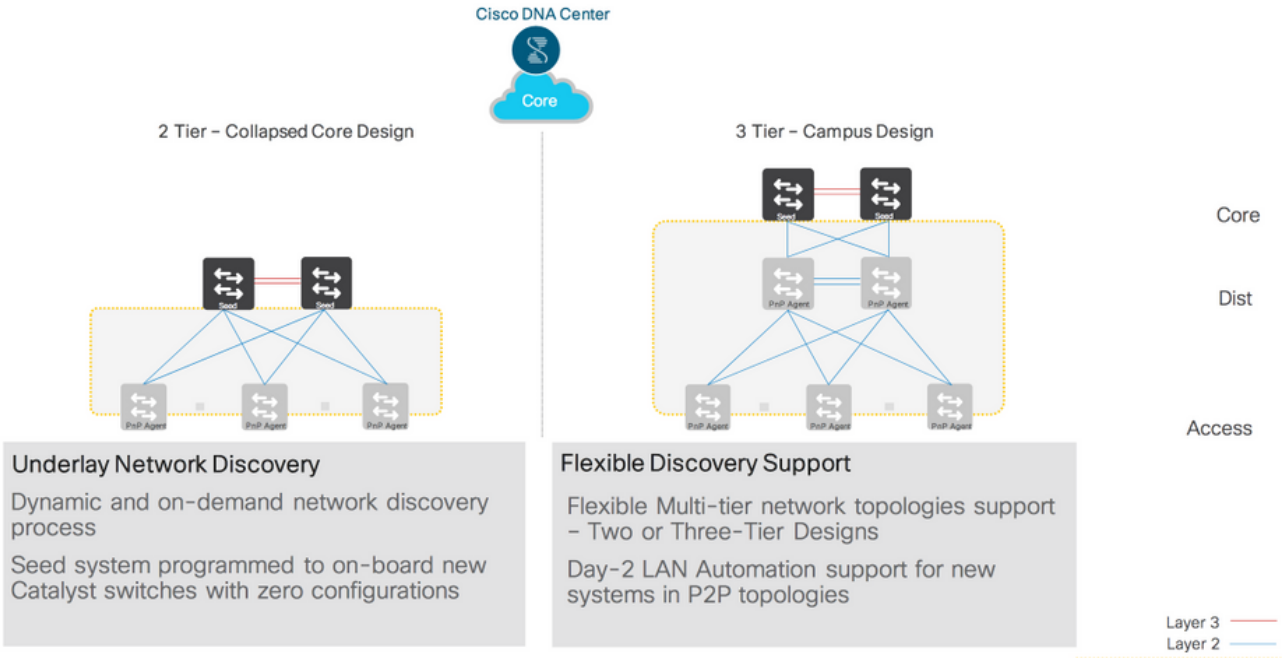
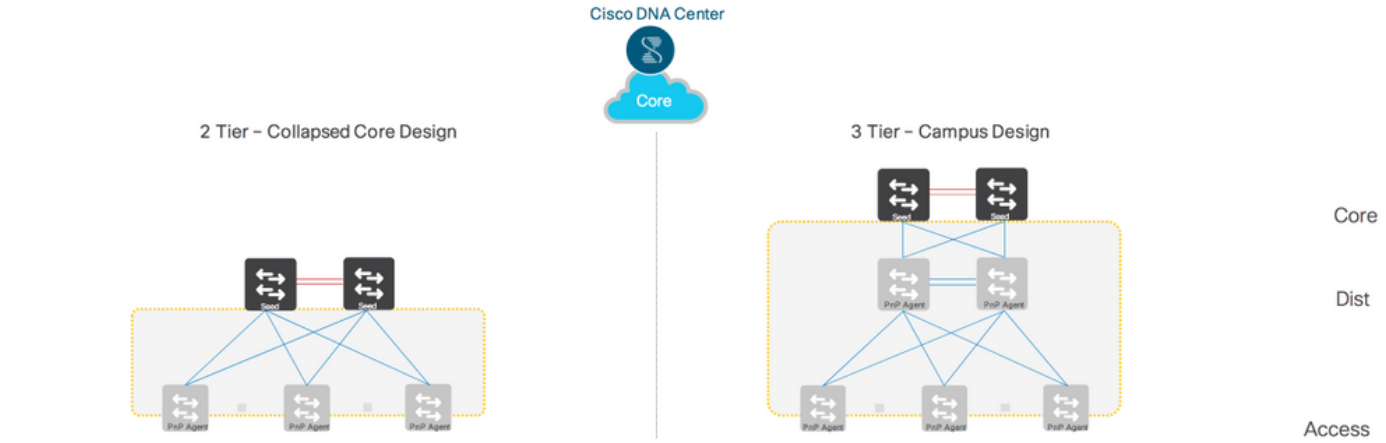


Figure 4 - Tier-2 and Tier-3 network design



Supported switches for each role at different layers

Figure 5 - Supported device family for primary and PnP-agent at different layers



Layer	Role	Supported Switch
Distribution	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[1]	IOS version	DNA Center
Seed PnP-Agent	C9500-32C C9500-32QC C9500-24Y4C C9500-48Y4C		16.11.x onwards	1.3 onwards
Seed PnP-Agent	C9500-12Q C9500-24Q C9500-40X C9500-16X	Any Front Panel Ports[2]		
Seed PnP-Agent	C9404R C9407R C9410R	Sup-1[3] Sup-1XL[3] Sup-1XL-Y[3] Any Line Card		
Seed PnP-Agent	C9300-24T C9300-24P C9300-24U C9300-48T C9300-48P C9300-48U C9300-24UX C9300-48UXM C9300-48UN	Any Uplinks and Modules Ports		
Seed PnP-Agent	C9200L-24T C9200L-24P C9200L-48T C9200L-48P	Any Uplinks and Modules Ports		1.2.8 onwards
Seed	C6807-XL	Sup6T 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[3] Sup8-E Any Uplinks and Modules Ports
Seed PnP-Agent	WS-C3850-24T WS-C3850-48T WS-C3850-24P WS-C3850-48P WS-C3850-48F WS-C3850-24U WS-C3850-48U WS-C3850-24XU WS-C3850-12X48U WS-C3850-12S WS-C3850-24S WS-C3850-12XS WS-C3850-24XS WS-C3850-48XS	Any Uplinks and Modules Ports
Seed PnP-Agent	WS-C3650-24TS WS-C3650-48TS WS-C3650-24PS WS-C3650-48PS WS-C3650-48FS WS-C3650-24TD WS-C3650-48TD WS-C3650-24PD WS-C3650-24PDM WS-C3650-48PD WS-C3650-48FD WS-C3650-8X24PD WS-C3650-12X48FD WS-C3650-48TQ WS-C3650-48PQ WS-C3650-48FQ WS-C3650-48FQM WS-C3650-8X24UQ WS-C3650-12X48UQ WS-C3650-12X48UR WS-C3650-12X48UZ	Any Uplinks and Modules Ports

[1]= Dedicated Management Port is unsupported in Cisco LAN Automation

[2]= 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 Vlan 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)

- Running multiple discovery sessions for devices across sites connected to same seed: 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
- Endpoint/client integration: Similarly, if there are clients conneted to a swicth that is being discovered, those clients will also contend for DHCP IP and may exahust the pool causinglan auto to fail. Its receommended 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.

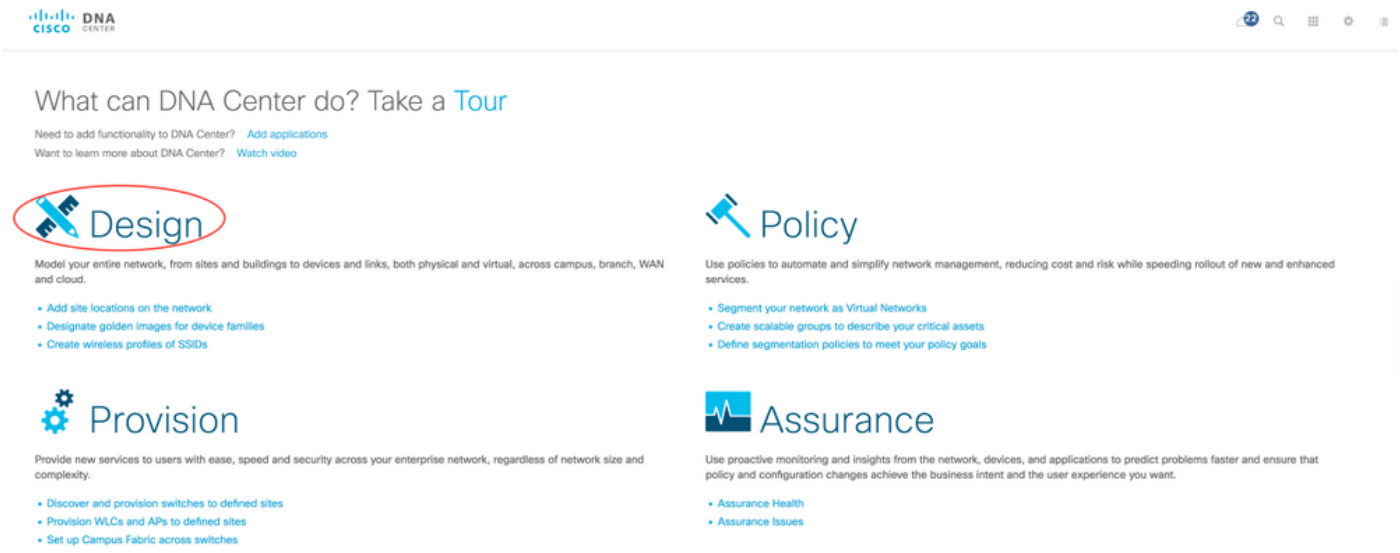
  - Bring the device to factory defaults by clearing the following from the swicth console

[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 | 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)

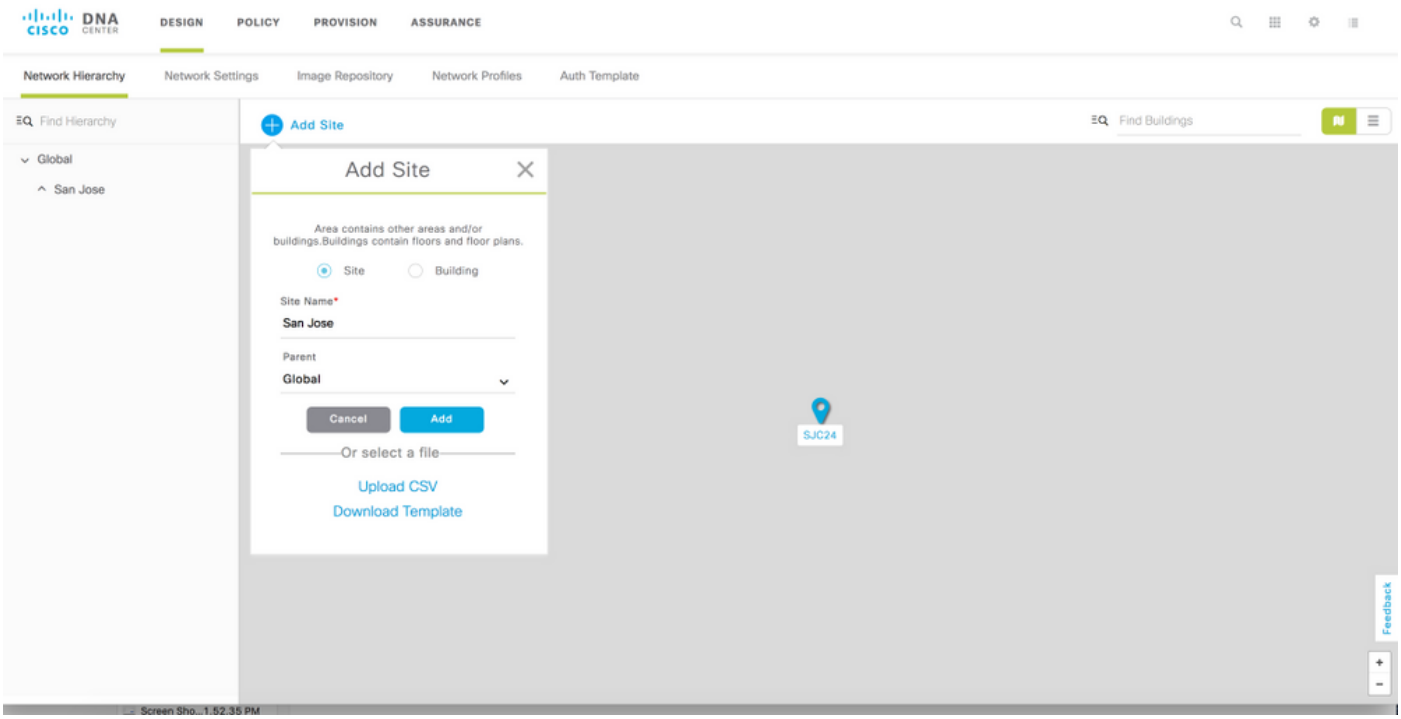
Design

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



Navigate to Design -> Network Hierarchy

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



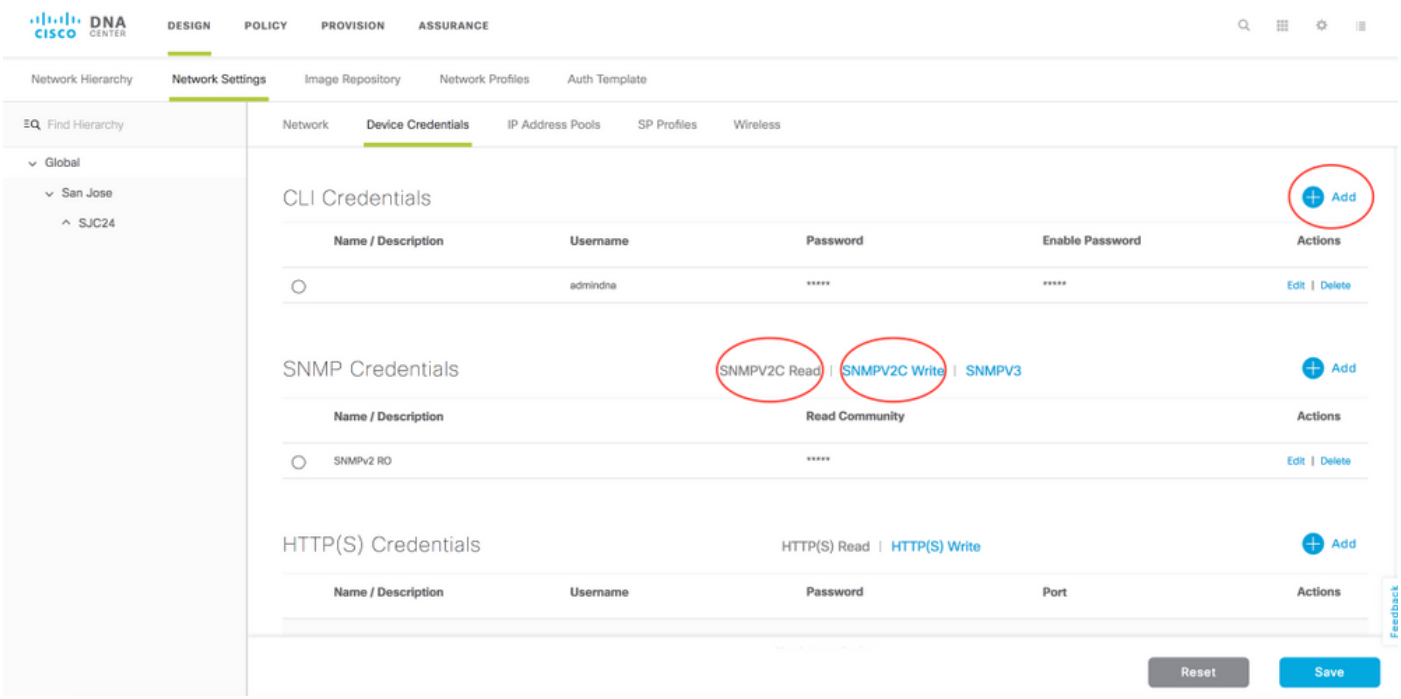
Navigate to Design -> Network Settings -> Device Credentials

- 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

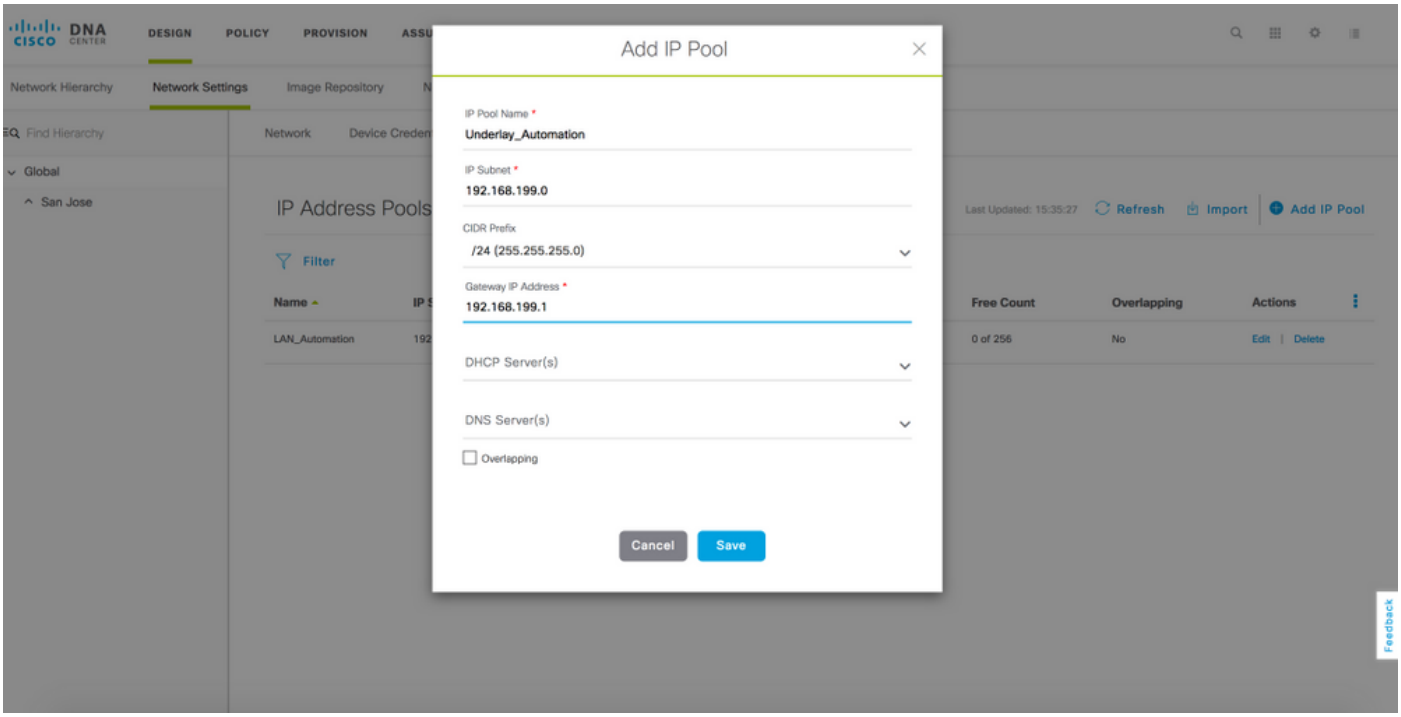
Note: Enable Password is mandatory for now. This is being addresed by CSCvm15743 after which enable password will not be mandatory

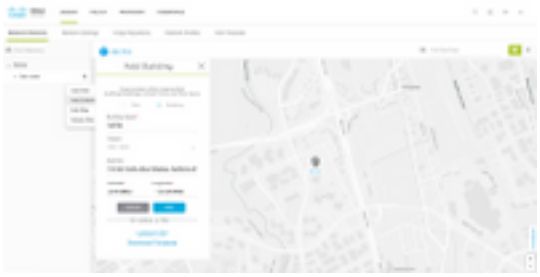


Navigate to Design -> Network Settings -> IP Address Pools

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

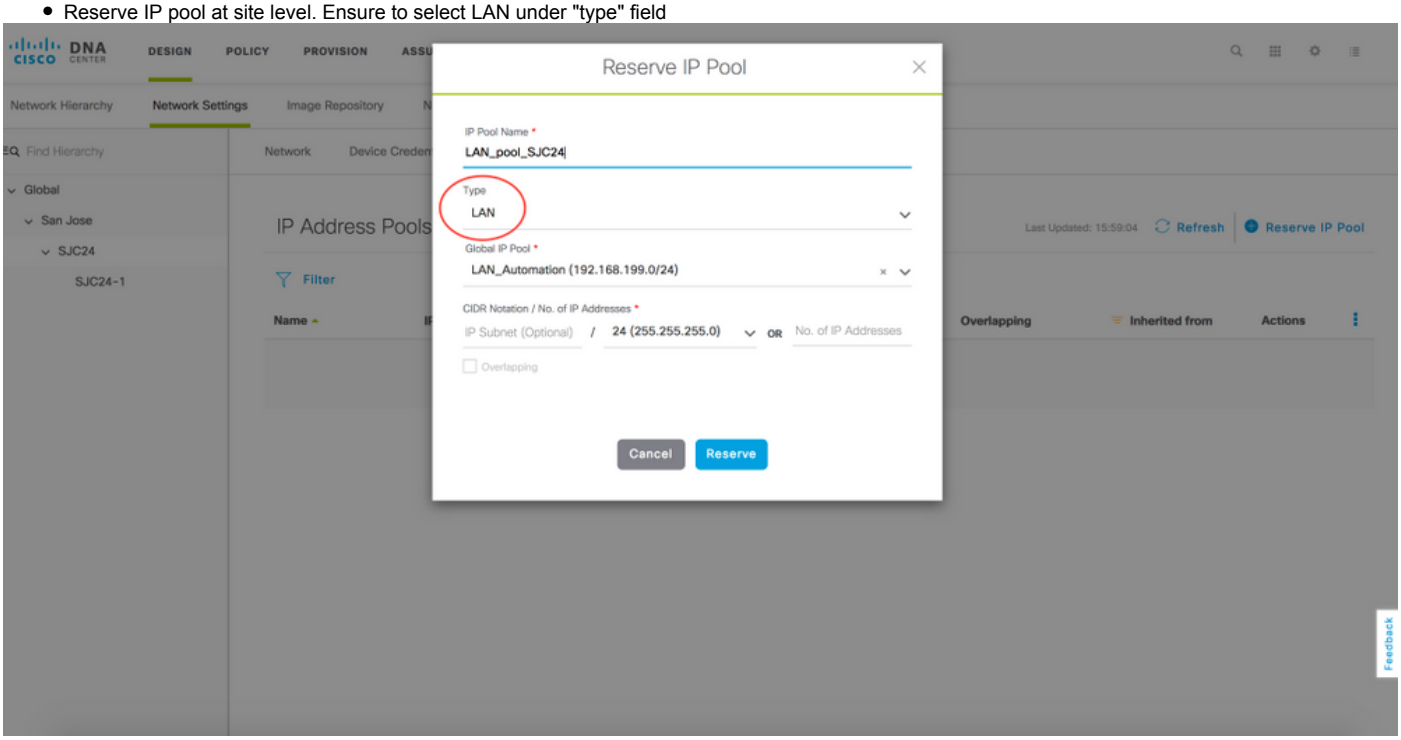
Note: Don't use address pool that is being used elsewhere in the network such as address pool belonging to loopback or other addresses configured on the device.





Next Navigate to DNAC → Design → Network Settings → Site → Click the Reserve IP Pool

- 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

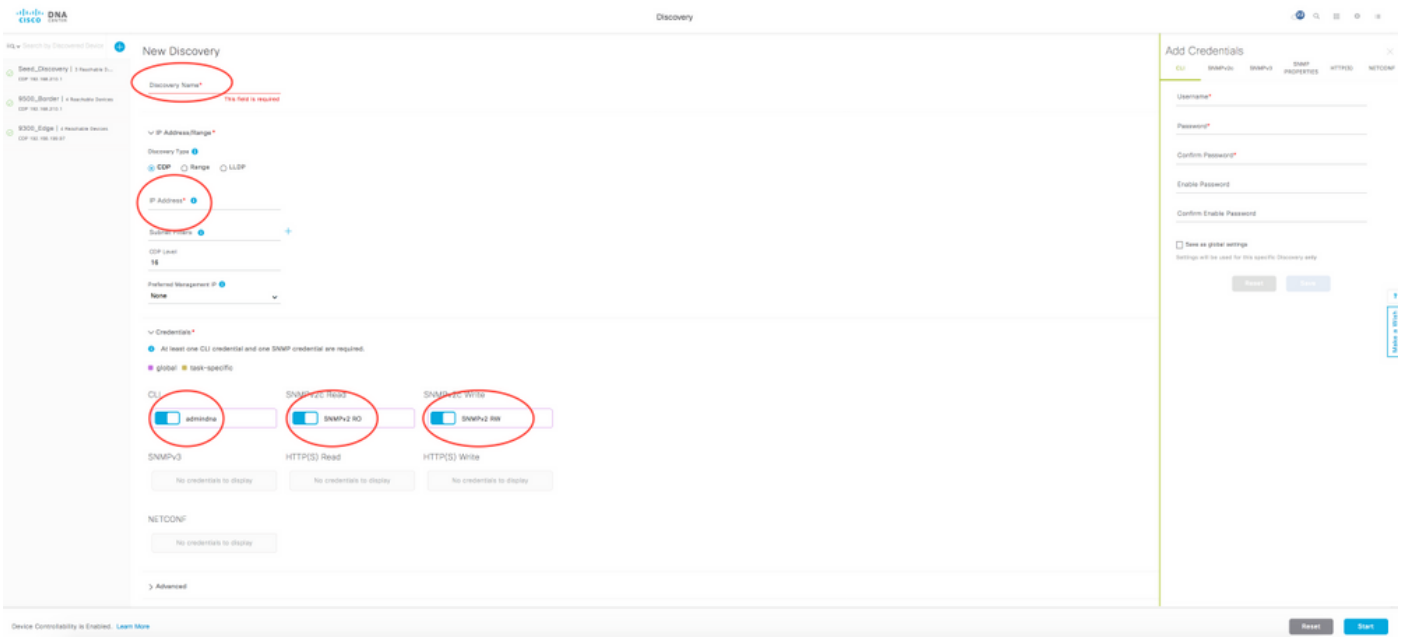
  - Discovery Name

  - 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)

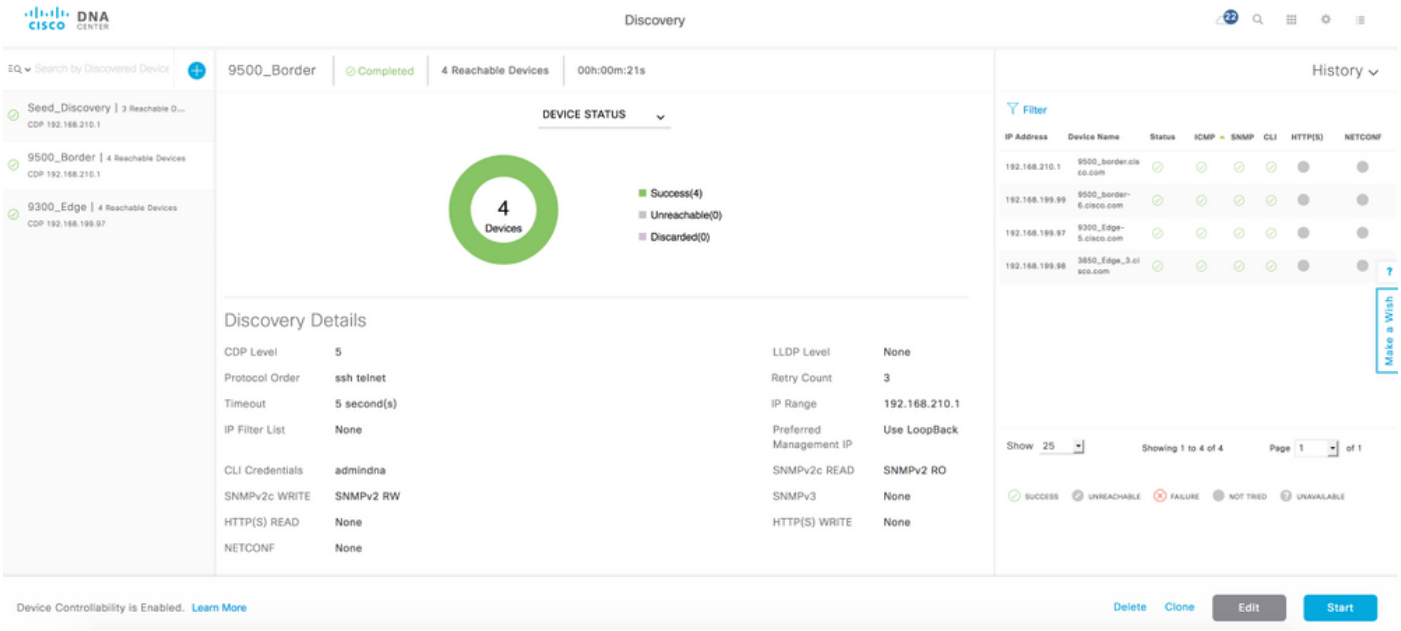
  - Credentials (Enable the CLI and SNMP credentials that you created in Step1)

  - Advanced - Choose SSH and/or Telnet (ensure the seed is configured for ssh)

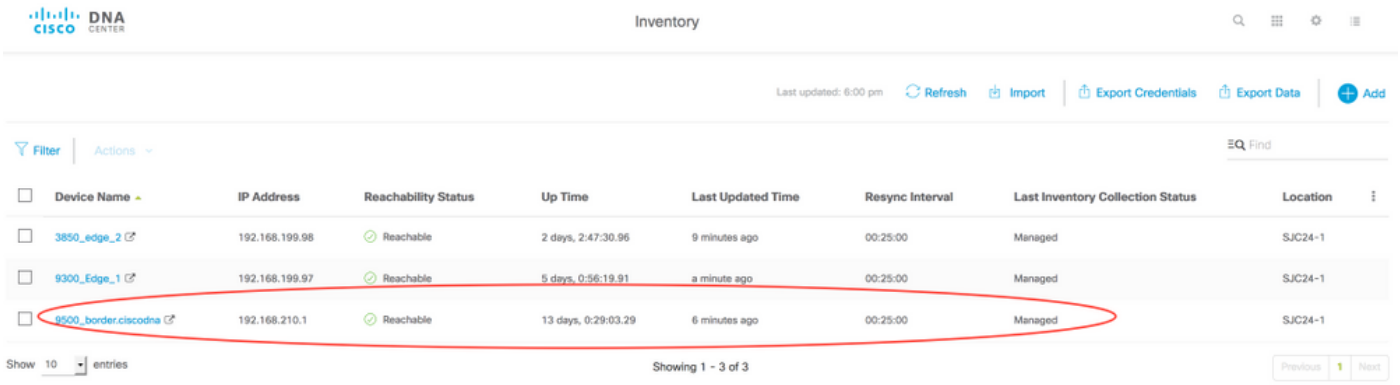
- Click on Start. Once the discovery starts, the page will present the discovery settings and details.



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

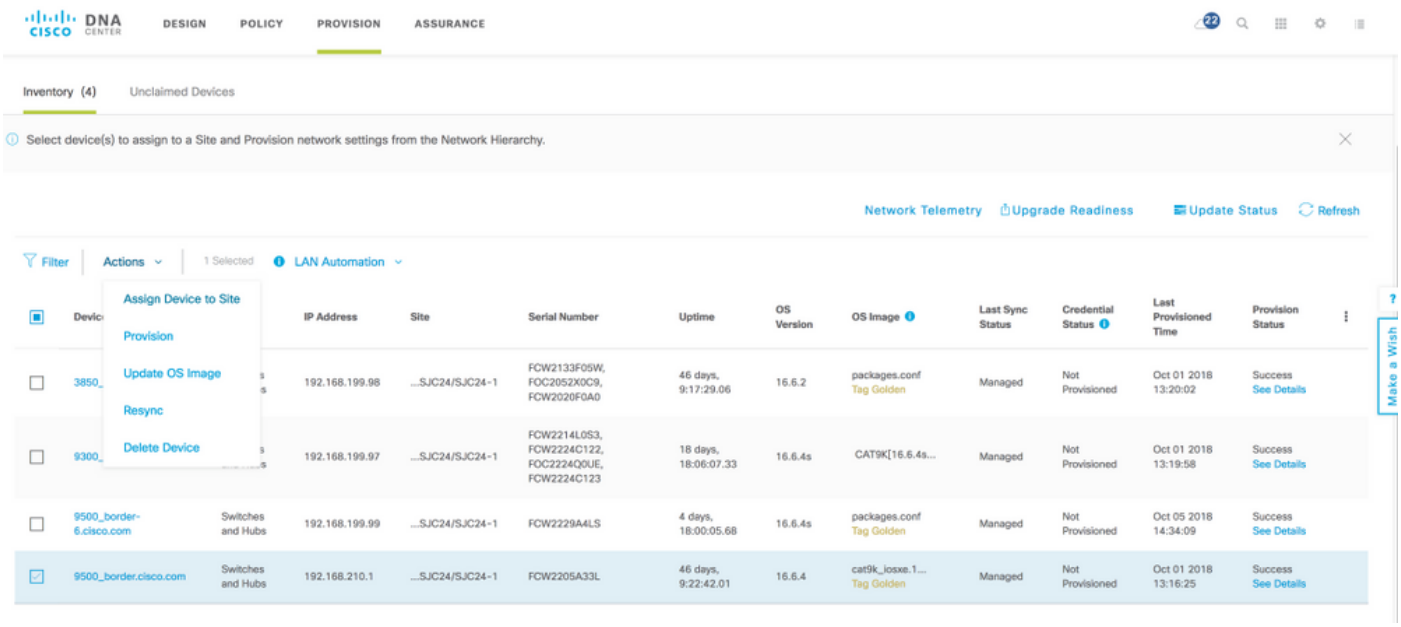


- Next, navigate to inventory page and verify the discovered device was added. When you enter the Device Inventory page all the devices should have the “Device Status” set as “Reachable” and “Last Inventory Collection Status” as “Managed

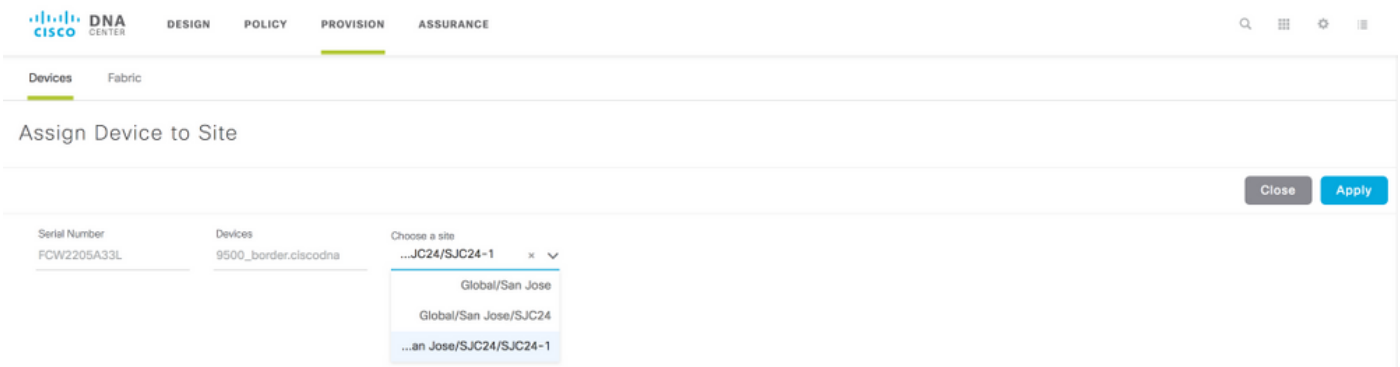


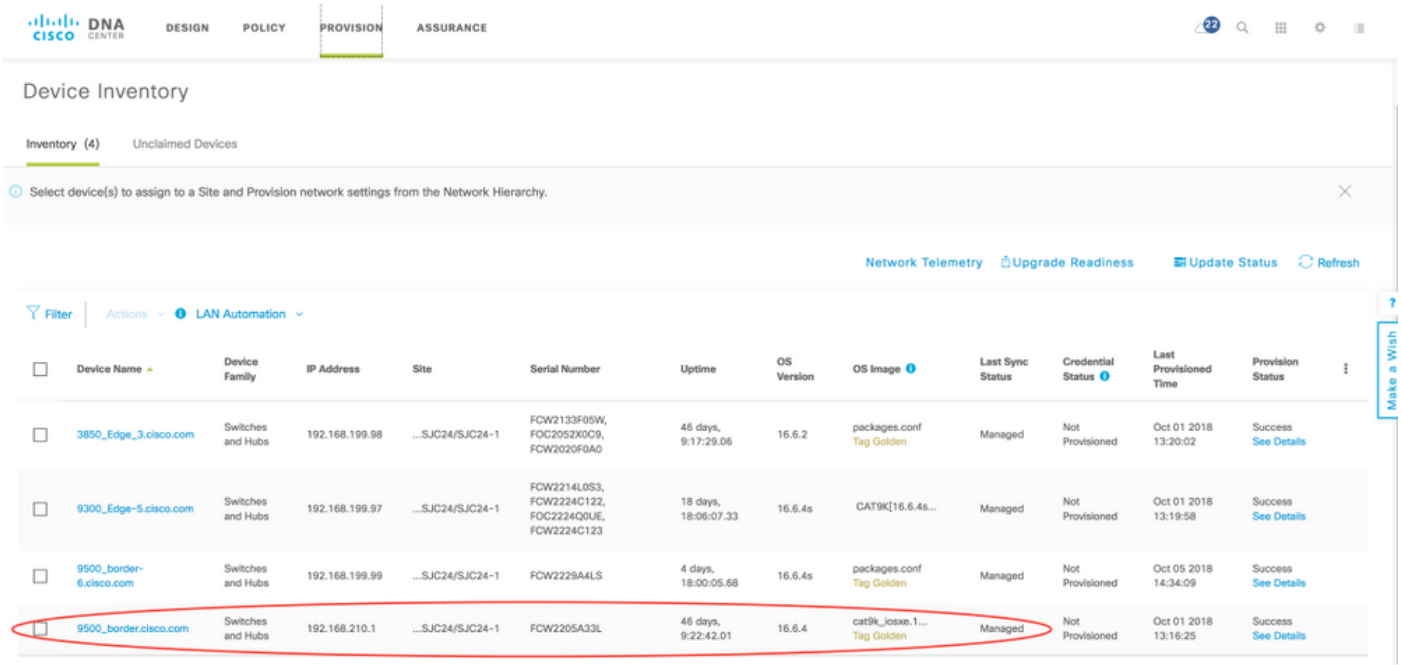
- Once in Managed state, add the discovered seed to the same site. Navigate to Provision -> Devices -> Inventory. Select the device and under Actions, click on "Assign Device to Site"

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)

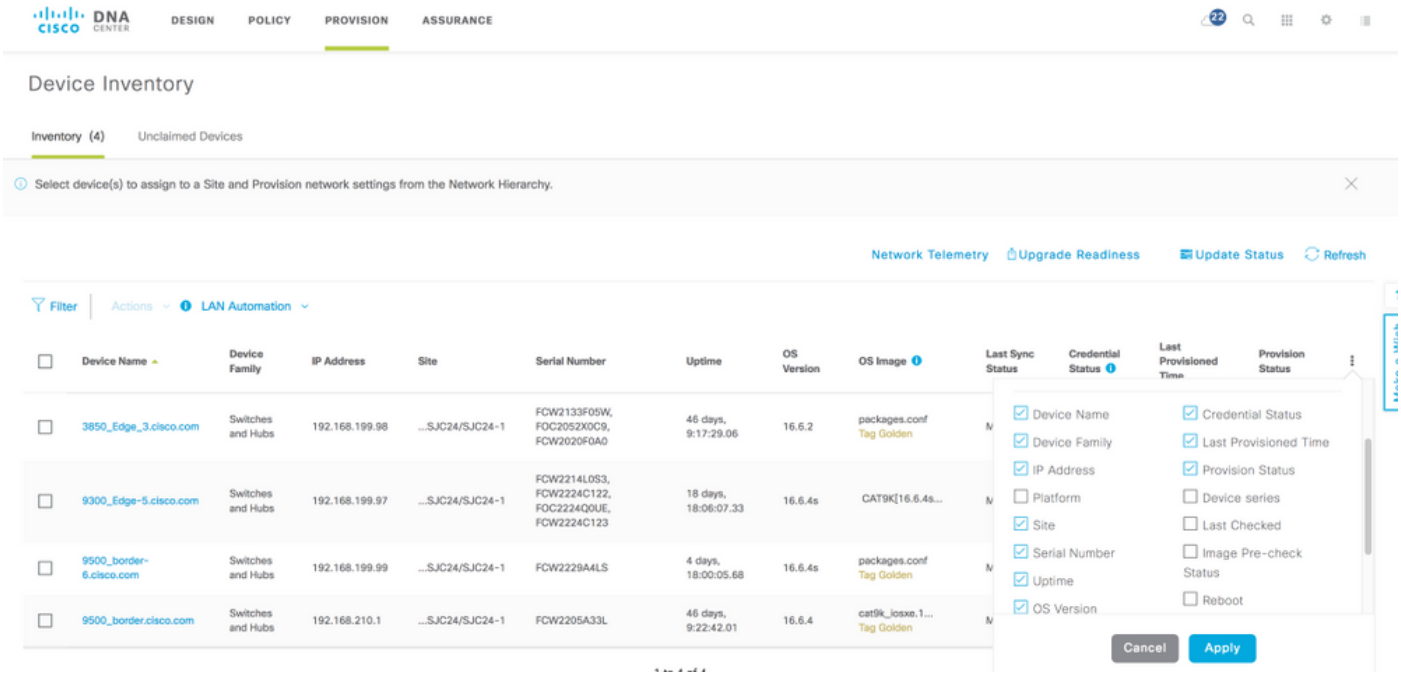


- On next page, select the site and click Apply





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



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

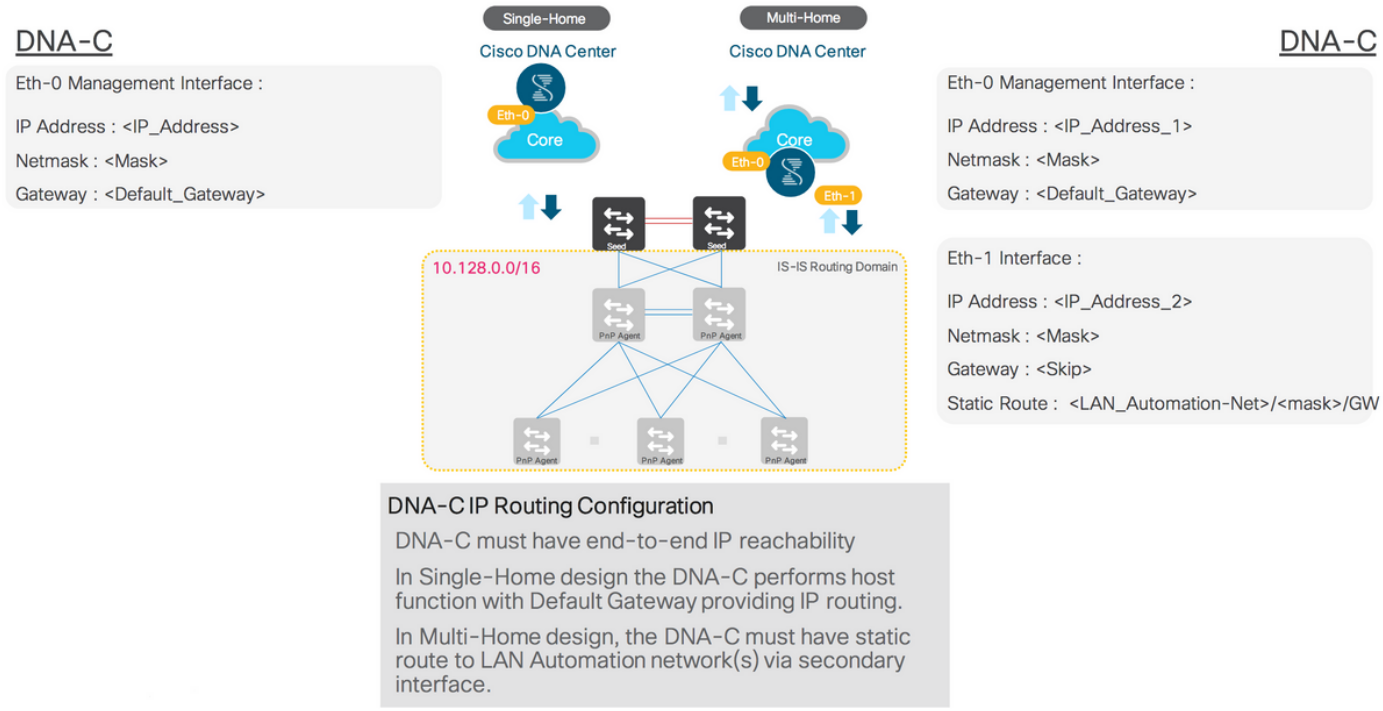
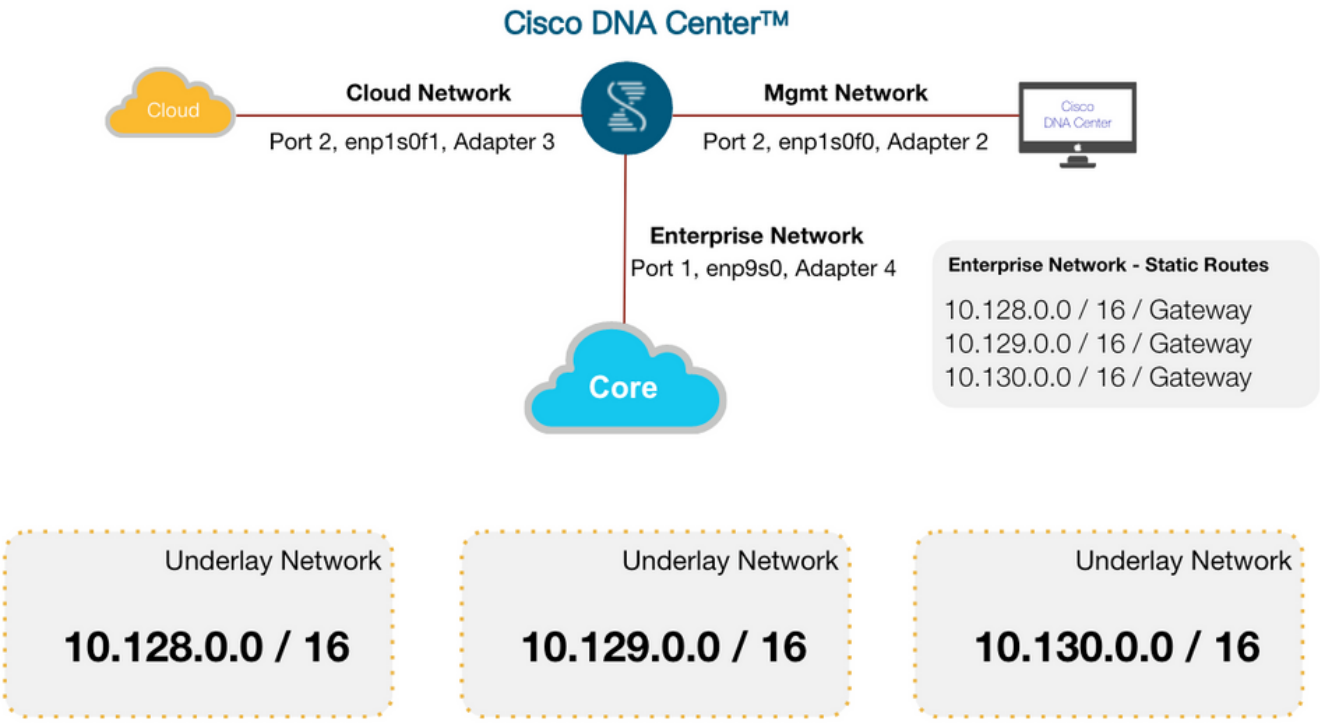


Figure 7 - DNA Center Static IP routing design



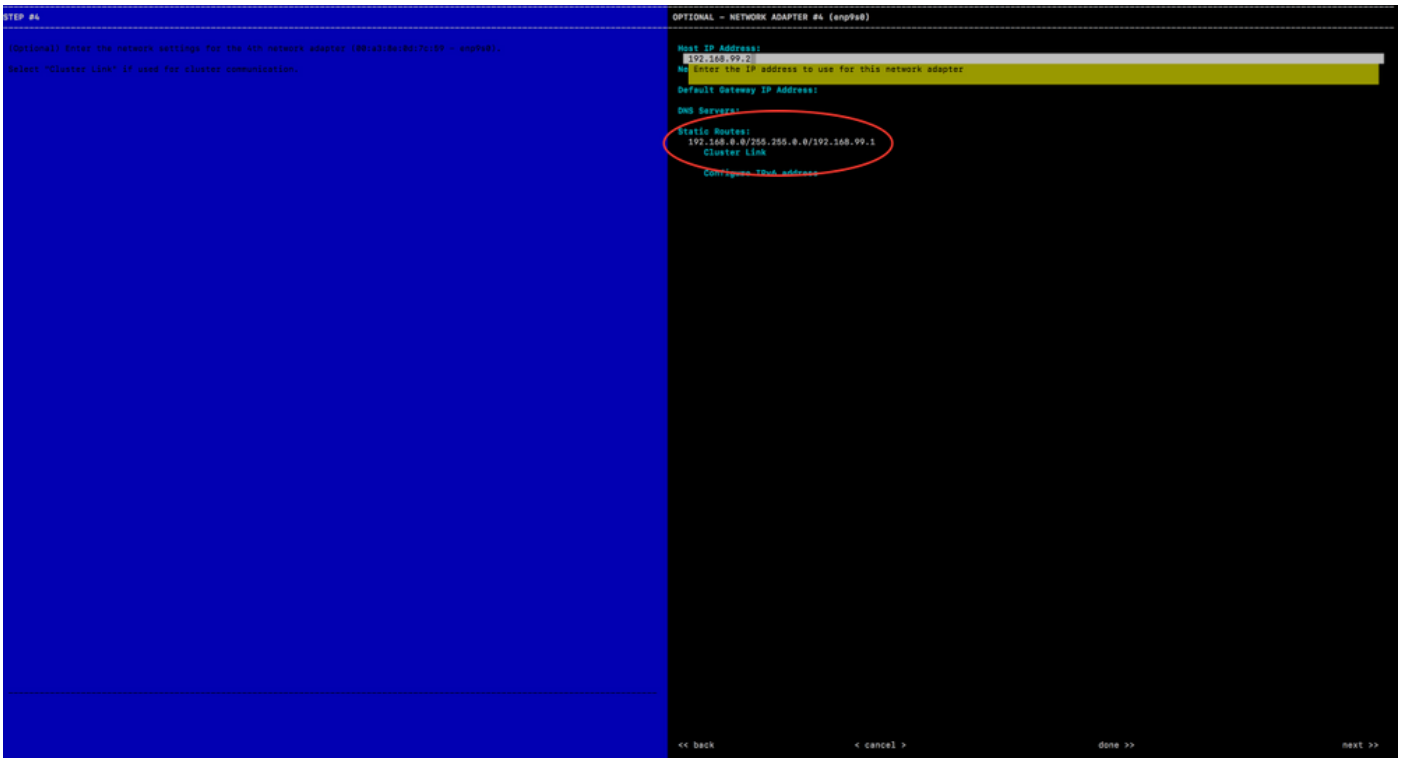
One way to fix the IP reachability issue is by adding a static route in DNAC in case of multi-home design. This can be done by network administrator during intial DNA Center configuration or later via maglev command (Don't use linux route command as maglev APIs don't pick the correct information if the 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 Number : 73-17952-06
Motherboard Serial Number : FOC21354B06
Model Revision Number : A0
Motherboard Revision Number : 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 swicth 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 swicthes 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

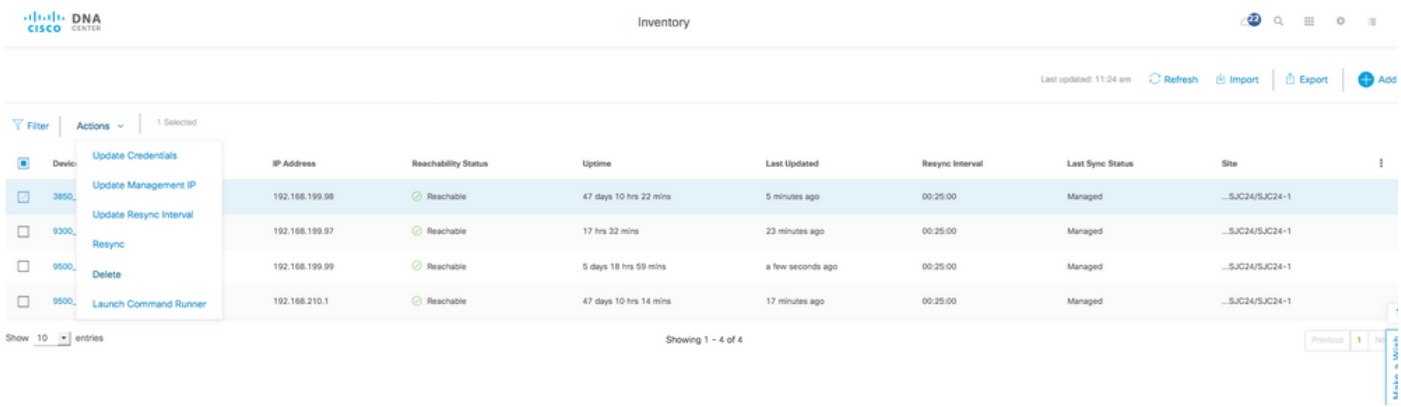
- Make sure the seed ports connected to the PNP-agents are layer 2 and defaulted. Example catalyst 6500 and 9500H ports are layer 3 by default

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

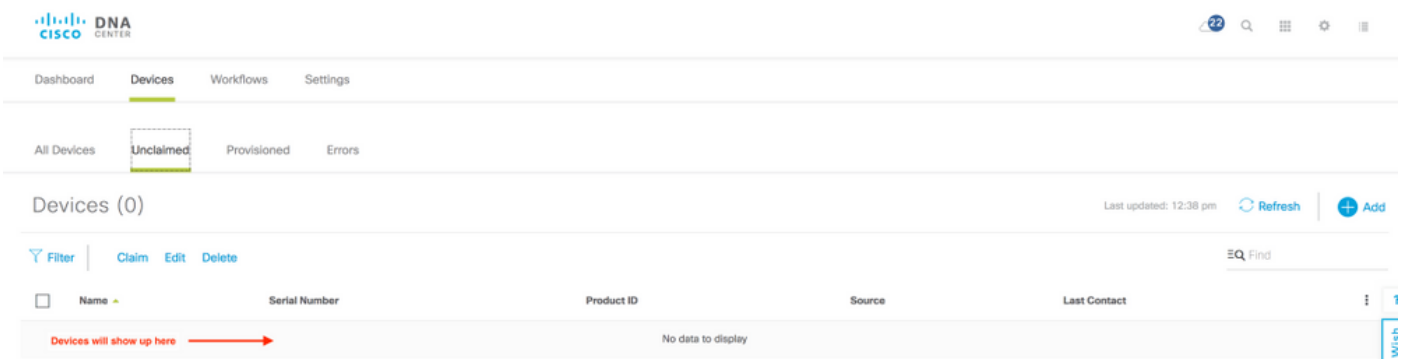
- If the device(s) to be discovered in upcoming LAN automation session are already present in inventory, then they should be removed from invmtoery first
- Navigate to Inventory from the home page. Filter the device by the serial number and click on Actions->Delete. Note if the device was provisioned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



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"



- 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 intial 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 Layer 3.
- All temporary DHCP and vlan 1 configuratrion 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.

Interface selection:

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 PNP-agents 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 PNP-agents 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.

ISIS password:

- 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

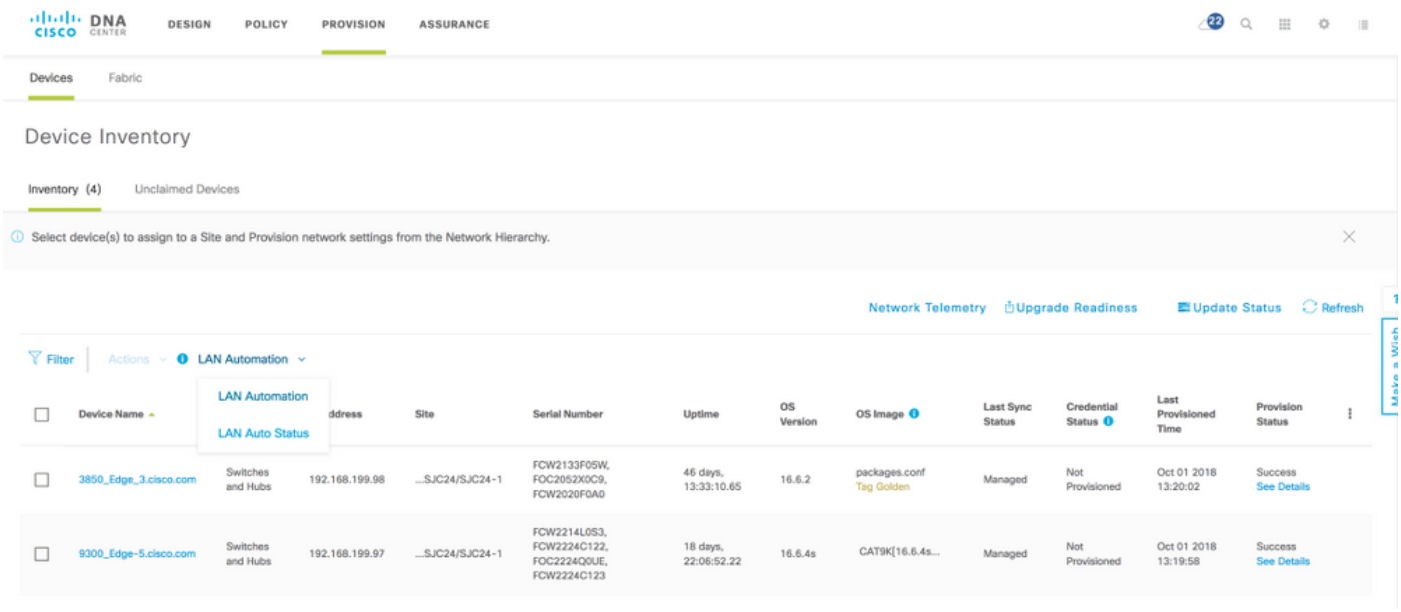
Case2: User leaves ISIS password field blank
2a. If primary seed has an ISIS password configured, then LAN Automation will configure primary seed's ISIS password on the PnP devices (and peer seed if it did not have the password already)
2b. If primary seed doesn't have an ISIS password but peer has, 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:

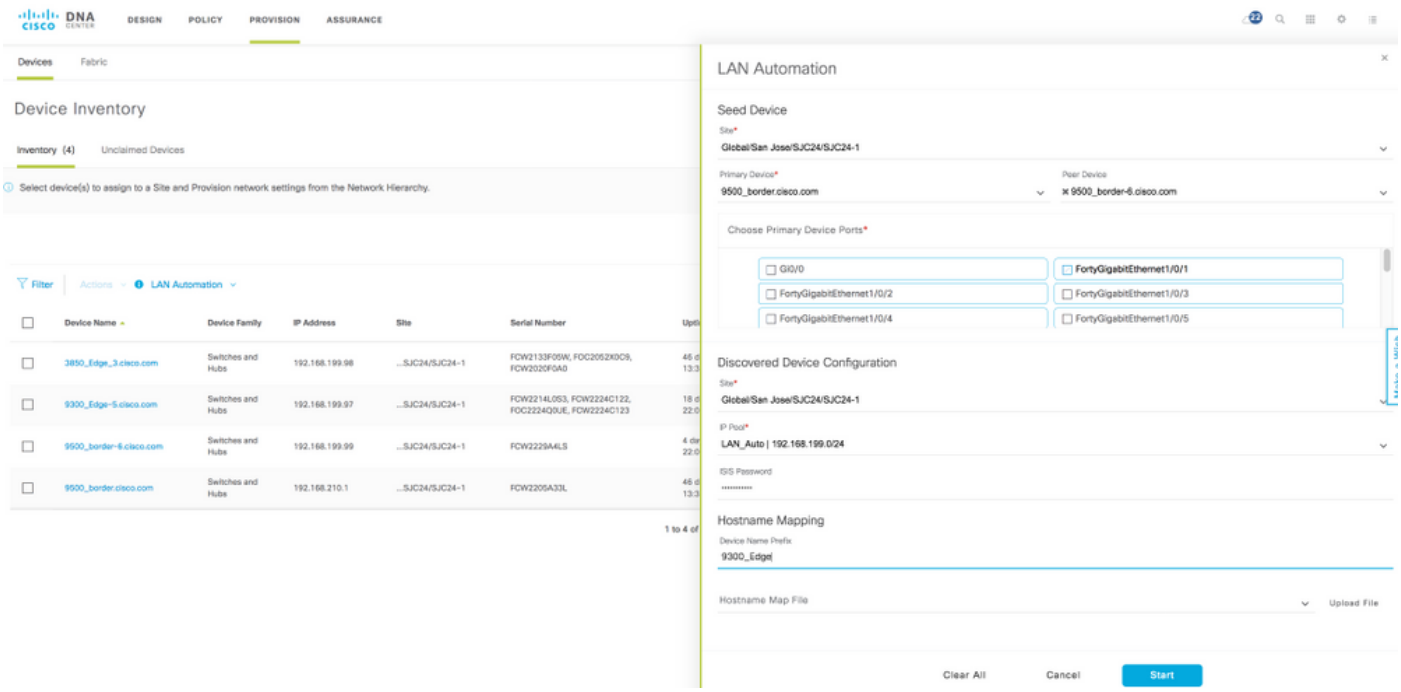
- **Default**: If no value is entered, Lan automation will set hostname as Switch followed by loopback address. Example: Switch-192-168-199-100
- **Device Name Prefix**: Device prefix is used for generating the hostnames for discovered devices. LAN automation keeps site counter and generates the name 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	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

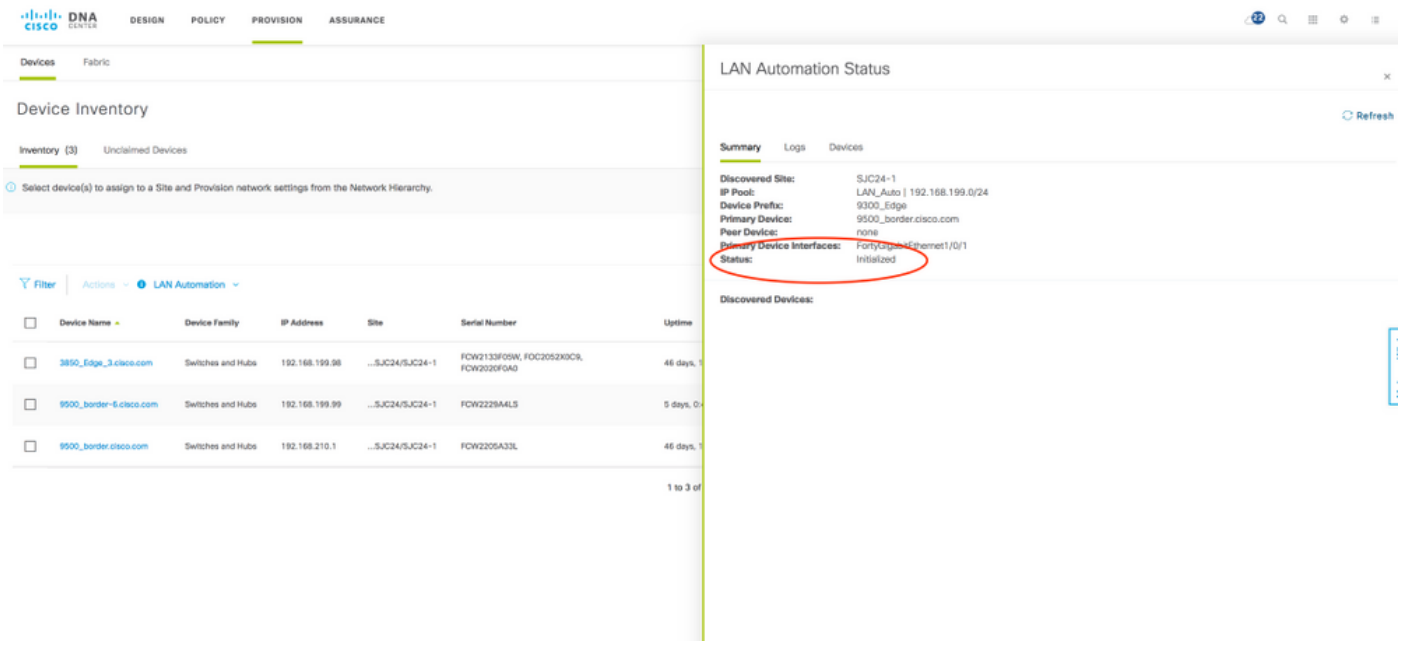
Navigate to Provision → Devices and click the 'Lan Automation' Icon



Next, fill in the values explained above and click start



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



- Once LAN Automation is started, below sample configuration gets pushed to the seed device(s)

Primary Seed Configuration

```
!exec: enable
!
system mtu 9100
!
ip multicast-routing
ip pim ssm default
!
```

Loopback IP and ISIS Configuration (If secondary seed is configured, it is also gets configured with loopback ip and isis config)

```
interface Loopback0
   ip address 10.4.210.123 255.255.255.255
   description Fabric Node Router ID
 !
router isis
   net 49.0000.0100.0421.0123.00
   domain-password *
   ispf level-1-2
  metric-style wide
  nsf ietf
   log-adjacency-changes
   bfd all-interfaces
   passive-interface Loopback0
   default-information originate
 !
 interface Loopback0
 ip router isis
clns mtu 1400
ip pim sparse-mode
 exit
 !
```

DHCP Pool Information

Secondary Seed Configuration

```
!exec: enable
!
system mtu 9100
!
ip multicast-routing
ip pim ssm default
!
 interface Loopback0
  ip address 10.4.210.124 255.255.255
  description Fabric Node Router ID
!
 router isis
   net 49.0000.0100.0421.0124.00
   domain-password *
   ispf level-1-2
   metric-style wide
   nsf ietf
   log-adjacency-changes
   bfd all-interfaces
   passive-interface Loopback0
   default-information originate
!
interface Loopback0
ip router isis
clns mtu 4100
ip pim sparse-mode
exit
!
```

```
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
 !
 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
 !
```

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
```

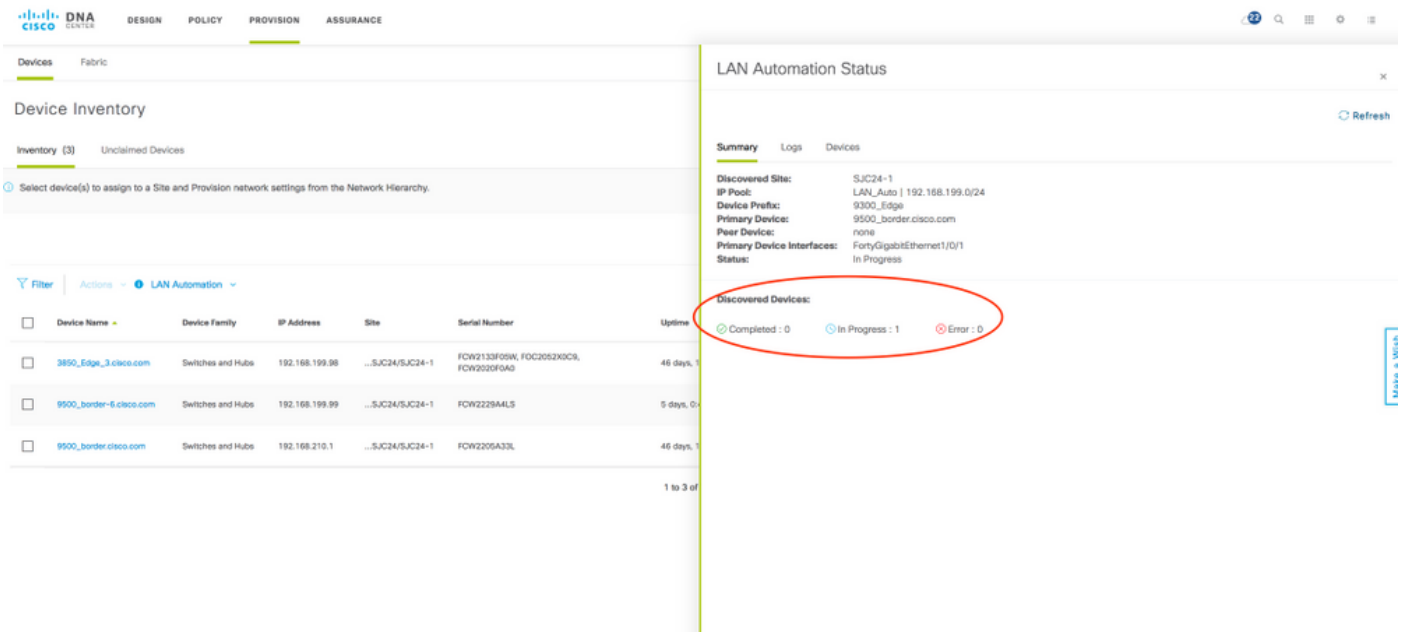
- After this device discovery happens and you will see some logs on the PNP-agent (Do not enter return on PNP-agent as yet)

%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/network-confg (Timed out) Aug 2 23:14:25.263: AUTOINSTALL: Tftp script execution not successful for Vl1.

- 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-cc_srdriver.16.06.04s.SPA.pkg,cat9k-espbase.16.06.04s.SPA.pkg,cat9k-guestshell.16.06.04s.SPA.pkg,cat9k-rpbase.16.06.04s.SPA.pkg,cat9k-sipbase.16.06.04s.SPA.pkg,cat9k-sipspa.16.06.04s.SPA.pkg,cat9k-srdriver.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...
```

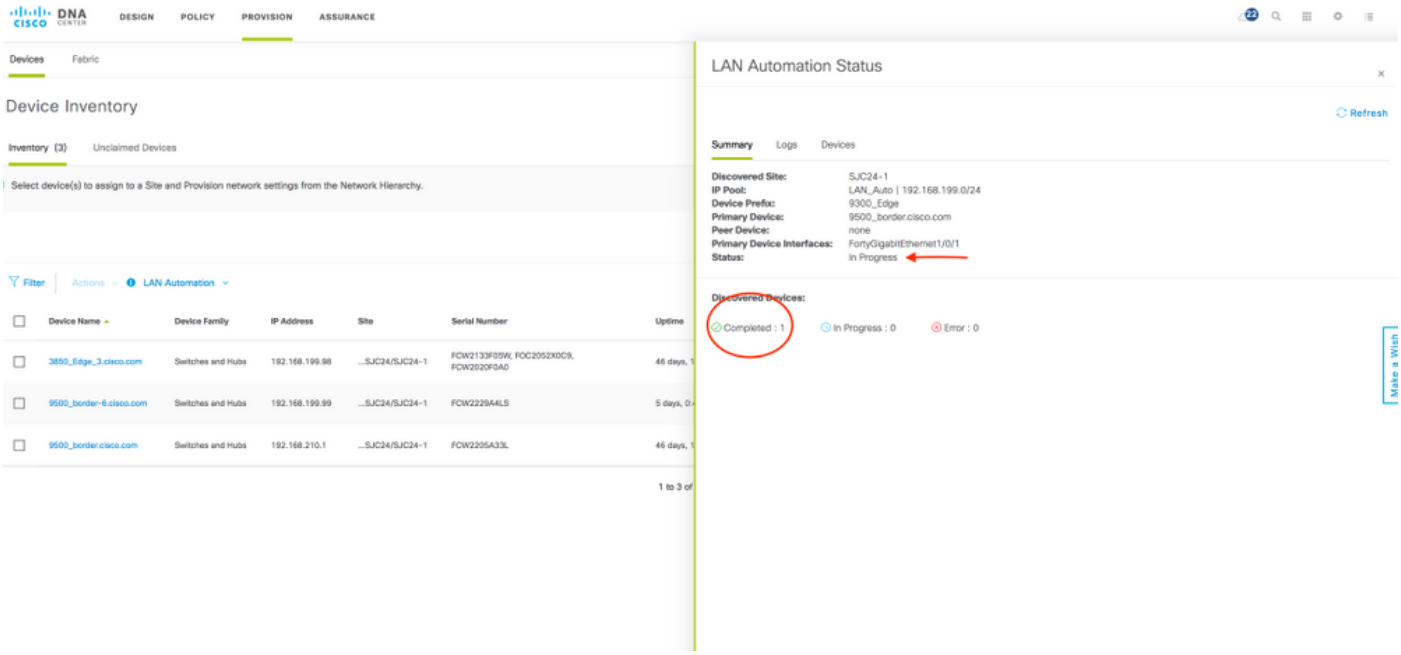
- Next, DNA Center will push part of configuration allowing devices to get on-boarded and managed by DNAC. LAN Automation Status will show "In Progress", Discovered Devices status will show aggregate status of all devices being discovered, and "Devices" tab will show status of individual devices being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

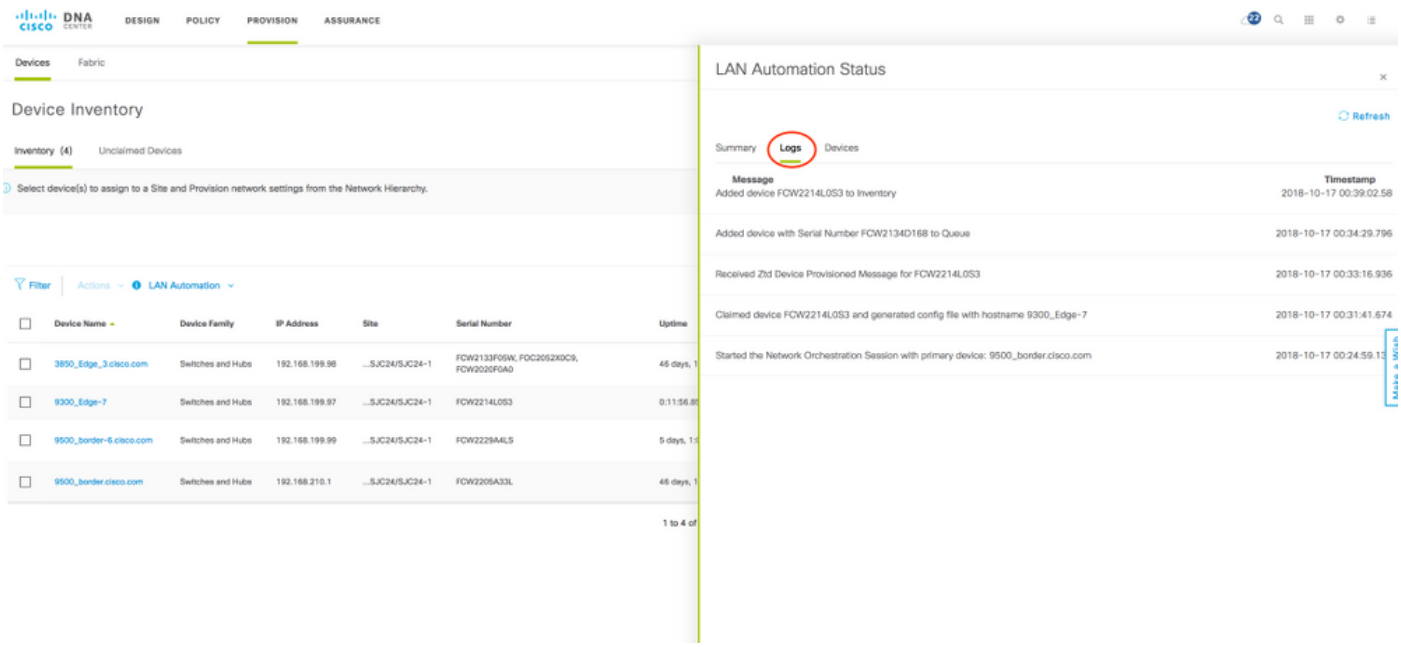


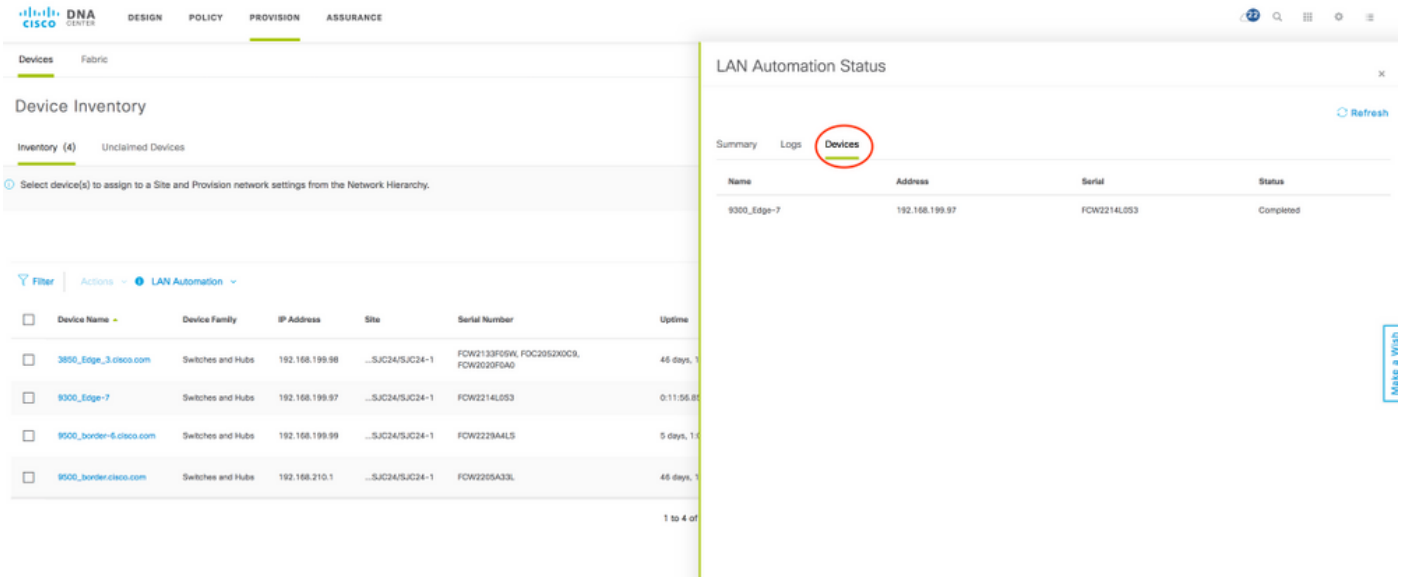
- During this time, you will see logs like below on the PNP-agent. At this point it is safe to press return on the console if you wish to. When you press return, you will see that hostname has changed to the value entered at "Hostname Mapping" when starting LAN auto

```
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
Aug  2 23:14:52.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24,
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

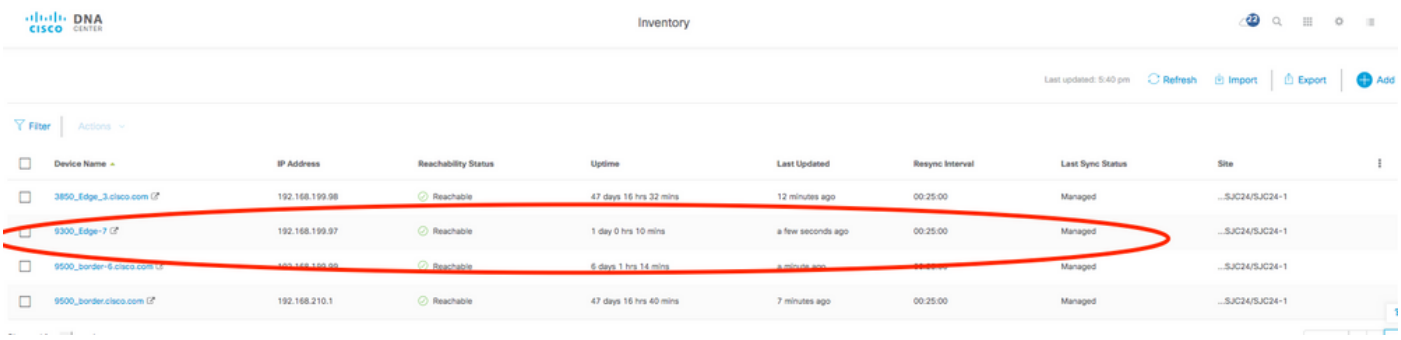






Navigate to Inventory and filter by the serial number. The newly discovered switches will show up

as 'Managed'



Below sample config is pushed to Discovered Device(s)

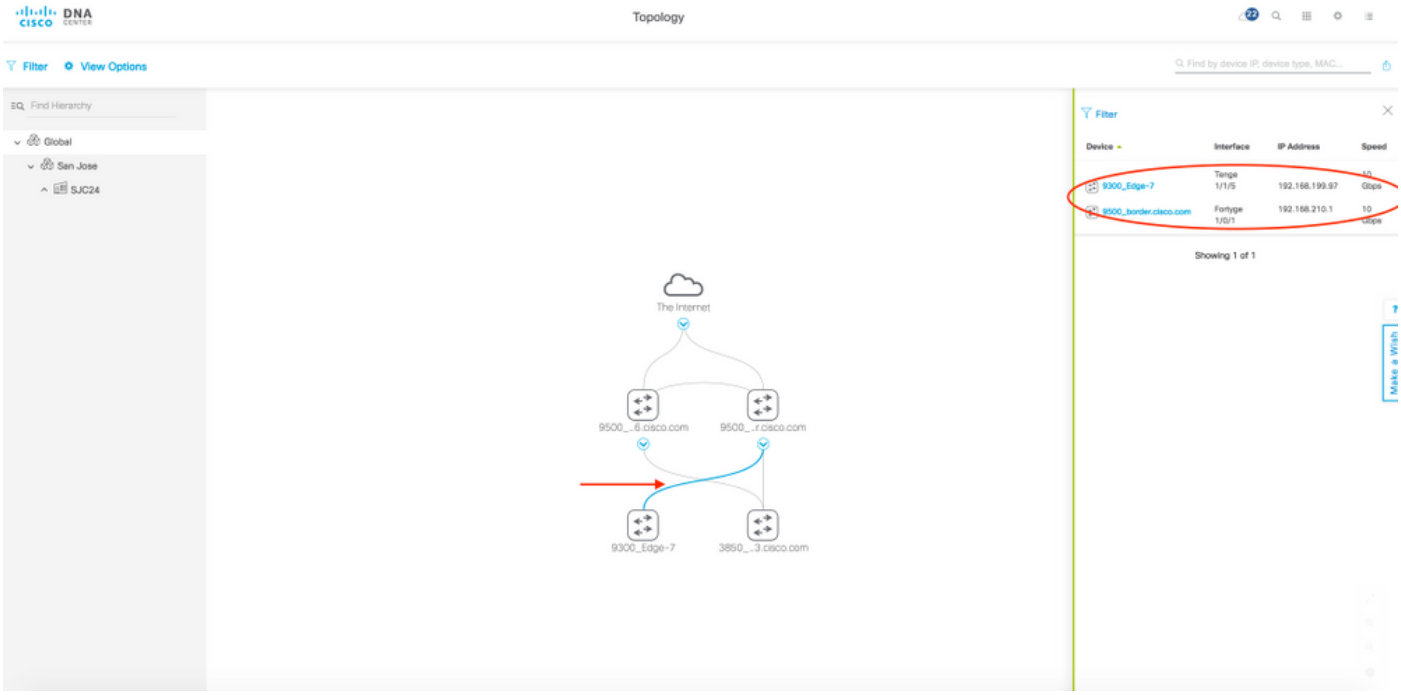
```
!
archive
log config
logging enable
logging size 500
hidekeys
!
!
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
service password-encryption
!
service sequence-numbers
!
! Setup NTP Server
! Setup Timezone & Daylight Savings
!
ntp server 10.4.250.104
!
! ntp update-calendar
!
! clock timezone <timezoneName> <timezoneOffsetHours> <timezoneOffsetMinutes>
! clock summer-time <timezoneName> recurring
!
! Disable external HTTP(S) access
! Disable external Telnet access
! Enable external SSHv2 access
!
no ip http server
!
no ip http secure-server
!
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
!
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
!
errdisable recovery interval 300
!
ip routing
!Config below applies only on underlay orchestration
!
! Setup a Loopback & IP for Underlay reachability (ID)
! Add Loopback to Underlay Routing (ISIS)
!
interface loopback 0
description Fabric Node Router ID
ip address 10.4.218.97 255.255.255.255
ip router isis
!
!
! Setup an ACL to only allow SNMP from Fabric Controller
! Enable SNMP and RW access based on ACL
!
snmp-server view DNAC-ACCESS iso in
!
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
!
!
! Set MTU to be Jumbo (9100, some do not support 9216)
!
system mtu 9100
! FABRIC UNDERLAY ROUTING CONFIG:
!
! 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
!
!
!
```

```
interface vlan1
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
!
!
!This config goes to subtended node

username lan-admin privilege 15 password 0 C1sco123
!
enable password C1sco123
!
!
hostname CL-9300_7
!
interface vlan1
ip router isis
!
!
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 are displayed. Click on the physical link between seed and discovered device. Confirm that the interfaces are correct



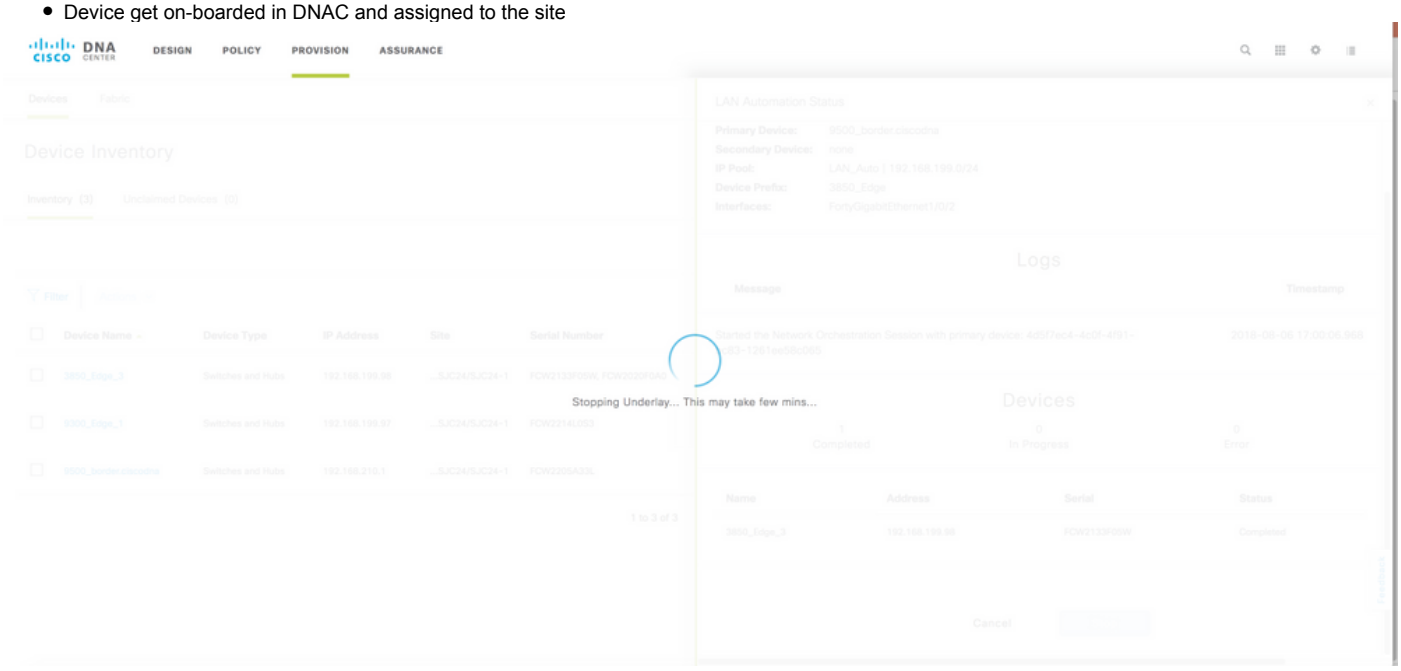
Note: If the physical link does not show up, re-sync that seed device where the physcal link connects. After re-sync check the topology page again to ensure the links shows up before stopping Lan auto. There have been issues where after stopping Lan auto, the link to secondary seed does not get configured.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

2. Stop Lan Automation

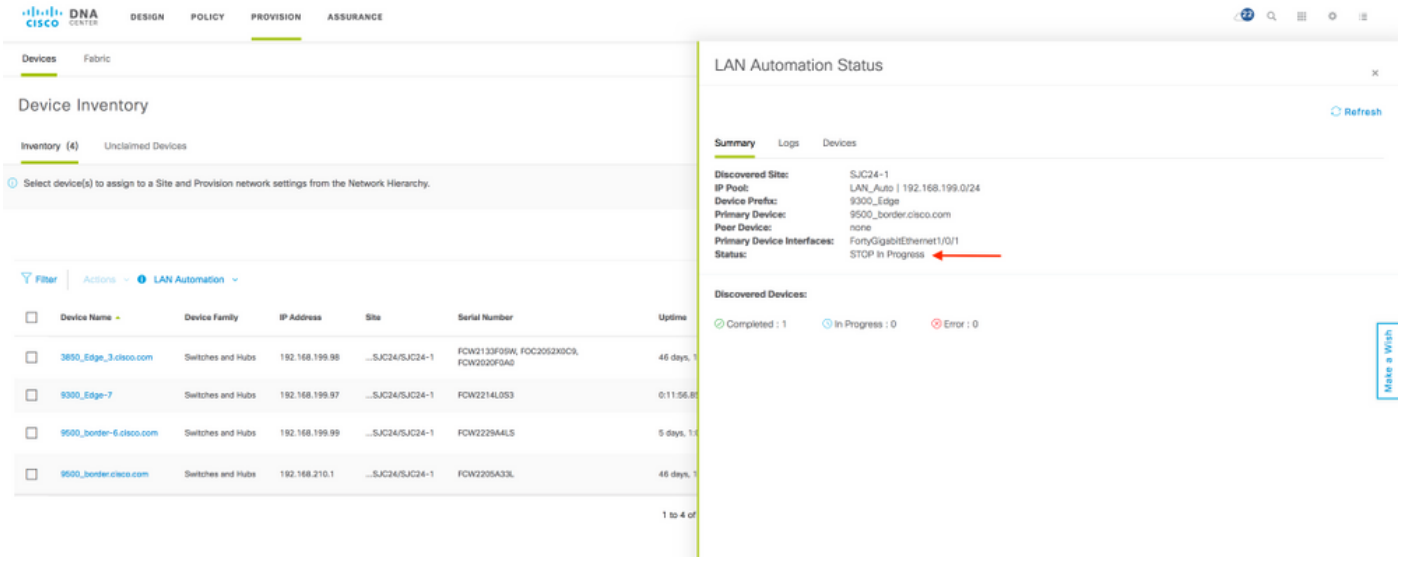
This is second stage of the Provision step. Purpose of this stage is to finish discovering all devices that a user wishes to and to prevent inadvertent discovery of any additional devices

- 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



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



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.

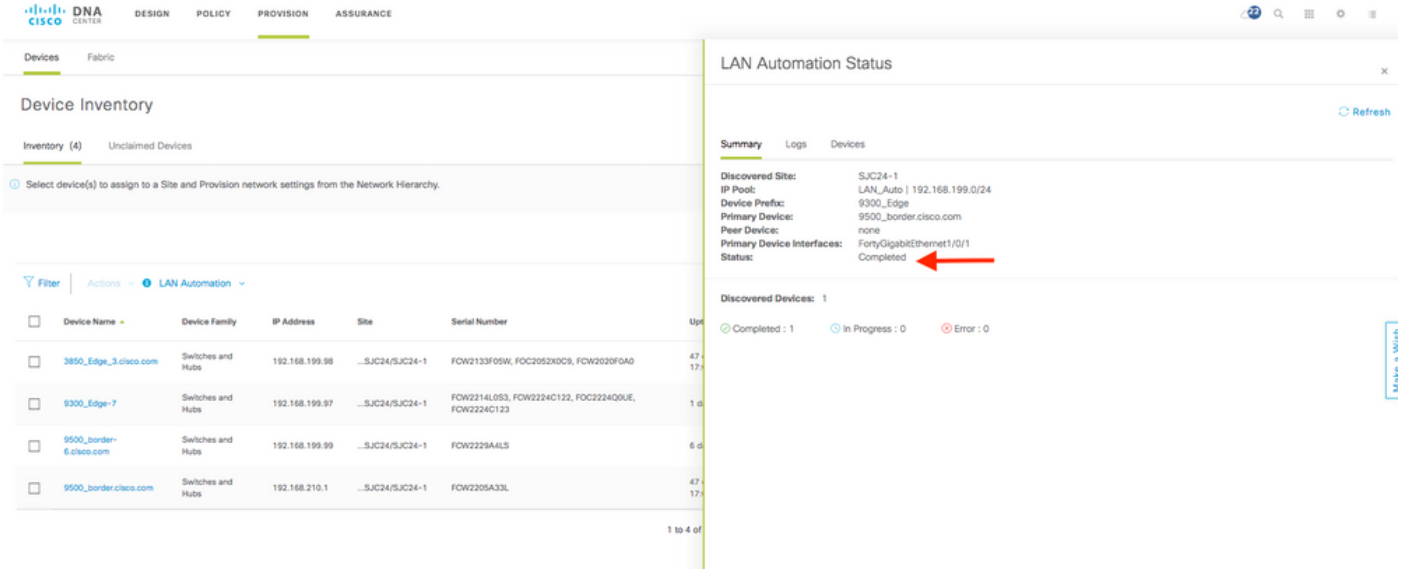
L3 link configuration pushed on stopping network orchestration (Each pair of interface gets its set of configuration):

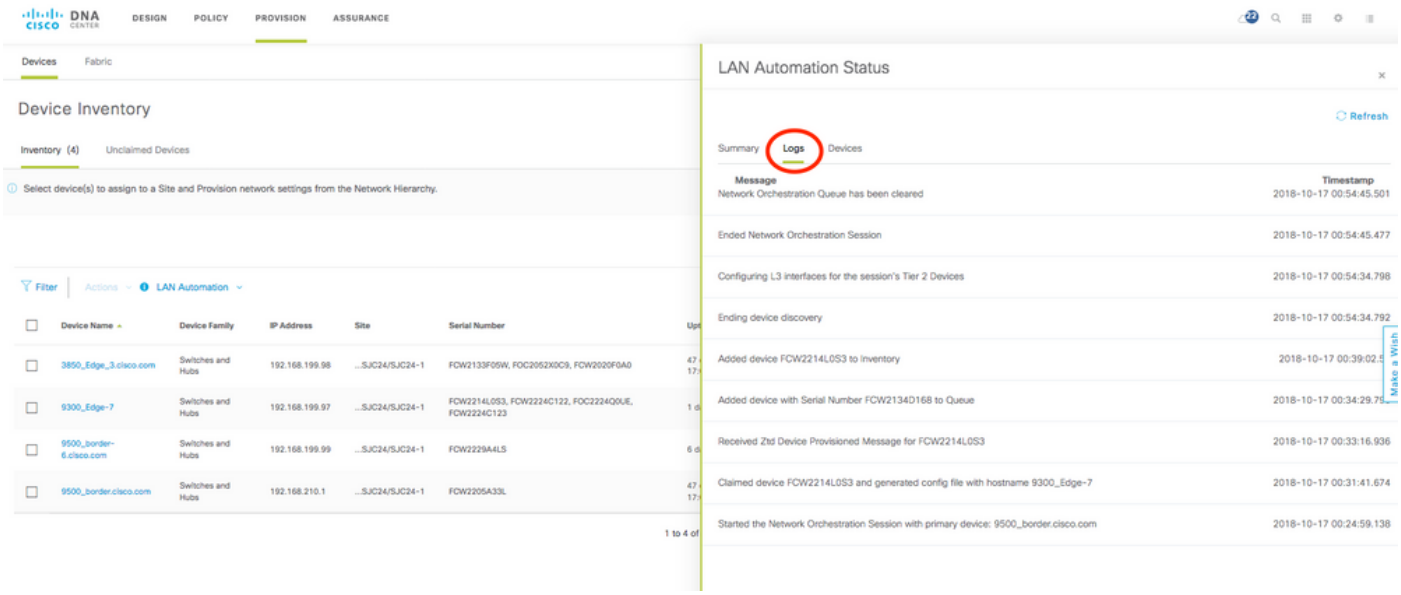
```
interface GigabitEthernet1/0/13
 description Fabric Physical Link
 no switchport
 dampening
 ip address 192.168.2.97 255.255.255.252
 ip router isis
 ip lisp source-locator Loopback0
 logging event link-status
 load-interval 30
 bfd interval 500 min_rx 50 multiplier 3
 no bfd echo
 isis network point-to-point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

- 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





Miscellaneous

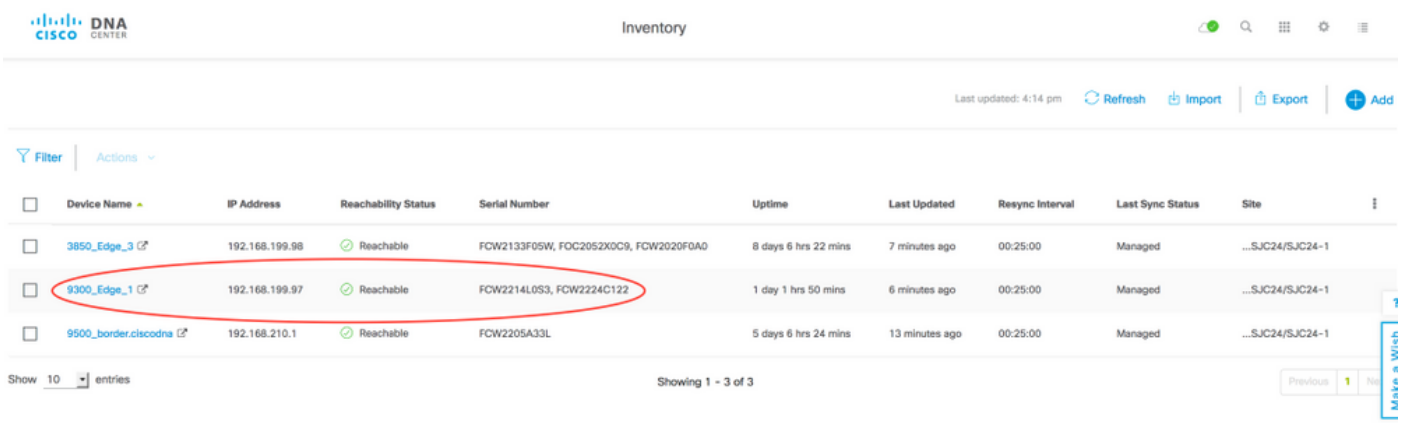
1. Adding a brand new switch or a switch never present in DNAC to a LAN automated stack

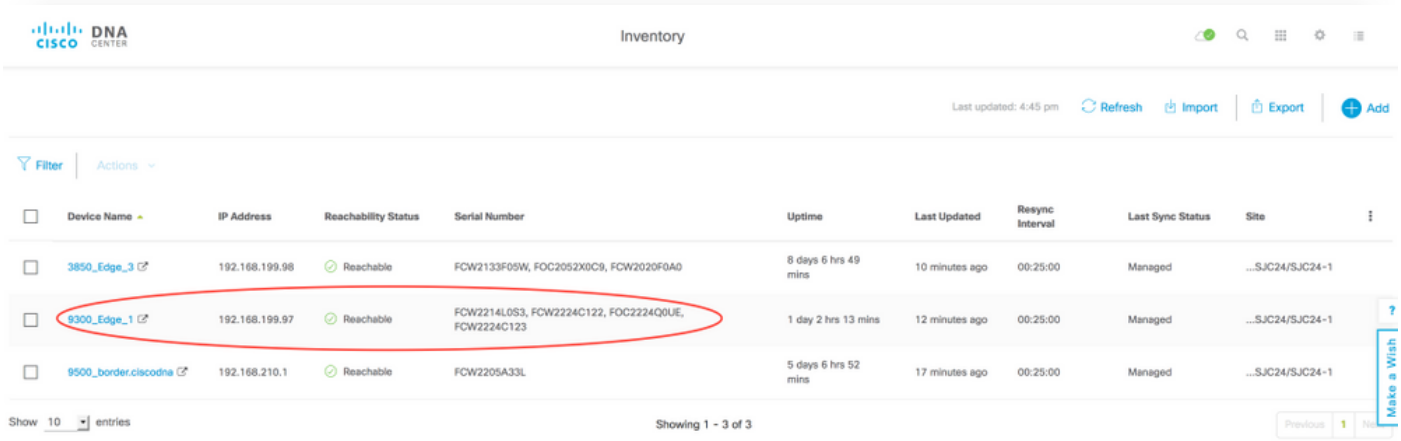
Switches can be added to a stack that is already Lan automated and in provisioned state without having to Lan automate/discover the new switch. Follow below steps for a smooth addition

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 right-to-use"
3. Ensure the switch is in same boot mode as the stack i.e either INSTALL (preferred) or BUNDLE
4.
```
9300_Edge_1#show ver | inc INSTALL
*     1  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  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 swicthes 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.
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:





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 swicth to be removed and under "Actions", click on "Delete Device"- If the swicth 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 swicth 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

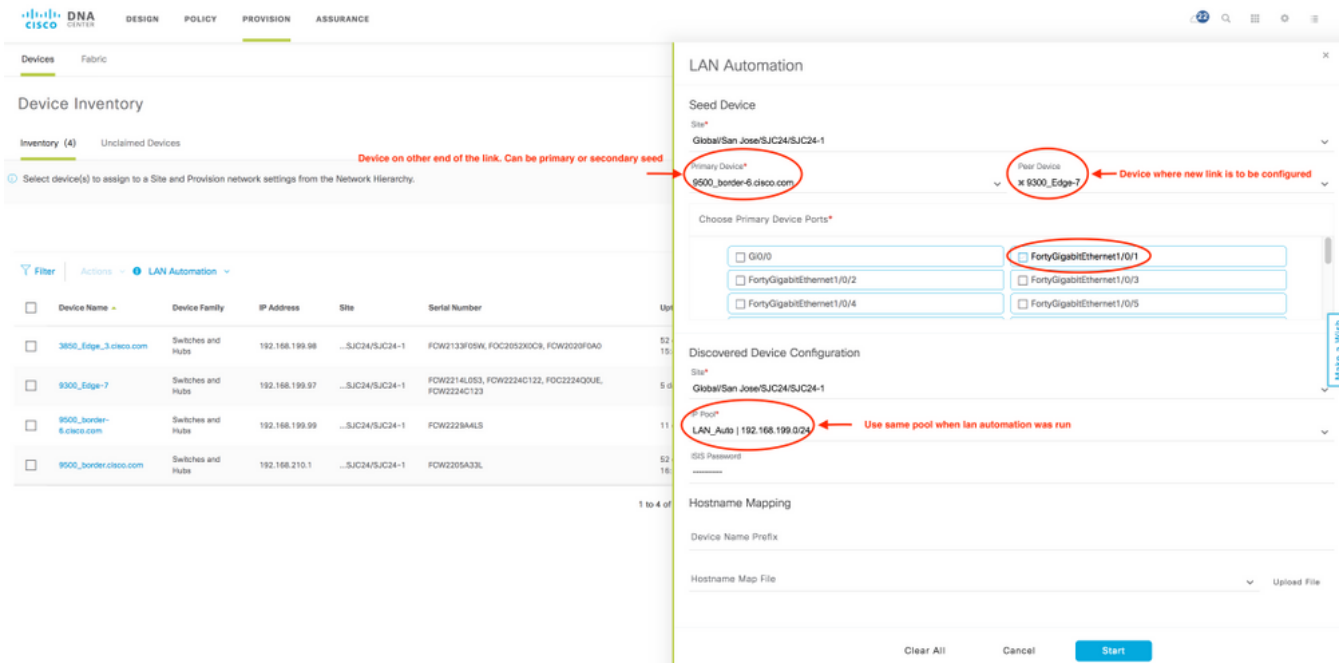
Use this method when you want to configure a) additional links between primary and peer seed devices or between distribution devices after lan auto was stopped b) uplinks from newly added switch to the stack to primary and peer seed

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.



- Start Lan auto. Wait for 2 minutes and then Stop lan 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 load-interval 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 192.168.199.86 255.255.255.252 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

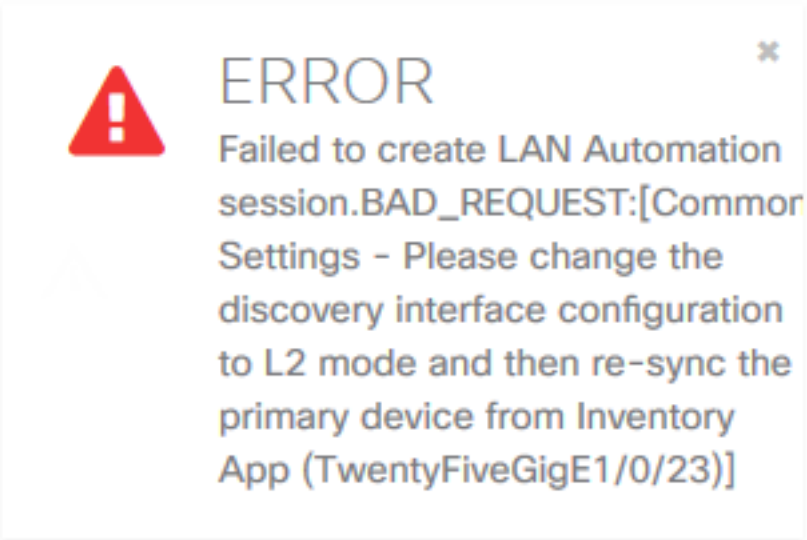
4. Moving uplink to the newly added switch

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

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 CSCvo40879 . 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 CSCvo42419 .



- 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
6. 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 CSCvp73666 . 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. CSCvr78668 CSCvr77659
- After upgrade to DNAC 1.3.1.3 Lan Automation will not work if any previous Lan automation had ISIS password configuration.CSCvr89951

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 lan automation relevant logs

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