

Cisco and Molex Smart Building Solution Implementation Guide

January 2024

Contents

System overview	5
System topology	5
System components	7
System networking	8
Initial installation of the lighting network	9
Initial installation with the Cisco Catalyst 9300 Series UPOE+ switch	9
Network topology	9
Configuring the Cisco Catalyst 9300 Series UPOE+ switch for initial installation	10
Initial light fixture installation	10
Configuring the DHCP server for light fixture IP addressing	10
Configuring MoDiag for light fixture provisioning	11
Lighting migration to the campus network architecture	11
Network topology	12
Campus network core/aggregation switch—Cisco Catalyst 9500 Series	14
Configuring StackWise Virtual	14
Configuring network Layer 2 and Layer 3	14
Configuring DHCP server for light fixture IP addressing	16
Configuring security features	17
Configuring network management (SNMP)	20
Wiring closet access switch (Cisco Catalyst 9300 Series)	21
Removing the initial installation configuration	21
Configuring network Layer 2 and Layer 3	21
Configuring MAB and filter-spec	23
Configuring PoE features	24
Configuring security features	25
Wiring closet access switch stack (Cisco Catalyst 9300 Series stack)	29
Cisco Catalyst 9300 Series stack configuration	29
Network Layer 2 and Layer 3 configuration	30
Configuring Auto SmartPort (recommended)	31
Configuring PoE features	33
Configuring security features	33
Configuring Auto SmartPort (optional)	37
Configuring network management (SNMP)	38

Provisioning light fixtures	38
Implementing data center applications for lighting	38
Configuring the firewall (Cisco Firepower 4112)	39
Configuring Cisco UCS	43
Configuring network device authentication (ISE)	44
Network management and monitoring with Cisco Catalyst Center	50
Configuring telemetry on Cisco Catalyst Center to collect PoE telemetry from the network	55
Configuring Molex CoreSync Manager services	58
Lighting control and maintenance	59
Light fixture control using Molex Facility Manager	59
Connecting to the controller using Facility Manager	59
Controlling on/off/dimming using the wireless wall switch	59
Configuring occupancy sensing	59
Configuring Ambient Lighting Sensing	59
Selecting light scenes using Facility Manager	60
Ongoing maintenance for light fixtures	60
Replacing light fixtures	60
Appendix A: Caveats	61
Appendix B: References	62
Cisco documentation	62
Molex documentation (refer directly to Molex representative for the following documents)	62
Appendix B: Glossary	63

The Cisco® and Molex end-to-end Smart Building Solution is a network-based connected lighting system that uses the Cisco Universal Power over Ethernet (UPOE+) switching products and Molex CoreSync products to provide indoor lighting services in the enterprise network.

Document scope

The Cisco and Molex Smart Building Solution Cisco Reference Design consists of a Design Guide, which provides overall guidance on the solution design, and this Implementation Guide.

This document provides implementation details for the initial installation of the Cisco and Molex Smart Building Solution, migration of the initial lighting setup to a production campus network topology, and ongoing lighting system management and maintenance.

This **Cisco and Molex Smart Building Solution Implementation Guide** provides the implementation details for the system topologies as discussed in the “System Architecture” section of the **Low-Voltage PoE Lighting Design Guide**, which can be found at the following URL:

- <https://www.cisco.com/c/en/us/solutions/enterprise-networks/low-voltage-poe-lighting-dg.html>

Note: The **Low-Voltage PoE Lighting Design Guide**, which is referred to frequently in this document, will be simply referred to as the “**Design Guide**” going forward.

The scope of this document is limited to implementation of a lighting network for initial installation and migration of the lighting setup to an enterprise campus network topology as described in the “System Architecture” section of the **Design Guide**.

Note: Detailed configuration steps for implementing a Molex lighting system are covered in the **Molex CoreSync Manager User Guide** that is referenced in this document wherever applicable.

The detailed implementation of a Cisco campus network architecture is beyond the scope of this document. For more details on the campus LAN architecture, refer to the **Design Zone for Campus Wired and Wireless LAN**, which can be found at the following URL:

- <https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html>

Audience

The audience of this guide comprises, but is not limited to, system architects, network/compute design engineers, systems engineers, field consultants, Cisco Advanced Services specialists, and customers who are designing and/or deploying the Cisco and Molex Smart Building Solution.

Readers should be familiar with IPv4 networking concepts and protocols, networking Layer 4 through Layer 7 services, and Cisco Catalyst™ switches, Cisco Catalyst Center, Cisco Unified Computing System (Cisco UCS®), and VMware hypervisors.

Implementation workflow

This section provides the high-level implementation flow for deploying the Cisco and Molex Smart Building Solution on a campus network topology as described in the **Design Guide**. It is suggested that you follow this implementation flow when deploying the solution on system topologies with campus network core and aggregation as described in the “System Architecture” section of the **Design Guide**.

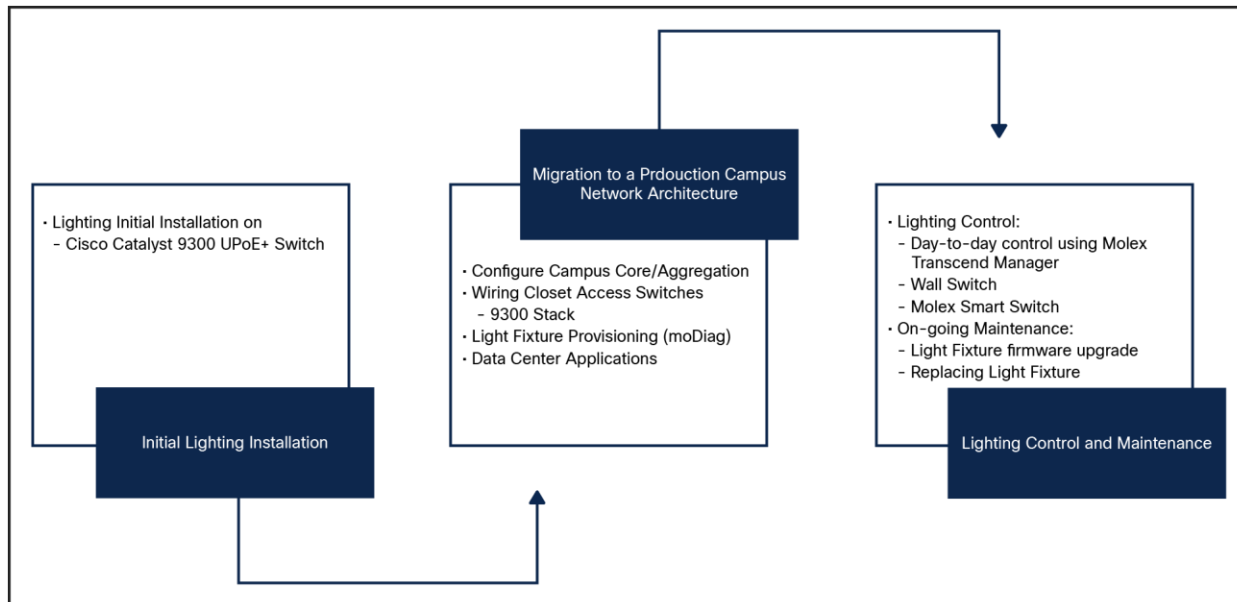


Figure 1.
Cisco and Molex Smart Building System implementation workflow

System overview

This section, which provides an overview of the Cisco and Molex Smart Building Solution implementation, includes the following major topics:

- [System topology, page 5](#)
- [System components, page 7](#)
- [System networking, page 8](#)

System topology

Different network topologies exist for deploying the Smart Building Solution based on the customer's requirements.

For more details on deployment topologies, refer to the “System Architecture” section of the **Design Guide**.

[Figure 1](#) shows a typical PoE lighting system implementation workflow and milestones achieved in the process from start to finish.

[Figure 2](#) shows the physical network topology for a lighting network integration with a campus network, where wiring closet access switches (Cisco Catalyst 9300 Series switch and stack) connect to the campus network aggregation/distribution switch (Cisco Catalyst 9500 Series). In this deployment, the aggregation switch aggregates the lighting wiring closet switches and provides IP addressing to light fixtures using Dynamic Host Configuration Protocol (DHCP). The aggregation switch in the campus network collapsed core/distribution layer connects to the data center via a firewall. The firewall allows only management traffic from the lighting network to flow to the data center.

Note: The campus network topology shown in [Figure 2](#) is one of the deployment models of campus network architectures (that is, the collapsed core network topology) considered for the system test bed. The detailed implementation of the campus network for enterprise network services is beyond the scope of this document. For detailed implementation and best practices for deploying the campus network, refer to the **Campus Network for High Availability Design Guide** at the following URL:

- http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

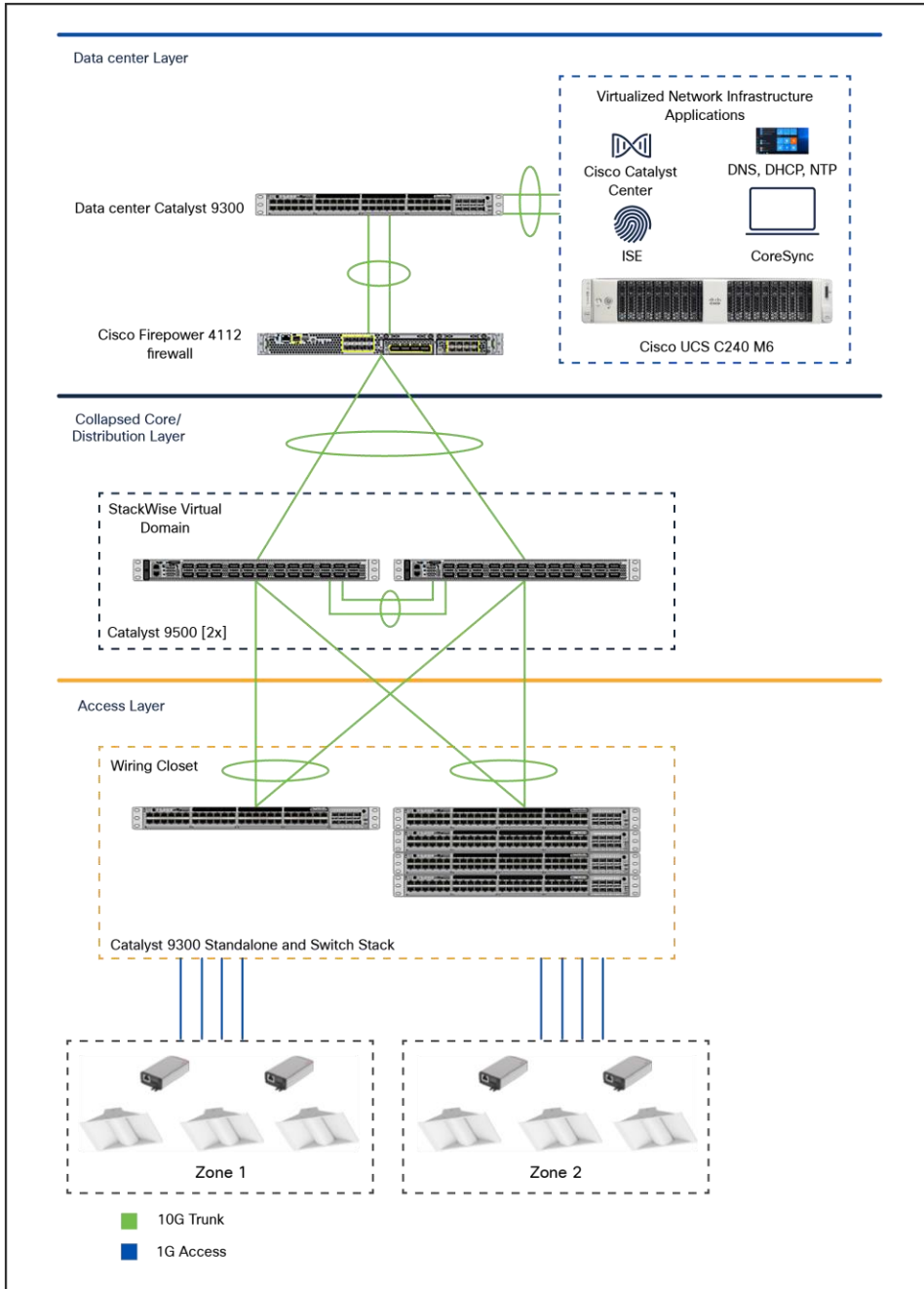


Figure 2. Cisco and Molex Smart Building Solution on a campus network topology with Cisco Catalyst 9300 Series Switches and stack in wiring closet

It is important to note that the architecture above is a sample reference design. The applications, services, and virtual machines can all reside on networks and appliances outside of this network physically and logically, with the most important factor being IP connectivity. In ideal situations, there would be no single point of failure such as the firewall or single data center switch, and they would be put into configurations with failover and/or high availability in mind, but for the sake of illustration, the reference network and architecture design is simplified here.

System components

The components validated within this system consist of a mix of Cisco products (see [Table 1](#)) and Molex products (see [Table 2](#)).

Table 1. Cisco components

Cisco product	Software release	Description
Cisco Catalyst 9300 Series Switch—wiring closet/access switch	17.9.1	UPOE+ switch
Cisco Catalyst 9300 Series Switch—data center switch or server access switch	17.9.1	Non-PoE switch
Cisco Catalyst 9500 Series Switch—core/distribution switch	17.3.4	Campus network Layer 3 aggregation switch
Cisco Catalyst Center	2.3.5	Network management and monitoring
Cisco UCS C240 M6 Rack Server	Cisco Integrated Management Controller 4.2	Hypervisor server to host applications and VMs
Cisco Identity Services Engine (ISE)	3.0	TACACS+ authentication and authorization server for network devices
Cisco Firepower® 4112 Security Appliance	9.16.1	Firewall to protect server farm

Table 2. Molex components

Molex product	Software release	Description
Molex CoreSync 2x2 LED troffer and lightbar		LED PoE light with integrated occupancy and ambient light sensors
Molex Gateway firmware	1.7.11	Firmware for lighting (updated firmware version)
Molex Sensor Board firmware	1.0.16	Firmware for sensor board
Molex CoreSync Manager	1.1.0.18	CoreSync management application
Molex Diagnostic Tool (MoDiag)	2.0.16.10	Molex diagnostic tool

[Table 3](#) lists third-party infrastructure components used in the system.

Table 3. Third-party system components

Product	Purpose	Version
Virtualization software for Cisco UCS	Hypervisor	VMware ESXi 7.0
Application platform	Operating system	Microsoft Windows 10 Enterprise Release SP1

System networking

The network-powered lighting system should be deployed on a separate logical network (VLAN). It is suggested that you use one VLAN or a network segment (subnet) for 500 light fixtures to reduce the size of the broadcast domains in the network. Therefore, an additional VLAN should be created when deploying more than 500 light fixtures. Use the multicast discovery control feature of the MoDiag tool within each VLAN to set the Molex CoreSync Manager IP address with which the light fixtures can communicate.

Note: The Molex MoDiag application's "extended range" accepts a range of only 250 simultaneous IP addresses to enable multicast discovery control within a VLAN. Therefore, a block of only 250 IP addresses needs to be configured in the MoDiag application. If more than 250 light fixtures exist in a VLAN, the MoDiag discovery must be relaunched for an additional block of IP addresses in the same VLAN for multicast-based discovery, control, and commissioning of these light fixtures.

This section summarizes the logical network (VLAN) configuration for the Cisco and Molex Smart Building Solution network. In [Table 4](#), which is a list of the example VLANs implemented for this solution, the subnet mask "255.255.254.0" is used for 500 light fixtures per VLAN as recommended in the **Design Guide**.

Table 4. Example of VLAN segmentation

VLAN	Purpose	Network/Mask
30	VLAN for light fixtures and MoDiag in the data network	10.30.0.0/23
40	VLAN for light fixtures and MoDiag in the data network	10.40.0.0/23
50	Management VLAN for the network management traffic	10.50.0.0/23
70	Data VLAN in the data center for applications	10.70.0.0/23

Note: The VLANs shown in [Table 4](#) are only examples that are used in this Cisco and Molex Smart Building Solution. VLAN numbering will vary based on your actual deployment.

Initial installation of the lighting network

The Cisco and Molex Smart Building Solution uses Cisco UPOE+ switches for the deployment scenarios discussed in the **Design Guide**. This section, which covers implementation details for the initial installation (day 0), includes the following major topics:

- [Initial installation with the Cisco Catalyst 9300 Series UPOE+ switch, page 9](#)
- [Light fixture initial installation, page 10](#)

During the initial installation, the electrician will install the light fixtures in the planned lighting spaces and the Molex Gateways will be wired back to the closet and connected to the Catalyst 9300 Series switch with the default factory configuration to verify the light fixture's operation.

Initial installation with the Cisco Catalyst 9300 Series UPOE+ switch

This section covers the network topology and configuration required on the Cisco Catalyst 9300 Series Switch for the initial installation of light fixtures.

Network topology

During the initial installation, light fixtures are connected to the wiring closet Cisco Catalyst 9300 Series UPOE+ access switch or to the switch stack, as shown in the network topology in [Figure 3](#).

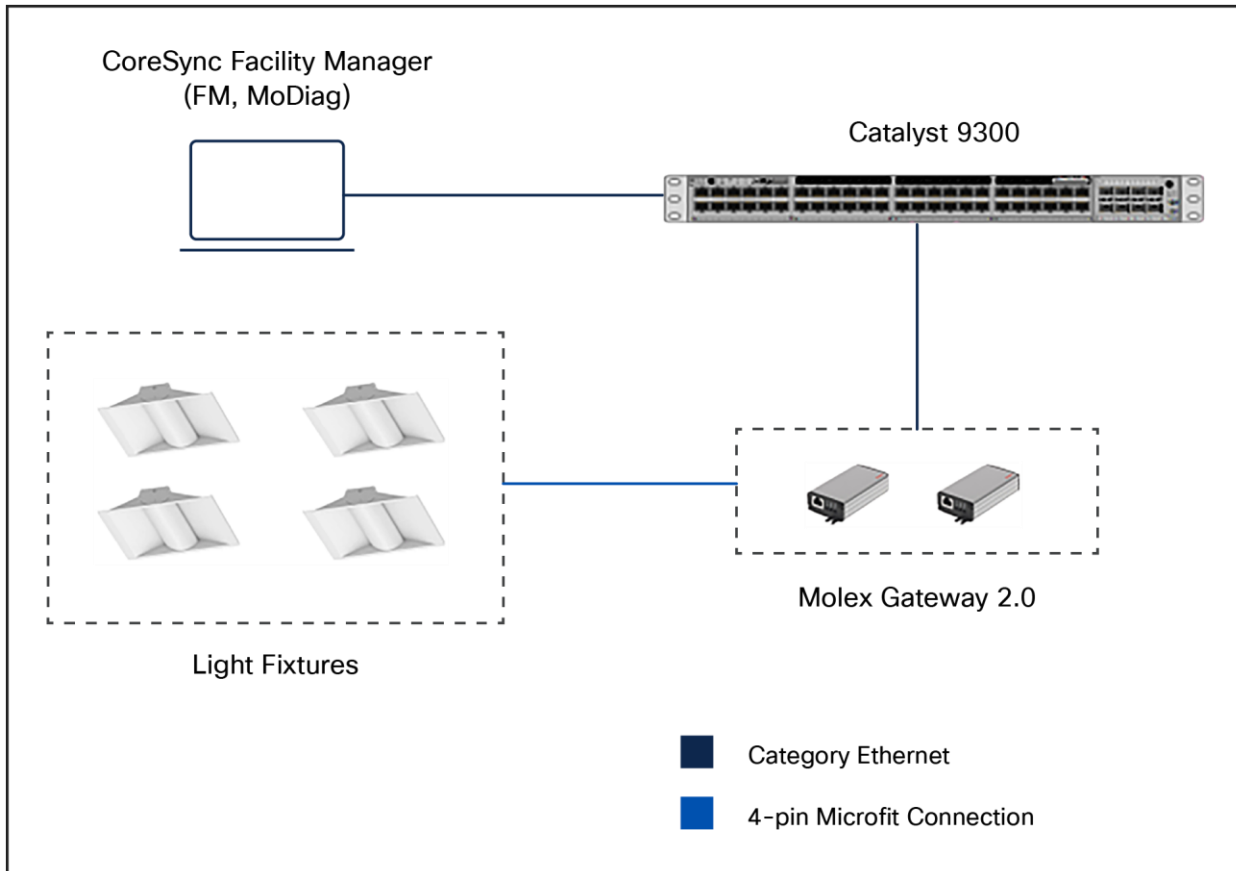


Figure 3. Cisco and Molex Smart Building Solution initial setup on wiring closet Cisco Catalyst 9300 Series Switch

Configuring the Cisco Catalyst 9300 Series UPOE+ switch for initial installation

Installation of Molex light fixtures

An electrician using an UPOE+ switch generally performs the initial installation of Molex light fixtures at the installation site.

When the light fixtures are connected to a Cisco Catalyst 9300 Series UPOE+ switch port, the fixtures turn on with low brightness; this verifies their hardware operation.

Initial network setup

An IT network engineer or the commissioning engineer generally performs the initial installation of the lighting network.

Prerequisites for initial installation

Perform the following prerequisite steps for initial lighting network setup:

The Cisco Catalyst 9300 Series Switch supports Perpetual and Fast PoE features (described in [Lighting migration to campus network architecture, page 11](#)) on Cisco IOS® Software Release 17.9.1. Therefore, it is suggested that you upgrade the IOS image on the switch to version 17.9.1 before beginning lighting network installation.

1. Enable Link Layer Discovery Protocol (LLDP) on the switch global configuration, using the command below. LLDP must be enabled on the switch for the Molex light fixtures' power negotiation and operation.

```
C9300-Switch(config)#lldp run
```

2. Enable 2-event classification on all the light ports:

```
C9300-Switch(config-if)#power inline port 2-event
```

The PoE power allocation for a class 4 device will be 30W if 2-event classification is enabled on the port; otherwise, it will be 15.4W.

3. Configure a Switched Virtual Interface (SVI) for the default VLAN 1:

```
interface vlan 1
ip address 10.1.0.1 255.255.254.0
```

Initial light fixture installation

This section covers IP addressing for light fixtures using the DHCP server and initial commissioning of light fixtures using Molex MoDiag.

Configuring the DHCP server for light fixture IP addressing

Commissioning the Molex light fixtures for the initial installation verifies the light fixture operation and control using the Molex MoDiag and CoreSync Manager applications. The light fixture requires IP addresses to be assigned in the network to perform setup for initial provisioning.

During the initial installation, the DHCP server IP addressing pool for light fixtures and wall dimmers is configured on the Cisco Catalyst 9300 Series access switch in the wiring closet to assign IP addresses to Molex endpoints.

[Table 5](#) is an example DHCP pool range for Molex light fixtures.

Table 5. IPv4 DHCP address pool on the Cisco Catalyst 9300/9500 Series

Pool network	Excluded IP range	Purpose
10.1.0.0/23	10.1.0.1 to 10.1.0.10	DHCP pool for Molex light fixtures in default VLAN 1

Configure the DHCP server on the Cisco Catalyst 9300 Series access switch. For example:

```
C9300-Switch (config)# ip dhcp pool Molex
  network 10.1.0.0 255.255.254.0
  default-router 10.1.0.1
C9300-Switch (config)# ip dhcp excluded-address 10.1.0.1 10.1.0.10
!
```

Configuring MoDiag for light fixture provisioning

Perform the steps described in this section to install and configure the Molex CoreSync Manager.

Installing Molex MoDiag

When installing MoDiag, the administrator should obtain the **Molex MoDiag Installation Guide** from Molex and install it on a machine that adheres to Molex’s requirements for said device, following the hardware, software, and network specifications.

Provisioning light fixtures

When provisioning the light fixtures, the administrator should obtain the **CoreSync Commissioning Guide** from Molex and follow the recommendations, instructions, and guidelines provided.

Verifying and upgrading the light fixture firmware

The light fixture's firmware version can be verified on the MoDiag application after MoDiag connects to the gateways powering the fixtures.

The **Molex CoreSync Commissioning Guide** provides the steps necessary to upgrade the firmware on the endpoints. The **MoDiag User Guide** provides the instructions for verifying the firmware version to confirm the successful upgrades and updates performed by the administrators.

Lighting migration to the campus network architecture

This section covers the implementation details for migrating a lighting deployment installed as an “initial install” to a converged campus network architecture. Lighting migration to the campus network topology is also discussed in more detail in the “System Architecture” section of the **Design Guide**.

Implementation of networking Layer 2, Layer 3, and security features required for network-powered lighting with campus network deployment is discussed in the following major topics:

- [Campus network core/aggregation switch Cisco Catalyst 9500 Series, page 14](#)
- [Wiring closet access switch \(Cisco Catalyst 9300 Series\), page 21](#)

- [Wiring closet access switch stack \(Cisco Catalyst 9300 Series stack\), page 29](#)
- [Provisioning light fixtures, page 38](#)
- [Implementing data center applications for lighting, page 38](#)

Network topology

During migration, the access switches in the wiring closet (Cisco Catalyst 9300 Series standalone or stack) connect to a production campus network core/aggregation switch with separate logical networks for Molex light fixtures, as shown in [Figures 4](#) and [5](#).

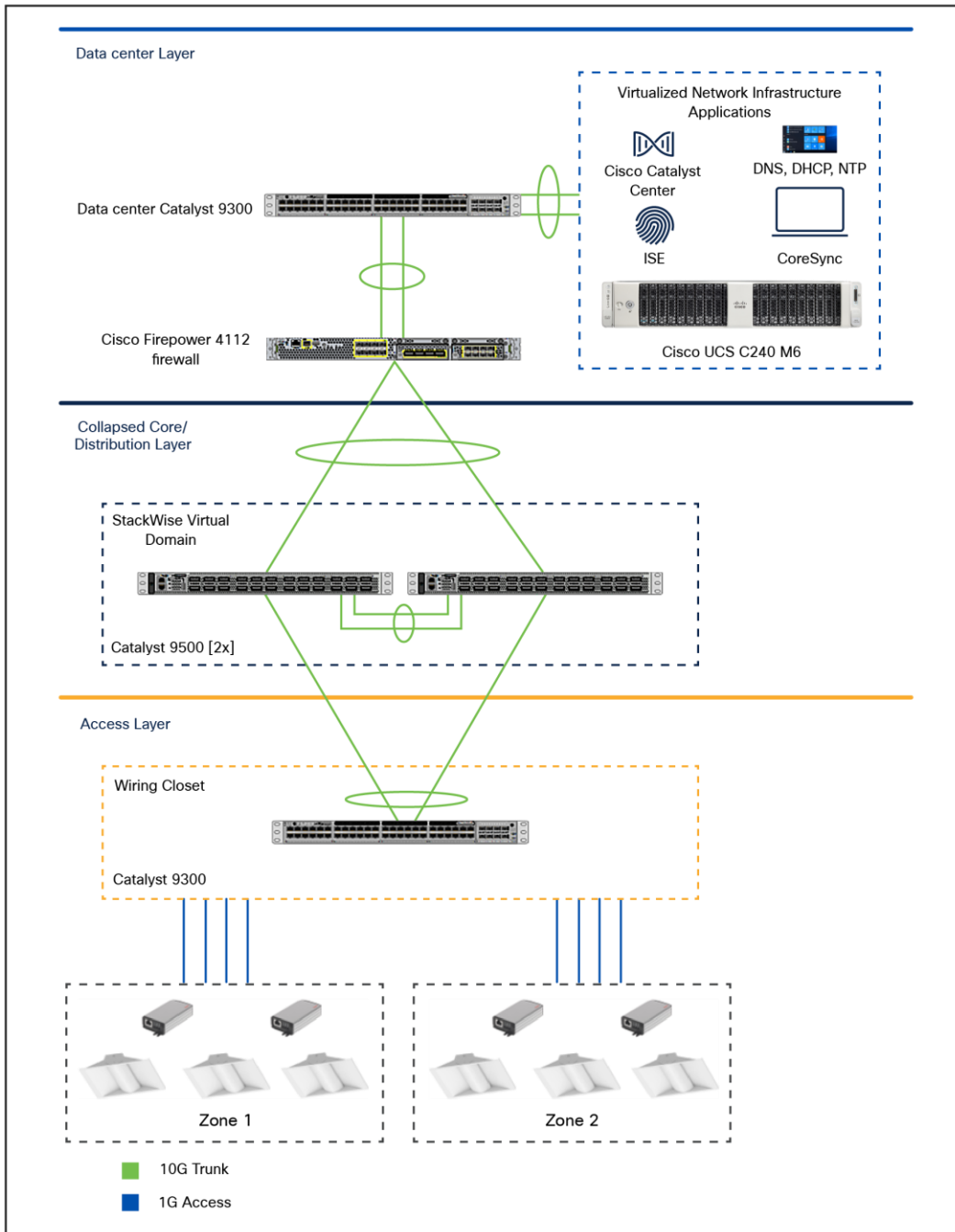


Figure 4.

Cisco and Molex Smart Building Solution on a campus network architecture with a Cisco Catalyst 9300 Series access switch

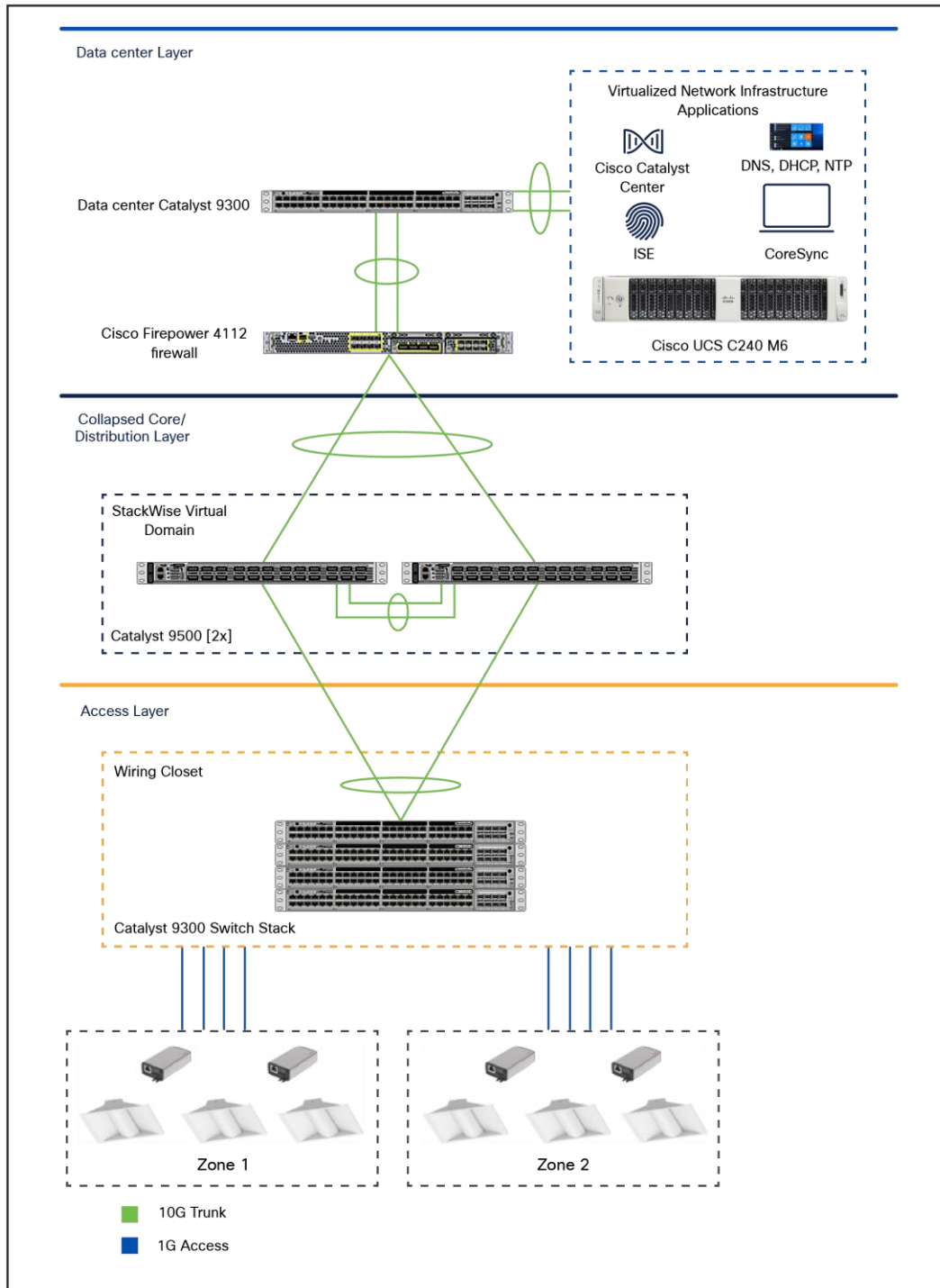


Figure 5. Cisco and Molex Smart Building Solution large-scale deployment on campus network architecture with Cisco Catalyst 9300 Series Switch stack

Campus network core/aggregation switch—Cisco Catalyst 9500 Series

The lighting network UPOE+ access switches (Cisco Catalyst 9300 Series standalone or stack) are connected to campus network aggregation switches when migrating from an initial lighting setup to a converged campus network/large-scale deployment. The detailed implementation of the campus network architecture is beyond the scope of this document.

Cisco Catalyst 9500 Series Switches, deployed in a pair, act as the campus network core, whereas the aggregation services and Layer 3 routing functionalities for the lighting endpoints are in the access layer. The implementation of the Cisco Catalyst 9500 Series Switch in a large-scale network-powered lighting architecture with security features, as described in the “System Design” section of the **Design Guide**, is covered in this section.

Configuring StackWise Virtual

The system topology in [Figure 4](#) shows one of the implementations of the campus network aggregation as a collapsed core/distribution model for this Cisco and Molex Smart Building Solution. The aggregation Cisco Catalyst 9500 Series Switches implement StackWise® Virtual to provide network redundancy at the aggregation layer.

StackWise Virtual combines a pair of Cisco Catalyst 9500 Series Switches into a single network element. StackWise Virtual manages the redundant links, which externally act as a single port channel. This also simplifies network configuration and operation by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

Note: The lighting network converges to a production campus network where implementation of StackWise Virtual may not be required at the network aggregation level. In this case, the StackWise Virtual configuration steps need not be performed.

For details on implementing StackWise Virtual on the Cisco Catalyst 9500 Series Switch, refer to the **High Availability Configuration Guide, Cisco IOS XE 17.3.x (Catalyst 9500 Switches)** at the following URL:

- [High Availability Configuration Guide, Cisco IOS XE 17.3.x \(Catalyst 9500 Switches\)](#)

Configuring network Layer 2 and Layer 3

This section defines the implementation of VLANs and Layer 3 logical interfaces on the Cisco Catalyst 9500 Series Switch.

1. Configure VLANs, which must be created along with port assignments, on the Cisco Catalyst 9500 Series Switch:

```
9500-Switch(config)#vlan 30,40,50
```

2. Create a Layer 3 SVI for the lighting VLANs. The example configuration below shows SVIs for the lighting VLANs and network management VLAN on the Cisco Catalyst 9500 Series Switch:

```
interface Vlan30
 ip address 10.30.0.1 255.255.254.0
interface Vlan40
 ip address 10.40.0.1 255.255.254.0
interface Vlan50
 ip address 10.50.0.1 255.255.254.0
```

Note: When migrating the lighting initial setup to a converged campus network, remove the SVIs for the lighting VLANs that you may have created on wiring closet access switches. SVIs for lighting VLANs are configured at the core/aggregation switches that provide Layer 3 services to the lighting network.

3. Create port channel interfaces on the Cisco Catalyst 9500 Series to the wiring closet switches (Cisco Catalyst 9300 Series standalone and stack), and Firepower in the network, as shown below:

```
interface Port-channel2
  description Etherchannel Link to FPR Firewall switchport
  switchport mode trunk
  spanning-tree portfast
```

```
interface Port-channel103
  description Etherchannel Link to 9300 Switch Stack switchport
  switchport mode trunk
  switchport trunk allowed vlan 30,40,50
```

```
interface Port-channel104
  description Etherchannel Link to 9300 Switch switchport
  switchport mode trunk
  switchport trunk allowed vlan 30,40,50
```

4. Enable EtherChannel on the appropriate physical switch ports connected to the Cisco Catalyst 9300 Series standalone and stack switches and the Firepower. The following configuration shows the port channel assignment to the switch physical ports:

Physical links to the Cisco Catalyst 9300 Series switch stack in the wiring closet:

```
interface TenGigabitEthernet1/1/3
  channel-group 103 mode active
interface TenGigabitEthernet2/1/3
  channel-group 103 mode active
```

Physical links to the Cisco Catalyst 9300 Series switch in the wiring closet:

```
interface TenGigabitEthernet1/1/4
  channel-group 104 mode active
interface TenGigabitEthernet2/1/4
  channel-group 104 mode active
```

Physical links to the Firepower 4112 firewall:

```
interface TenGigabitEthernet1/1/10
  channel-group 2 mode active
interface TenGigabitEthernet2/1/10
  channel-group 2 mode active
```

5. The following command adds static default routes to the Firepower 4112 firewall:

```
ip route 10.70.0.0 255.255.254.0 10.50.0.2
```

6. Enable rapid per-VLAN spanning tree:

```
spanning-tree mode rapid-pvst
```

7. Enable VLAN Trunk Protocol (VTP) pruning:

```
vtp pruning
```

Configuring DHCP server for light fixture IP addressing

When migrating the lighting initial setup to a converged campus network, the DHCP server IP addressing pool for light fixtures and wall dimmers is configured on the Cisco Catalyst 9500 Series aggregation switch to assign IP addresses to Molex endpoints, as shown in [Figure 4](#).

Note: Make sure to remove the DHCP server configuration on the wiring closet access or director switches (Cisco Catalyst 9300 Series) that was performed during the initial lighting setup.

[Table 6](#) shows an example DHCP pool range for Molex endpoints.

Table 6. Example IPv4 DHCP address pool on the Cisco Catalyst 9500 Series

Pool network	Excluded IP range	Purpose
10.30.0.0/23	10.30.0.1 to 10.30.0.10	DHCP pool for Molex light fixtures in VLAN 30
10.40.0.0/23	10.40.0.1 to 10.40.0.10	DHCP pool for Molex light fixtures in VLAN 40

Perform the following step to configure the DHCP server pool on the Cisco Catalyst 9500 Series aggregation switch for the lighting network.

Configure DHCP pools for light fixtures on the Cisco Catalyst 9500 Series:

```
ip dhcp pool MOLEX-VLAN30
network 10.30.0.0 255.255.254.0
default-router 10.30.0.1
!
!
ip dhcp pool MOLEX-VLAN40
network 10.40.0.0 255.255.254.0
default-router 10.40.0.1
!
ip dhcp excluded-address 10.40.0.1 10.40.0.10
ip dhcp excluded-address 10.30.0.1 10.30.0.10
!
```

Configuring security features

Security features in the lighting network are important to protect light fixtures from network attacks such as IP addresses from untrusted DHCP servers, Address Resolution Protocol (ARP) attacks, Denial-of-Service (DoS) attacks, and broadcast storms. If proper security configurations are not implemented on switches, the light fixtures and the whole network become more susceptible to such attacks. Therefore, features such as DHCP snooping, port security, ARP inspection, and ARP rate limiting will enable security on the switch and its ports to keep the network safe.

This section defines the recommended Layer 2 security features to be enabled within the campus network on the Cisco Catalyst 9500 Series. For a detailed description of the Layer 2 security features, refer to the Security Configuration Guide, Cisco IOS XE 17.3.x (Catalyst 9500 Switches) at the following URL:

- [Security Configuration Guide, Cisco IOS XE 17.3.x \(Catalyst 9500 Switches\)](#)

IP DHCP snooping (optional)

IP DHCP snooping is needed on the Catalyst 9500 Series Switch only if a separate centralized DHCP server exists that is connected to the switch. In that case, the Catalyst 9500 Series Switch also needs to be configured as a DHCP relay agent.

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

When light fixtures are powered on, they request an IP address from a DHCP server. IP DHCP snooping ensures that only DHCP packets received on trusted ports that are sent by the server are forwarded to the lights.

Perform the following steps on the Cisco Catalyst 9500 Series Switch to configure IP DHCP snooping.

Note: The DHCP snooping table does not match the IP Source Guard table, and the light fixtures don't receive the IP address properly. Therefore, the DHCP snooping feature will not work as expected in this Cisco Reference Design release.

1. Configure the required port as a DHCP snooping trusted port:

```
interface Port-channel105
  description Etherchannel Link to Centralized DHCP server
  ip dhcp snooping trust
!
```

2. Enable IP DHCP snooping globally for the per-port command to take effect:

```
ip dhcp snooping vlan 30-50
no ip dhcp snooping information option
ip dhcp snooping
!
```

IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

Only the IP-to-MAC bindings learned on the Cisco Catalyst 9500 Series on trusted ports will be allowed to send or receive traffic. All the packets received on trusted ports with a different binding to a particular MAC address will be dropped.

Note: The DHCP snooping table does not match the IP Source Guard table, and the light fixtures don't receive the IP address properly. Therefore, the IP Source Guard feature will not work as expected in this Cisco Reference Design release.

Perform the following step on the Cisco Catalyst 9500 Series Switch to configure IP Source Guard.

Configure IP Source Guard on the downlink port channel interfaces to the Cisco Catalyst 9300 Series stack and standalone switches that have trusted IP-to-MAC bindings:

```
interface Port-channel103
  description Etherchannel Link to 9300 Switch Stack
  ip verify source
```

```
interface Port-channel104
  description Etherchannel Link to 9300 Switch Standalone
  ip verify source
```

ARP inspection (optional)

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

Since it is highly unlikely that attackers will connect to the free ports of the Cisco Catalyst 9500 Series, configuring DAI on the Cisco Catalyst 9500 Series is optional.

Lights and any other devices connected on untrusted ports of the Cisco Catalyst 9500 Series will automatically be put in an error-disabled state so that the device won't be able to get access to the network.

Perform the following steps on the Cisco Catalyst 9500 Series Switch to configure DAI:

1. Configure the required port channels as ARP inspection trusted ports, as shown in this example configuration:

```
interface Port-channel103
  description Etherchannel Link to 9300 Switch Stack
  ip arp inspection trust

interface Port-channel104
  description Etherchannel Link to 9300 Switch Standalone
  ip arp inspection trust
```

-
2. Enable global ARP inspection for the required VLANs so that the per-port command takes effect:

```
ip arp inspection vlan 30,50
```

Storm control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

A broadcast or unicast storm is usually capable of creating a loss of access to the light fixtures and Storm Control Manager (SCM), depending on the port bandwidth consumed by the storm. Storm control limits the propagation of such packets to the light fixtures and maintains proper access to the light fixtures for SCM.

Perform the following configuration on the Cisco Catalyst 9500 Series Switch to configure storm control:

Configure storm control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentages of line rates:

```
interface Port-channel103
description Etherchannel Link to 9300 Switch Stack
storm-control broadcast level pps 5000 4500
storm-control multicast level pps 5000 4500
storm-control unicast level pps 5000 4500
storm-control action trap
```

```
interface Port-channel104
description Etherchannel Link to 9300 Switch Standalone
storm-control broadcast level pps 5000 4500
storm-control multicast level pps 5000 4500
storm-control unicast level pps 5000 4500
storm-control action trap
```

Disabling Telnet

Since Telnet is not secure, we recommend disabling it so that it can't be used to access the device. The following commands disable Telnet and enable only Secure Shell (SSH) access to the Cisco Catalyst 9500 Series Switch:

```
line vty 0 15
transport input ssh
```

Configuring network management (SNMP)

Simple Network Management Protocol (SNMP) is used to manage and monitor the switches in the lighting network.

SNMP traps are configured to send light fixture ports up/down status alerts to a network management server that helps monitor the light fixtures' port status.

Configuring switch network management

The SNMP v3 protocol configuration is used on the Cisco Catalyst 9500 Series Switch for network management. Perform the following steps to configure SNMP v3:



Figure 6.

Network management SNMP configuration flow

1. **Configure SNMP v3 view:**

```
snmp-server view MOLEX iso included
```

2. **Configure SNMP v3 group:**

```
snmp-server group MOLEX v3 auth read MOLEX write MOLEX
```

3. **Configure SNMP v3 user:**

```
snmp-server user MOLEX v3 auth md5 123456789012345 priv aes 128 123456789012345
```

4. **Configure SNMP traps:**

```
snmp-server enable traps port-security
```

```
snmp-server enable traps snmp
```

5. **Verify that the SNMP user, group, and view have been created, using the following commands:**

```
C9500#show snmp user
```

```
C9500#show snmp group
```

```
C9500#show snmp view
```

Wiring closet access switch (Cisco Catalyst 9300 Series)

This section covers the Cisco Catalyst 9300 Series wiring closet access switch stack, Layer 2 and Layer 3 networking, security, and network management configurations.

Removing the initial installation configuration

When migrating the initial lighting setup on the Cisco Catalyst 9300 Series Switch in the wiring closet to a campus network, follow the steps below to remove the initial switch configuration:

1. Remove the DHCP pool from the switch by issuing a no command:

```
C9300-Switch (config)# no ip dhcp pool Molex
C9300-Switch (config)# no ip dhcp excluded-address 10.1.0.1 10.1.0.10
```

2. Remove the IP address for VLAN 1:

```
interface vlan 1
no ip address
```

Configuring network Layer 2 and Layer 3

This section describes the implementation of VLANs and logical SVI for management traffic on the Cisco Catalyst 9300 Series Switch. The LLDP and 2-event classification must already have been enabled in the initial installation.

1. Configure VLANs, which must be created along with port assignments on the Cisco Catalyst 9300 Series switch stack. The following is an example VLAN configuration:

```
C9300-switch (config)#vlan 30,40,50
```

2. Configure the switch ports connected to light fixtures/wireless gateway on the appropriate lighting VLAN in access mode and to use the subscriber-id and client-id to obtain the DHCP IP address from the locally configured address pool:

```
interface GigabitEthernet 1/1
switchport mode access
switchport access vlan 30
ip dhcp server use subscriber-id client-id
!
```

3. Configure IP DHCP pools on the 9300 Series access switches, as well as the desired corresponding interface, to assign an IP address to any device connected to the interface:

```
ip dhcp pool MOLEX-VLAN30
network 10.30.0.0 255.255.254.0
address 10.30.0.21 client-id "Gi1/0/26" ascii
address 10.30.0.22 client-id "Gi1/0/27" ascii
address 10.30.0.23 client-id "Gi1/0/28" ascii
address 10.30.0.24 client-id "Gi1/0/29" ascii
address 10.30.0.25 client-id "Gi1/0/30" ascii
address 10.30.0.26 client-id "Gi1/0/31" ascii
default-router 10.30.0.1
ip dhcp excluded-address 10.30.0.1 10.30.0.10
```

```
ip dhcp pool MOLEX-VLAN40
network 10.40.0.0 255.255.254.0
address 10.40.0.21 client-id "Gi1/0/13" ascii
address 10.40.0.21 client-id "Gi1/0/14" ascii
address 10.40.0.22 client-id "Gi1/0/15" ascii
address 10.40.0.23 client-id "Gi1/0/16" ascii
address 10.40.0.24 client-id "Gi1/0/17" ascii
address 10.40.0.25 client-id "Gi1/0/18" ascii
default-router 10.40.0.1
ip dhcp excluded-address 10.40.0.1 10.40.0.10
```

4. Provide shutdown and no shutdown Command-Line Interface (CLI) commands on the switch ports where light fixtures and CoreSync gateways are connected. This enables the light fixtures to initiate DHCP requests to obtain IP addresses on the newly configured VLANs.

```
Interface range GigabitEthernet 1/0/26-31
shutdown
no shutdown
```

Note: The shutdown and no shutdown commands on the interfaces will cause momentary disruption of the light fixtures. The light fixtures will then illuminate and become fully operational for controls once the new IP addresses are assigned after the light fixtures are recommissioned using Molex applications.

5. Create a Layer 3 SVI for the management VLAN and default gateway as required. The following is an example configuration of a management VLAN SVI on the Cisco Catalyst 9300 Series switch stack:

```
interface Vlan50
ip address 10.50.0.4 255.255.254.0
ip default-gateway 10.50.0.1
```

6. Create port channel uplink interfaces on the Cisco Catalyst 9300 Series to the campus network aggregation switch (Cisco Catalyst 9500 Series), as shown in [Figure 2](#):

```
interface Port-channel104
description Etherchannel Link to 9500 Switch
switchport
switchport mode trunk
switchport trunk allowed vlan 30,40,50
```

-
7. Enable port channels on the appropriate physical switch ports connected to the Cisco Catalyst 9500 Series Switch. The following configuration shows the port channel assignment to the physical switch ports:

Physical links to Cisco Catalyst 9500 Series active and standby StackWise Virtual domain switches:

```
interface TenGigabitEthernet1/1/3
  channel-group 104 mode active

interface TenGigabitEthernet1/1/4
  channel-group 104 mode active
```

8. Enable rapid per-VLAN spanning tree.

```
spanning-tree mode rapid-pvst
!
```

Configuring MAB and filter-spec

The following configurations must be added on the light fixture access ports, both on Cisco Catalyst 9300 Series switch stack and standalone. The configuration below is mandatory for the visibility of mud-url on the switch and ISE.

Here, access sessions are configured in order to enable authentication to a port. Access-session host mode allows the host to gain access to a controlled port, and access-session port control sets the authorization for the port.

```
interface GigabitEthernet2/1/1
switchport access vlan 30
switchport mode access
power inline port 2-event
access-session host-mode single-host
access-session closed
access-session port-control auto
mab
spanning-tree portfast
service-policy type control subscriber MAB_Policy
```

```
device-sensor filter-list lldp list lldp-list
tlv name end-of-lldpdu
tlv name chassis-id
tlv name port-id
tlv name time-to-live
tlv name port-description
tlv name system-name
tlv name system-description
tlv name system-capabilities
tlv name management-address
device-sensor notify all-changes
```

```
access-session attributes filter-list list listA
access-session accounting attributes filter-spec include list listA
```

MAB policy

The MAC Authentication Bypass (MAB) policy is defined as follows. Here the control class specifies MAB authentication as the default, and it is used to authenticate a session. MAB is configured as the highest priority (10).

```
policy-map type control subscriber MAB_Policy
  event session-started match-all
  10 class always do-until-failure
  10 authenticate using mab
```

Configuring PoE features

All of the light fixtures receive power via the UPOE+ ports of the Cisco Catalyst 9300 Series Switch. The switch allocates power based on the type of connected light fixtures. Perpetual PoE can help sustain the PoE under specific circumstances in which the switch undergoes a power failure or a soft reload.

The following configurations are not mandatory during migration. Perpetual PoE and Fast PoE have to be configured only for those Cisco Catalyst 9300 Series Switch access ports connected to light fixtures that need to remain illuminated even during a reload or that you want to have turn on quickly after power is restored to the switch.

Perpetual PoE

Perpetual PoE is a PoE enhancement feature on the Cisco Catalyst 9300 Series Switch that helps enable light fixtures connected on catalyst switch ports to continue to receive power during a soft reload of the switch.

To enable Perpetual PoE, perform the following configuration on the Cisco Catalyst 9300 Series switch stack for the light fixture access ports.

Configure the required PoE switch port with the `perpetual-poe-ha` command, which enables Perpetual PoE on that port:

```
interface GigabitEthernet2/1/1
  power inline port perpetual-poe-ha
```

Fast PoE

The Fast PoE feature on Cisco Catalyst 9300 Series Switch ports helps enable Molex light fixtures to illuminate with low brightness within 10 seconds of power restoration on the switch or stack of switches when a power interruption caused the switch to go down.

First configure the Cisco Catalyst 9300 Series switch stack for the light fixture access ports to configure Perpetual PoE. Then configure the required edge port with the `poe-ha` command, which enables Fast PoE on that port:

```
interface GigabitEthernet2/1/1
  power inline port perpetual-poe-ha
  Power inline port poe-ha
```

Configuring security features

The integrated security features on the Cisco Catalyst 9300 Series switch stack can provide threat defense capabilities for mitigating man-in-the-middle attacks and protecting the critical network infrastructure. This section details the switch configurations necessary for basic Layer 2 security features to be enabled as specified in the **Design Guide**.

For more information on configuring the security features, refer to the Security Configuration Guide, Cisco IOS XE 17.9.x:

- [Security Configuration Guide, Cisco IOS XE 17.9.x](#)

IP DHCP snooping

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure IP DHCP snooping:

1. Configure the required port channel connected to the Cisco Catalyst 9500 Series Switch as the DHCP snooping trusted port:

```
interface Port-channel103
 ip dhcp snooping trust
!
```

2. Enable IP DHCP snooping globally for the per-port command to take effect:

```
ip dhcp snooping vlan 30-50
no ip dhcp snooping information option
ip dhcp snooping
!
```

IP Source Guard

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure IP Source Guard:

1. Configure IP Source Guard on the port channels that have trusted IP-to-MAC bindings:

```
interface Port-channel103
 ip verify source
!
```

2. Configure the same on the light fixture access ports:

```
interface GigabitEthernet2/0/1
 ip verify source
!
```

ARP inspection

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure ARP inspection:

1. Configure the required port as an ARP inspection trusted port:

```
interface Port-channel104
  ip arp inspection trust
!
```

2. Configure the same on the light fixture access ports:

```
interface GigabitEthernet2/0/1
  ip arp inspection trust
!
```

3. Enable ARP inspection globally for the required VLANs so that the per-port command takes effect:

```
ip arp inspection vlan 30,40,50
```

ARP rate limiting

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure ARP rate limiting.

Configure ARP rate limiting according to the maximum allowable packet rate on the light fixture access ports.

For example:

```
interface GigabitEthernet2/0/1
  ip arp inspection limit rate 100
```

Port security

You can use port security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to 1 and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

With port security, the MAC addresses of light fixtures that are learned on any secured port will be the only MAC addresses permitted on that port. If any other device is connected on that port, it will throw a security violation alert. So if one light's MAC address is already learned via sticky mode on a particular port, then after connecting a new light, that sticky mapping command needs to be removed first so that the new light's MAC address can be learned.

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure port security.

Configure port security on the light fixture access ports in sticky mode with a maximum allowable number of MAC addresses of 1. Keep the violation as restrict.

For example:

```
interface GigabitEthernet2/0/1
  switchport access vlan 30
  switchport mode access
  switchport port-security violation restrict
  switchport port-security mac-address sticky
  switchport port-security aging type inactivity
  switchport port-security
```

Storm control

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure storm control.

Configure storm control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentages of line rates on the light fixture access ports as follows:

```
interface GigabitEthernet2/0/1
  storm-control broadcast level pps 4000 3500
  storm-control multicast level pps 4000 3500
  storm-control unicast level pps 4000 3500
```

PortFast and BPDU Guard

PortFast and BPDU Guard prevent loops by moving a nontrunking port into an error-disabled state when a BPDU is received on that port. When you enable BPDU Guard on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the Spanning Tree blocking state.

The ports connected to lights don't have to do a BPDU check for Spanning Tree, and therefore those ports can be configured for PortFast and BPDU Guard.

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure PortFast and BPDU Guard.

Enable PortFast on the light fixture access ports, since no BPDUs are expected on that port, and then enable BPDU Guard:

```
interface GigabitEthernet2/0/1
  spanning-tree portfast
  spanning-tree bpduguard enable
```

Port access lists

Port Access Lists (PACLs) filter incoming traffic on Layer 2 interfaces using Layer 3 information, Layer 4 header information, or non-IP Layer 2 information. The PACL feature uses standard or extended IP ACLs or named MAC-extended ACLs that you want to apply to the port.

The ports on which lights are connected should be able to filter packets based on specific Layer 4 port numbers so that unwanted traffic doesn't reach the light. In this scenario, PACLs specifically filter the port numbers that CoreSync Manager uses to communicate with the light fixtures.

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure a PACL:

1. Configure an IP access list to permit the incoming traffic only for Layer 4 port numbers specific to communication between the lights and SCM:

```
ip access-list extended 101
  permit udp any any eq 5683
  permit udp any eq bootpc any eq bootps
  permit udp any eq bootps any eq bootpc
  permit udp any eq 9761
  permit udp any eq snmp any eq snmp
  permit icmp any
```

2. Apply this IP access list for the ingress traffic on the light fixture access ports. For example,

```
interface GigabitEthernet2/1/14
  ip access-group 101 in
  ip access-group 101 out
```

Disabling Telnet

Telnet should be disabled for accessing the device, as it is not secure. The following commands disable Telnet and enable only SSH access to the Cisco Catalyst 9300 Series Switch:

```
line vty 0 15
  transport input ssh
!
```

Configuring network management (SNMP)

SNMP is used to collect information from network devices in order to manage the network.

Refer to [Configuring switch network management, page 20](#), for information on configuring network management on a Cisco Catalyst 9300 Series standalone switch.

Wiring closet access switch stack (Cisco Catalyst 9300 Series stack)

This section covers the Cisco Catalyst 9300 Series wiring closet access switch stack, Layer 2 and Layer 3 networking, security configuration, and network management configurations.

Cisco Catalyst 9300 Series stack configuration

A switch stack can have up to nine stacking-capable switches connected through their StackWise-480 ports. The stack members work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

The switches in the stack are assigned roles as active, standby, and member. However, all switches in the stack are operational. A switch stack always assigns one switch in the active role and one in the standby role. If the active switch becomes unavailable, the standby switch assumes the role of the active switch and continues to keep the stack operational. The active switch controls the operation of the switch stack and is the single point of stackwide management.

In this system implementation, a stack of four Cisco Catalyst 9300 UPOE+ switches (24 UPOE+ ports per switch) are configured in the network topology according to the system requirements. Since each of those switches has 24 UPOE+ ports, light fixtures connected to any of them can be configured via the active switch of the stack.

A higher priority value for a stack member increases the probability of it being elected active switch and retaining its stack member number. The priority value can be 1 to 15. The default priority value is 1. You can display the stack member priority value by using the `show switch EXEC` command.

Note: We recommend assigning the highest priority value to the switch that you prefer to be the active switch. This ensures that the switch is reelected as the active switch if a reelection occurs.

- To install a Cisco Catalyst Switch Data Stack and Stack Manager, refer to the **Cisco Catalyst 9300 Series Switches Hardware Installation Guide** at the following URL:
 - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig.html
- To configure a switch stack, refer to the **Stacking and High Availability Configuration Guide, Cisco IOS XE 17.9.x (Catalyst 9300 Switches)** at the following URL:
 - [Stacking and High Availability Configuration Guide, Cisco IOS XE 17.9.x](#)

When migrating the lighting initial setup on the Cisco Catalyst 9300 Series Switch in the wiring closet, perform the following steps to configure the switch stack:

1. Make sure that the four switches that are going to be part of the stack all have the same boot configuration. Use the `show boot` command to verify their boot parameters:

```
show boot
-----
Switch 3
-----
Current Boot Variables:
BOOT variable = flash: cat9k_iosxe.17.09.01.SPA.conf;
Boot Variables on next reload:
BOOT variable = flash: cat9k_iosxe.17.09.01.SPA.conf;
Allow Dev Key = yes
```

```
Manual Boot = no
Enable Break = yes
```

2. The boot variable for all the switches should be the same image file as shown above. To configure that, use the following show command:

```
boot system switch all flash:cat9k_iosxe.17.09.01.SPA.conf
no boot manual
```

3. Once all the switches boot up with the same image and license, connect them in ring form to bring up the stack. Provision each of the switches from the master as shown below:

```
switch 1 provision C9300-48H
switch 2 provision C9300-48H
switch 3 provision C9300-48H
switch 4 provision C9300-48H
```

4. The switch that is needed to be “active” after a stack reload/reboot should be configured with a higher stack priority value of 15. The priority of the switch can be configured in the Enable mode as shown below:

```
switch 1 priority 15
switch 2 priority 14
```

Network Layer 2 and Layer 3 configuration

This section defines the implementation of VLANs and logical SVI for management traffic on the Cisco Catalyst 9300 Series switch stack.

1. Enable LLDP on the switch stack as follows:

```
C9300-Switch (config)#lldp run
```

2. Enable 2-event classification on all light fixture ports:

```
power inline port 2-event
!
```

3. Configure VLANs, which must be created along with port assignments on the Cisco Catalyst 9300 Series switch stack. The following is an example VLAN configuration:

```
C9300-Switch (config)#vlan 30,40,50
```

4. Configure switch ports connected to light fixtures and wall dimmers on the appropriate lighting VLAN in access mode:

```
interface GigabitEthernet 1/1
 switchport mode access
 switchport access vlan 30
!
```

5. Create a Layer 3 SVI for the VLANs and default gateway as required. The following is an example configuration of a management VLAN SVI on the Cisco Catalyst 9300 Series switch stack:

```
interface Vlan50
 ip address 10.50.0.4 255.255.254.0
!
ip default-gateway 10.50.0.1
```

6. Create port channel uplink interfaces on the Cisco Catalyst 9300 Series switch stack to the campus network aggregation switch (Cisco Catalyst 9500 Series) as shown in [Figure 2](#).

```
interface Port-channel103
  description Etherchannel Link to C9500 Switch
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 30,40,50
```

7. Enable port channels on the appropriate physical switch ports connected to the Cisco Catalyst 9500 Series Switch. The following configuration shows the port channel assignment to physical switch ports:

Physical links to Cisco Catalyst 9500 Series active and standby StackWise Virtual switches:

```
interface TenGigabitEthernet3/1/3
  channel-group 103 mode active
interface TenGigabitEthernet3/1/4
  channel-group 103 mode active
```

8. Enable rapid per-VLAN spanning tree.

```
spanning-tree mode rapid-pvst
!
```

Configuring Auto SmartPort (recommended)

Rather than manually enabling all the commands separately, you can use the Auto SmartPort feature to perform the access port configurations shown in the following sections much more simply. This also saves a great deal of time when several lights are connected on the switch.

Auto SmartPort enables curation of the access ports connected to end hosts such as light fixtures. When an Auto SmartPort macro is configured for a particular type of host device, the moment a port comes up with that type of host device, a macro is triggered that instantly puts a set of preconfigured commands on that access port. For the light fixtures, the macro will enable the basic configuration needed by the light ports (such as port security, ARP inspection, DHCP snooping, and access VLAN). As soon as the port goes down for any reason, the same configuration commands will be removed from the port, which saves the time otherwise needed to manually remove commands from different ports.

If Auto SmartPort causes any issues, it can be disabled in the global mode of the switch, and each of the access port commands can be entered manually to troubleshoot the issue.

For details on the functionality of the Auto SmartPort feature, refer to the **Interface and Hardware Components Configuration Guide, Cisco IOS XE 17.9.x (Catalyst 9300 Switches)**, which can be found at the following URL:

- [Interface and Hardware Components Configuration Guide, Cisco IOS XE 17.9.x](#)

1. The macro needed for the light port configuration is shown below:

```
macro auto execute CISCO_LIGHT_EVENT {
  if [[ $LINKUP == YES ]]
  then conf t
  interface $INTERFACE
  macro description $TRIGGER
```

```
power inline port 2-event
switchport access vlan 30
switchport mode access
power inline port perpetual-poe-ha
power inline port poe-ha
ip arp inspection trust
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
spanning-tree portfast
spanning-tree bpduguard enable
ip verify source
access-session host-mode single-host
access-session port-control auto
mab
  service-policy type control subscriber MAB_Policy
exit
fi
```

```
if [[ $LINKUP == NO ]]
then conf t
interface $INTERFACE
macro description
no switchport access vlan 30
no power inline port poe-ha
no power inline port perpetual-poe-ha
no switchport port-security
no ip arp inspection trust
no switchport port-security
no switchport port-security violation restrict
no switchport port-security mac-address sticky
no spanning-tree portfast
no spanning-tree bpduguard enable no ip verify source
no access-session host-mode single-host
no success-session port-control auto
no mab
exit fi
}
```

2. Auto SmartPort can be enabled globally using the following command:

```
macro auto global processing
```

Configuring PoE features

All light fixtures receive power via the UPOE+ ports of the Cisco Catalyst 9300 Series Switch. The switch allocates powers to the light fixtures connected to it based on their type. The Perpetual PoE feature can help sustain the PoE when the switch undergoes a power failure or a soft reload.

The following configurations are not mandatory during initial installation. They have to be configured only on those access ports of a Cisco Catalyst 9300 Series Switch to which certain light fixtures are connected that need to remain illuminated during a reload or that you want to be able to turn on quickly after power is restored on the switch.

Perpetual PoE

To configure Perpetual PoE, perform the following configuration on the Cisco Catalyst 9300 Series switch stack for the light fixture access ports.

Configure the required edge port with the `perpetual-poe-ha` command, which enables Perpetual PoE on that port:

```
interface GigabitEthernet2/1/1
    power inline port perpetual-poe-ha
```

Fast PoE

The Fast PoE feature on Cisco Catalyst 9300 Series switch ports helps enables Molex light fixtures to illuminate with low brightness within 10 seconds (about 15W of power is given via ethernet cable two pair by the switch hardware) after power is restored on a switch or stack of switches, when power interruption caused the switch to go down.

Configure the required edge port with the `poe-ha` command, which enables Fast PoE on that port:

```
interface GigabitEthernet2/1/1
    power inline port perpetual-poe-ha
    power inline port poe-ha
```

Configuring security features

The integrated security features on the Cisco Catalyst 9300 Series switch stack can provide threat defense capabilities for mitigating man-in-the-middle attacks and protecting the critical network infrastructure. This section details the switch configurations necessary for basic Layer 2 security features to be enabled as specified in the **Design Guide**.

For more information on configuring the security features, refer to the consolidated **Security Configuration Guide, Cisco IOS XE 17.9.x (Catalyst 9300 Series)** at the following URL:

- [Security Configuration Guide, Cisco IOS XE 17.9.x](#)

IP DHCP snooping

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure IP DHCP snooping:

1. Configure the required port as a DHCP snooping trusted port:

```
interface Port-channel103
    ip dhcp snooping trust
!
```

-
2. Enable IP DHCP snooping globally for the per-port command to take effect:

```
ip dhcp snooping vlan 30-50
no ip dhcp snooping information option
ip dhcp snooping
!
```

IP Source Guard

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure IP Source Guard:

1. Configure IP Source Guard on the ports that have trusted IP-to-MAC bindings:

```
interface Port-channel103
ip verify source
!
```

2. Configure the same on the light fixture access ports:

```
interface GigabitEthernet2/0/1 ip verify source
!
```

ARP inspection

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure ARP inspection:

1. Configure the required port as ARP inspection trusted port:

```
interface Port-channel103
ip arp inspection trust
!
on light fixture access ports,
interface GigabitEthernet2/0/1
ip arp inspection trust
!
```

2. Enable ARP Inspection globally for the required VLANs so that the per-port command takes effect:

```
ip arp inspection vlan 30,40,50
```

ARP rate limiting

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure ARP rate limiting.

Configure ARP rate limiting according to the maximum allowable packet rate on the light fixture access ports.

For example:

```
interface GigabitEthernet2/0/1
ip arp inspection limit rate 100
```

Port security

You can use port security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to 1 and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

With port security, the MAC addresses of light fixtures that are learned on any secured port will be the only MAC addresses permitted on that port. If any other device is connected on that port, it will throw a security violation alert.

Perform the following step on the Cisco Catalyst 9300 Series stack switch to configure port security.

Configure port security on light fixture access ports in sticky mode with the maximum allowable number of MAC address as 1. Keep the violation as restrict. For example,

```
interface GigabitEthernet2/0/1
  switchport access vlan 30
  switchport mode access
  switchport port-security violation restrict
  switchport port-security mac-address sticky
  switchport port-security aging type inactivity
  switchport port-security
```

Storm control

Perform the following step on the Cisco Catalyst 9300 Series stack switch to configure storm control.

Configure storm control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentages of line rates on light fixture access ports as follows:

```
interface GigabitEthernet2/0/1
  storm-control broadcast level pps 4000 3500
  storm-control multicast level pps 4000 3500
  storm-control unicast level pps 4000 3500
```

PortFast and BPDU Guard

PortFast and BPDU Guard prevent loops by moving a nontrunking port into an error-disabled state when a BPDU is received on that port. When you enable BPDU Guard on the switch, Spanning Tree shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the Spanning Tree blocking state.

The ports connected to lights don't have to do a BPDU check for Spanning Tree, and therefore those ports can be configured for PortFast and BPDU Guard.

Perform the following step on the Cisco Catalyst 9300 Series switch stack to configure PortFast and BPDU Guard.

Enable PortFast on the light fixture access ports, since no BPDUs are expected on that port, and then enable BPDU Guard:

```
interface GigabitEthernet2/0/1
  spanning-tree portfast
  spanning-tree bpduguard enable
```

Port access lists

PACLs filter incoming traffic on Layer 2 interfaces using Layer 3 information, Layer 4 header information, or non-IP Layer 2 information. The PACL feature uses standard or extended IP ACLs or named MAC-extended ACLs that you want to apply to the port.

The ports on which lights are connected should be able to filter packets based on specific Layer 4 port numbers so that unwanted traffic doesn't reach the light. PACLs, in this scenario, filter specifically the port numbers that CoreSync Manager uses to communicate with the lights.

Perform the following steps on the Cisco Catalyst 9300 Series switch stack to configure a PACL:

1. Configure an IP access list to permit the incoming traffic only for Layer 4 port numbers specific to communication between the lights and SCM:

```
ip access-list extended 101
  permit udp any any eq 5683
  permit udp any eq bootpc any eq bootps
  permit udp any eq bootps any eq bootpc
  permit udp any any eq 9761
  permit udp any eq snmp any eq snmp
  permit icmp any any
```

2. Apply this IP access list for the ingress traffic on the light fixture access ports. For example,

```
interface GigabitEthernet2/1/14
  ip access-group 101 in
  ip access-group 101 out
```

Disabling Telnet

Telnet should be disabled for accessing the device, as it is not secure. The following commands disable Telnet and enable only SSH access to the Cisco Catalyst 9300 Series Switch.

```
line vty 0 15
  transport input ssh
!
```

Configuring Auto SmartPort (optional)

Auto SmartPort enables automatic configuration of the access ports connected to end hosts such as light fixtures. When an Auto SmartPort macro is configured for a particular type of host device, the moment a port comes up with that type of host device, a macro is triggered that instantly puts a set of preconfigured commands on that access port. For the light fixtures, the macro will enable the basic configuration needed by the light ports (such as port security, ARP inspection, DHCP snooping, and access VLAN). As soon as the port goes down for any reason, the same configuration commands will be removed from the port, which saves the time otherwise needed to manually remove commands from different ports.

1. The macro needed for the light port configuration is shown below:

```
macro auto execute CISCO_LIGHT_EVENT {
if [[ $LINKUP == YES ]]
then conf t
interface $INTERFACE
macro description $TRIGGER
power inline port 2-event
switchport access vlan 30
switchport mode access
power inline port poe-ha
power inline port perpetual-poe-ha
ip arp inspection trust
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
spanning-tree portfast
spanning-tree bpduguard enable
ip verify source
access-session host-mode single-host
access-session port-control auto
mab
service-policy type control subscriber MAB_Policy
exit
if [[ $LINKUP == NO ]]
then conf t interface $INTERFACE no macro description
no switchport access vlan 30 no power inline port poe-ha
no power inline port perpetual-poe-ha
no switchport port-security
no ip arp inspection trust
no switchport port-security
no switchport port-security violation restrict
no switchport port-security mac-address sticky
no spanning-tree portfast
no spanning-tree bpduguard enable
```

```
no ip verify source
no access-session host-mode single host
no access-session port-control auto
exit fi
}
```

2. Auto SmartPort can be enabled globally using the following command.

```
macro auto global processing
```

Configuring network management (SNMP)

SNMP is used to collect information from network devices in order to manage the network.

Refer to [Configuring switch network management, page 20](#), for information on configuring network management on a Cisco Catalyst 9300 Series switch stack.

Provisioning light fixtures

This section describes how to commission the light fixtures using MoDiag and CoreSync Manager when migrating the light fixtures from initial installation to the existing converged campus network.

During the migration phase, the light fixtures are assigned IP addresses from the DHCP pool configured on the Cisco Catalyst 9500 Series aggregation switch in the light fixtures' VLANs. The MoDiag application is required to set the CoreSync Manager IP address for light fixtures to communicate with CoreSync Manager. Refer to the **Molex MoDiag User Guide** for detailed steps on setting up the IP address.

A new CoreSync Manager Design Tool project must be created based on the new IP addresses of the light fixtures that are required to be commissioned in the campus network. Refer to the **Molex CoreSync Manager User Guide** for detailed steps for this procedure.

Implementing data center applications for lighting

This section covers the implementation of required data center applications and services in a campus network for Cisco and Molex Smart Building Solution deployment, as shown in [Figure 2](#). It includes the following major topics:

- [Configuring the firewall, page 39](#)
- [Configuring Cisco UCS, page 43](#)
- [Configuring network device authentication \(ISE\), page 44](#)
- [Configuring network management \(Cisco Catalyst Center\), page 50](#)
- [Configuring Molex CoreSync Manager services, page 57](#)

Configuring the firewall (Cisco Firepower 4112)

In the Cisco and Molex Smart Building Solution, when migrating a lighting initial setup to a campus network, the Cisco Firepower 4112 is recommended in the campus network data center edge as the firewall to protect the applications in the data center. Traffic coming into the data center from the network, along with traffic from the lighting network, should pass through the Firepower firewall.

The Firepower 4112 is configured to operate in routed mode. Several tasks are required to complete the firewall configuration. The workflow is shown in [Figure 7](#).

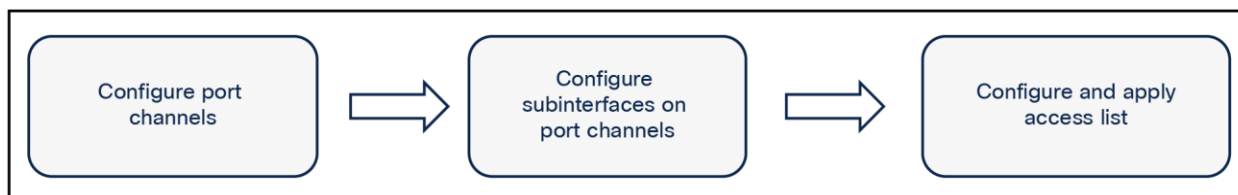


Figure 7.
Firewall configuration flow diagram

Configuring the port channel to the network

Configure the port channel on the firewall toward the data center and toward the campus network aggregation switch (Cisco Catalyst 9500 Series) as per the topology in [Figure 2](#). The port channel can be created by performing the following steps:

1. The firewall is configured with a port channel having two member links to the Cisco Catalyst 9500 Series. The port channel includes the two 10 Gigabit Ethernet interfaces available on the Firepower 4112. No name or security level is assigned to the port channel.

```
interface Port-channel2
description C9500 Uplink
!
interface TenGigabitEthernet0/6
channel-group 2 mode active
!
interface TenGigabitEthernet0/7
channel-group 2 mode active
```

2. VLAN subinterfaces provide access to different components in the network, such as the data center and management network. Subinterfaces based on VLANs are configured on the port channel. The VLAN and subinterface configuration for campus network access is as follows:

```
interface Port-channel12.50
vlan 50
```

3. The Firepower 4112 is configured with a port channel having two member links to the Cisco Catalyst 9300 Series data center switch. The port channel includes the two Gigabit Ethernet interfaces available on the Firepower 4112. No name or security level is assigned to the port channel.

```
interface Port-channell1
description #To DC switch##
!
```

```
interface GigabitEthernet0/4
  channel-group 1 mode active
```

```
!
```

```
interface GigabitEthernet0/5
  channel-group 1 mode active
```

4. VLAN subinterfaces provide access to different components in the network, such as the data center and management network. Subinterfaces based on VLANs are configured on the port channel. The VLAN and subinterface configuration for data center network access is as follows:

```
interface Port-channel1.70
  vlan 70
```

Configuring firewall interfaces

The firewall interfaces are configured with names, security levels, and IP addresses. [Table 7](#) summarizes the interface configuration used, along with the corresponding zones.

Table 7. Firewall interface configuration

Zone	Interface	Security level	Description
Inside	Port-channel1.70	100	Used to connect to the data center
Outside	Port-channel2.50	0	Used to connect to the campus network

```
!
```

```
interface Port-channel1.70 nameif inside
  security-level 100
  ip address 10.70.0.1 255.255.254.0
```

```
!
```

```
interface Port-channel2.50 nameif outside
  security-level 0
  ip address 10.50.0.2 255.255.254.0
```

```
!
```

The firewall security level can be configured between 0 and 100; 0 is the least secure zone, and 100 is the most secure zone.

Configuring access control lists

By default, the Firepower 4112 denies all traffic moving from a lower security level to a higher security level. Access Control Lists (ACLs) are configured to enable required traffic between interfaces. The Access Control Entries (ACEs) are as follows:

ACL to allow traffic from the campus network to data center:

```
access-list campustodatacenter extended permit ip 10.30.0.0 255.255.254.0 10.70.0.0
255.255.254.0
access-list campustodatacenter extended permit ip 10.50.0.0 255.255.254.0 10.70.0.0
255.255.254.0
access-list campustodatacenter extended permit ip 10.40.0.0 255.255.254.0 10.70.0.0
255.255.254.0
```

Apply the ACL on the outside interface (toward the corporate network):

```
access-group campustodatacenter in interface outside
```

The access-list configurations above are very simplistic and rudimentary in nature to allow the VLANs to communicate via IP, but as component parameters are discovered later down the line, it is best practice to tighten the parameters of the access-list configurations further by including protocols, port numbers, and other considerations that can be specified to allow only the necessary traffic between the gateways and applications, services, and/or virtual machines. The ports and protocols used between CoreSync, the gateways, and other parts of the network are shown in the table below.

Table 8. Ports and protocols used between CoreSync, gateways, and network

Protocol	Port number
FTP data transfer	20
FTP control command	21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DHCP	67
DHCP	68
TFTP (Trivial File Transfer Protocol)	69
HTTP (Hyper Text Transfer Protocol)	80
SNMP (Simple Network Management Protocol)	161
SNMP traps	162
HTTPS (Hyper Text Transfer Protocol Secure)	443
CoAP (Constrained Application Protocol)	5683

The ports used by the gateway to communicate back to CoreSync are shown in the following table.

Table 9. Ports and protocols back to CoreSync

Protocol	Port number
CoAP/UDP	5683
UDP	9760, 9761, 9762
JSON-RPC	8545
SNMP	161, 162
TFTP/UDP	69

The ports used by CoreSync are shown in the following table.

Table 10. Ports and protocols used by CoreSync

Protocol	Port number
CoAP/UDP	5683
UDP	9760, 9761, 9762
JSON-RPC	8545
TCP	80, 8080, 8090
NTP	123

The ports used via BACnet and REST API are shown in the following table.

Table 11. Ports and protocols used via BACnet and REST API

Protocol	Port number
CoreSync server	80
Molex API (TCP)	3000
MongoDB	27017
BACnet Configuration Tool (BCT)	85, 90, 96
BACnet Gateway UDP port range	47808 - 47823
Data Simulator	100

Cisco recommends that administrators have discussions with Molex to come up with an optimal configuration that will allow all the necessary ports to be open for the PoE solution to operate as intended while restricting all other communication, following the principles of a zero-trust philosophy.

Configuring Cisco UCS

Configuring the virtualization infrastructure

This section describes how to deploy a Cisco UCS C240 M6 server to provide the virtualized infrastructure required to deploy virtual machines (VMs) (for example, Cisco Catalyst Center and Cisco ISE). Where applicable, refer to the following Cisco and VMware documentation for details:

- **Cisco UCS C240 M6 Server Installation and Service Guide** at the following URL:
 - https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c240m6/install/b-c240-m6-install-guide.html.
- **Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 4.3** at the following URL:
 - https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_3/b_cisco_ucs_c-series_gui_configuration_guide_43.html.

Note: The Cisco UCS C-Series server platform discussed in this section is used for hosting applications such as Network Time Protocol (NTP), Cisco Catalyst Center infrastructure, and ISE through server virtualization. However, any UCS server series or desktop server can be chosen for deployment if the application's hardware requirements match the server hardware resources.

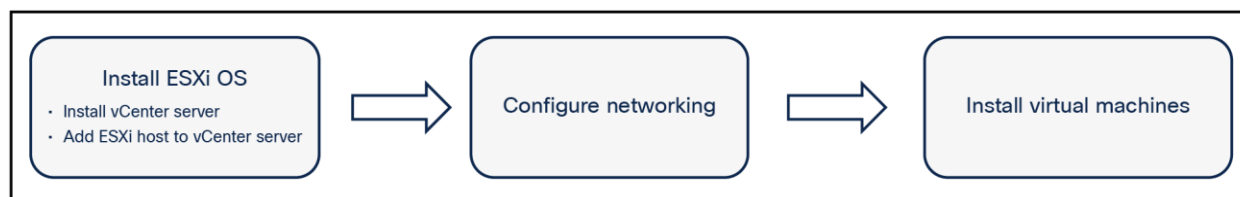


Figure 8.
Flow diagram for virtualization configuration

ESXi installation and configuration

To install and configure ESXi on a UCS C240 server, refer to the “Installing & Setting Up ESXi” section in the **vSphere Installation and Setup Guide**.

Refer to the detailed vCenter server installation steps in the “Installing vCenter Server” section of the **vSphere Installation and Setup Guide**.

Note: We recommend immediately completing all licensing through the vCenter management application during the ESXi installation process.

ESXi networking

This section covers the ESXi networking configuration for the UCS C-Series server platform for data center applications such as Cisco Catalyst Center, Cisco ISE, and the NTP server as shown in [Figure 2](#).

Note: The data center networking switches and configurations may vary based on the enterprise IT network data center deployment. Where applicable, follow the deployment procedures used in the enterprise data center deployment and enable networking according to the production campus network.

To configure ESXi networking on the UCS ESXi host, refer to **Configuring Network Settings** at the following URL:

- <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-26F3BC88-DAD8-43E7-9EA0-160054954506.html>

Configuring network device authentication (ISE)

This section covers how to deploy Cisco ISE 3.0 on the UCS server platform in the data center for network device authentication (RADIUS) and security.

Installing Cisco ISE

The prerequisites and the necessary information to install ISE can be found in the **Cisco Identity Services Engine Installation Guide, Release 3.0**, at the following URL:

- https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install_guide/b_ise_InstallationGuide30.html

The above book describes different deployment scenarios with ISE. Choose a scenario that meets your use case needs.

Configuring Cisco ISE

ISE 3.0 is used to provide device authentication and authorization in the network via RADIUS. It is deployed in a VM and assigned an IP address in the VLAN 70 residing behind the firewall. The firewall ports need to be opened for RADIUS communication from the management VLAN 50 to ISE.

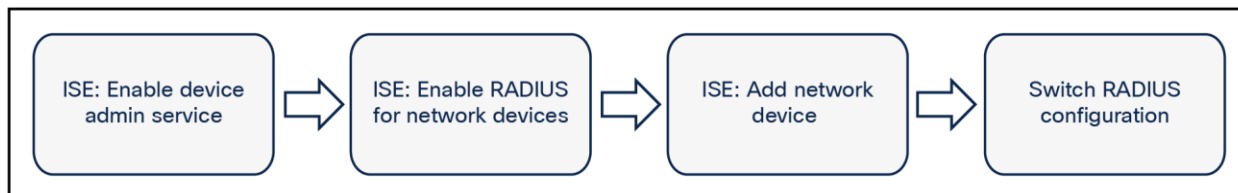


Figure 9.
AAA configuration flow

Switch AAA configuration

Perform the following steps on each access switch in the network (for example, the Cisco Catalyst 9300 Series switch stacks in the deployment, as shown in [Figure 2](#)) to configure Authentication, Authorization, and Accounting (AAA).

The steps described in this section should also be part of the switch configuration files(s), if you are using the Smart Install feature to configure the switches as described in [Initial Installation of the Lighting Network, page 9](#).

1. On the switches, configure ISE as the RADIUS server:

ISE is the name of the RADIUS defined server. Any user-defined name can be used. The RADIUS server "ISE" is added to the aaa group server.

```
aaa new-model
aaa group server radius ise-group
  server name ISE
radius server ISE
  address ipv4 10.70.0.100 auth-port 1645 acct-port 1646
  key cisco
```

2. Create a local user with full privilege for fallback with the username command shown here:

```
username administrator password 0 C1sco
username cisco password 0 cisco
```

3. Configure login authentication, exec, and console authorization using the following commands.

These commands show the different authentication groups that could be created.

```
aaa authentication login default group ise-group local
aaa authentication login SMIconsole none
aaa authentication login telnetConsole local
aaa authentication enable default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

4. Use the method telnetConsole on VTY authentication and authorization.

After the above step, the different authentication groups that have been created should be attached to their respective login type.

```
line con 0
  login authentication SMIconsole
  stopbits 1
  speed 115200
line vty 0 4
  login authentication telnetConsole
line vty 5
  login authentication telnetConsole
```

ISE configuration

Perform the following steps on the ISE server to enable RADIUS-based device authentication and authorization:

1. Log in to ISE. [Figure 10](#) shows the ISE summary after successful login.

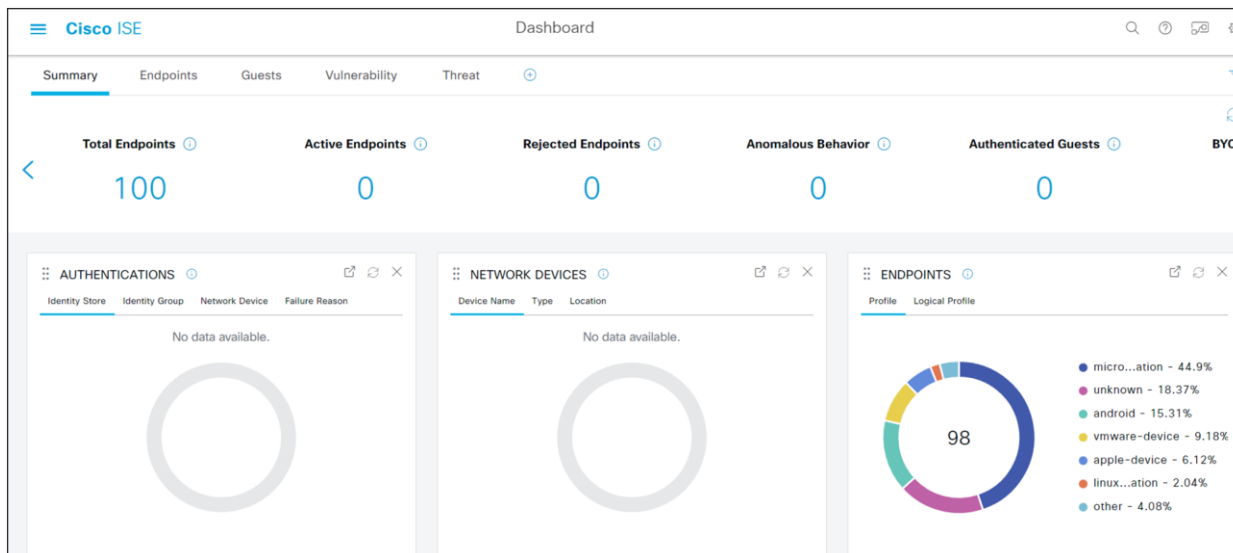


Figure 10.
Login Success page

2. Add the Cisco Catalyst 9300 Series standalone switch or the stack as a network device to ISE. To add a network device, select **Network Devices** from **Administration > Network Resources**.

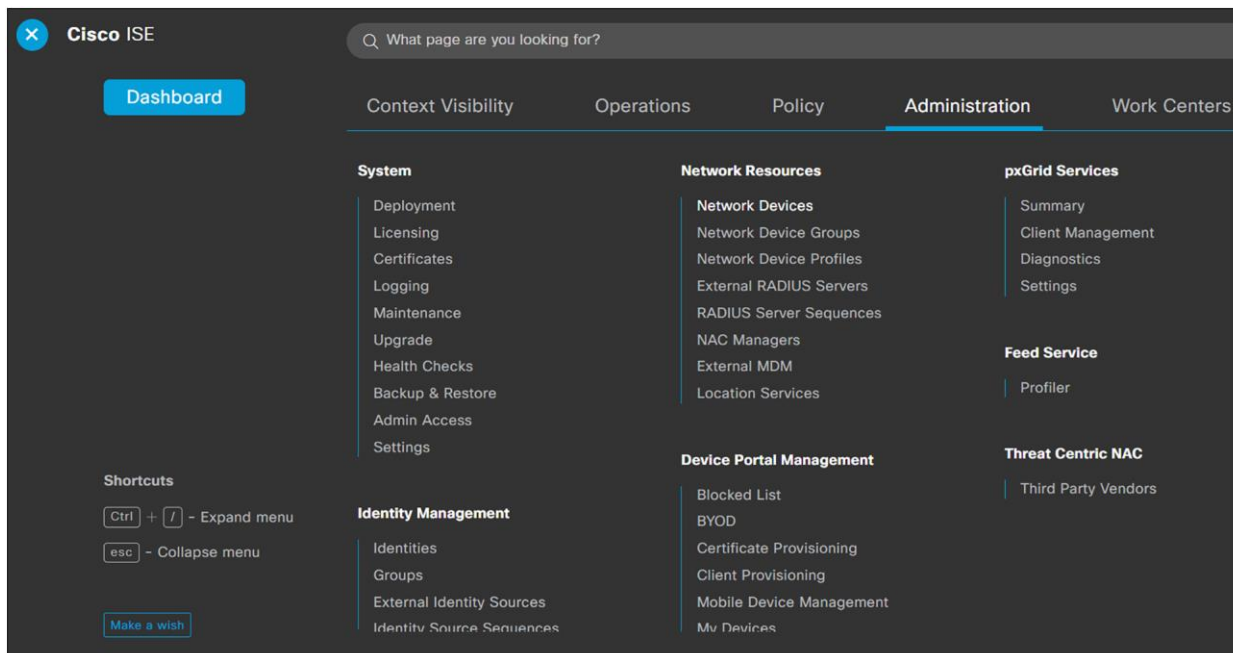


Figure 11.
Select Network Devices

3. Upon selecting Network Devices, the page should display the devices (if any) that were added.

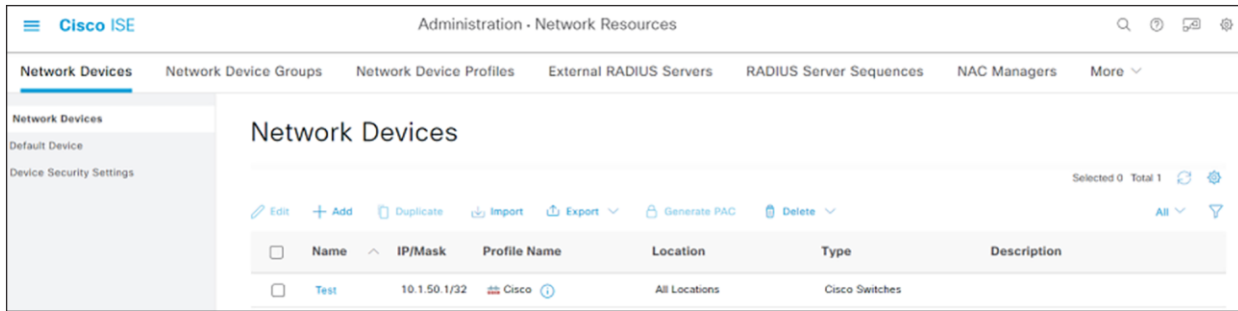


Figure 12.
Network Devices page

4. To add a network device to the list, click **Add** and enter the device name and the correct IP address. The IP address of the network device should be reachable from ISE.

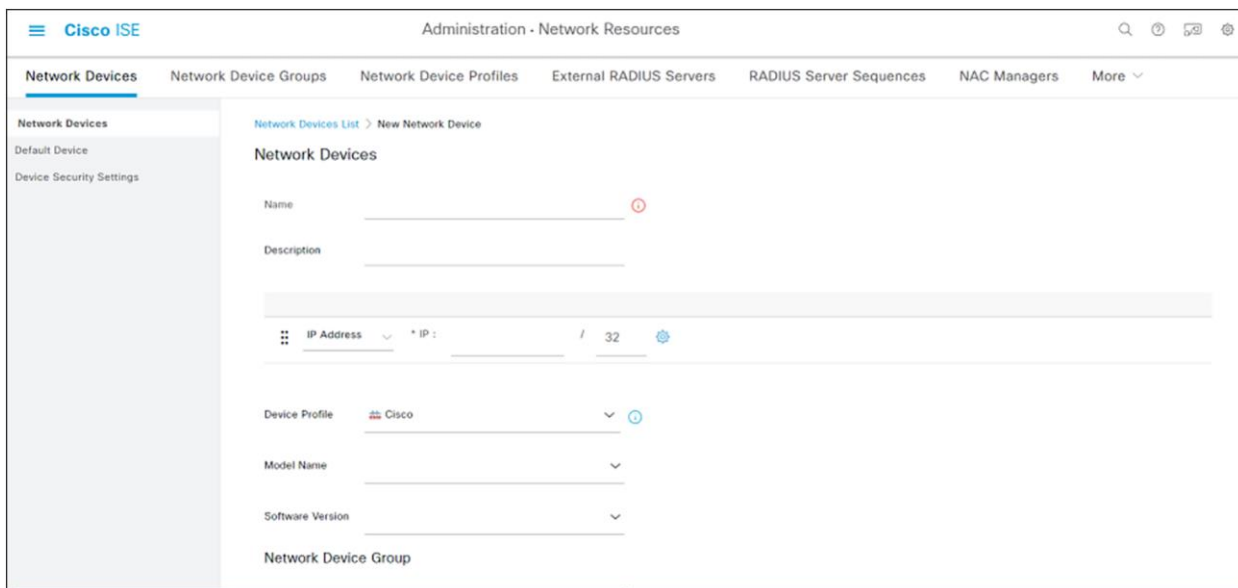


Figure 13.
Adding a network device

5. After adding a network device, select the RADIUS authentication settings and enter the preshared key that is common to the network device. This preshared key should be same as the key added in the AAA configuration of the network device.

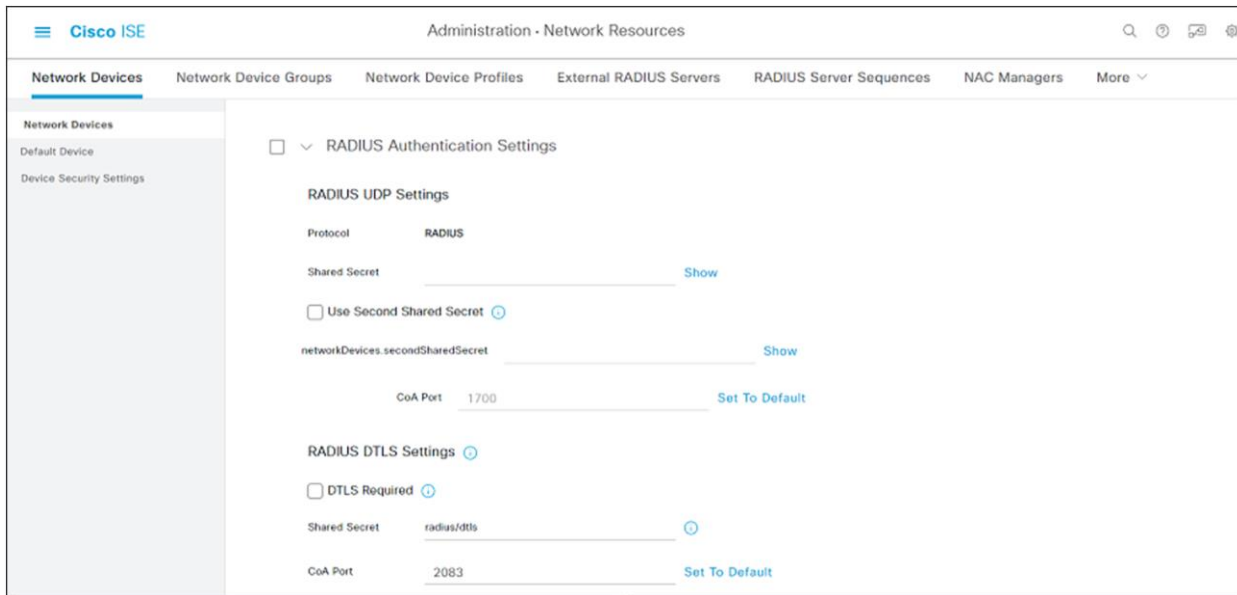


Figure 14.
RADIUS authentication settings

- To create an identity (user), go to **Administration > Identity Management > Identities > Users**. Add the name and the login password. These credentials will be used to log in to the network device from ISE.

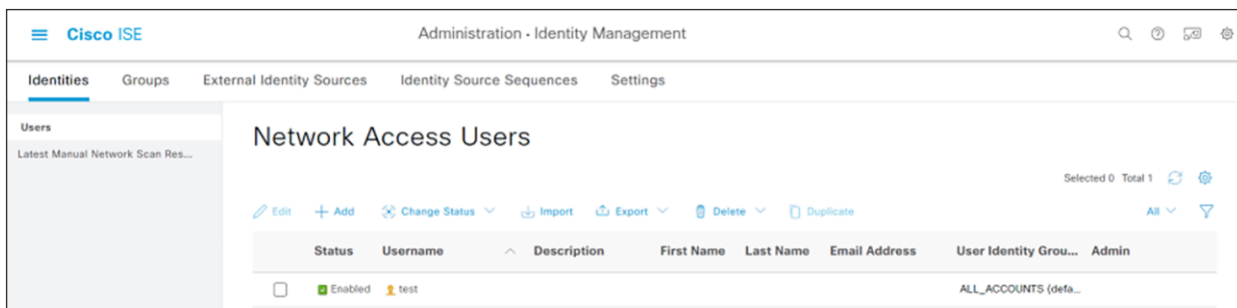


Figure 15.
Adding a user identity in Identity Management

The screenshot shows the 'New Network Access User' configuration page in Cisco ISE. The page is titled 'Administration - Identity Management' and has a navigation menu with 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' section is active, showing a sidebar with 'Users' and a main content area with the following form:

- Network Access User** (Section Header)
- * Username: [Text Input]
- Status: Enabled (Dropdown)
- Email: [Text Input]
- Passwords** (Section Header)
- Password Type: Internal Users (Dropdown)
- Password: [Text Input] Re-Enter Password: [Text Input]
- * Login Password: [Text Input]
- Enable Password: [Text Input]

Figure 16.
Creating a new user in Identity Management

This completes the ISE RADIUS configuration for network devices authentication and authorization.

7. After performing the above steps, the endpoints can be seen in **Context Visibility > Endpoints**.

The screenshot shows the 'Context Visibility - Endpoints' page in Cisco ISE. The page displays a table of endpoints with the following columns: MAC Address, Status, IP Address, Username, Hostname, Location, Endpoint Profile, Authentication Failure Reason, Authentication Policy, and Authorization Policy. The table contains 10 rows of data, each representing an endpoint with its respective MAC address, IP address, and profile.

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason	Authentication Policy	Authorization Policy
00:00:20:00:44:00		10.254.11.193		sview2qv2...		Unknown			
00:0C:29:27:D1:EF		10.254.11.188				VMWare-Device			
00:0C:29:4B:41:AC		10.254.11.206		DESKTOP-...		Microsoft-Workstat...			
00:0C:29:4D:81:5A		10.254.11.194				VMWare-Device			
00:0C:29:58:91:2C		10.254.11.222				VMWare-Device			
00:0C:29:6A:52:...						VMWare-Device			
00:0C:29:6A:52:E0		10.254.11.193		firepower		VMWare-Device			
00:0C:29:6C:B9:25		10.254.11.229		DESKTOP-...		Microsoft-Workstat...			
00:0C:29:9A:CD:3F						VMWare-Device			
00:0C:29:A2:E2:AE		10.254.11.184				Linux-Workstation			

Figure 17.
Endpoints list

- To see the mud-url, click one of the endpoints, select the **Attributes** tab, and scroll to the bottom of the tab. This is shown in the figure below.

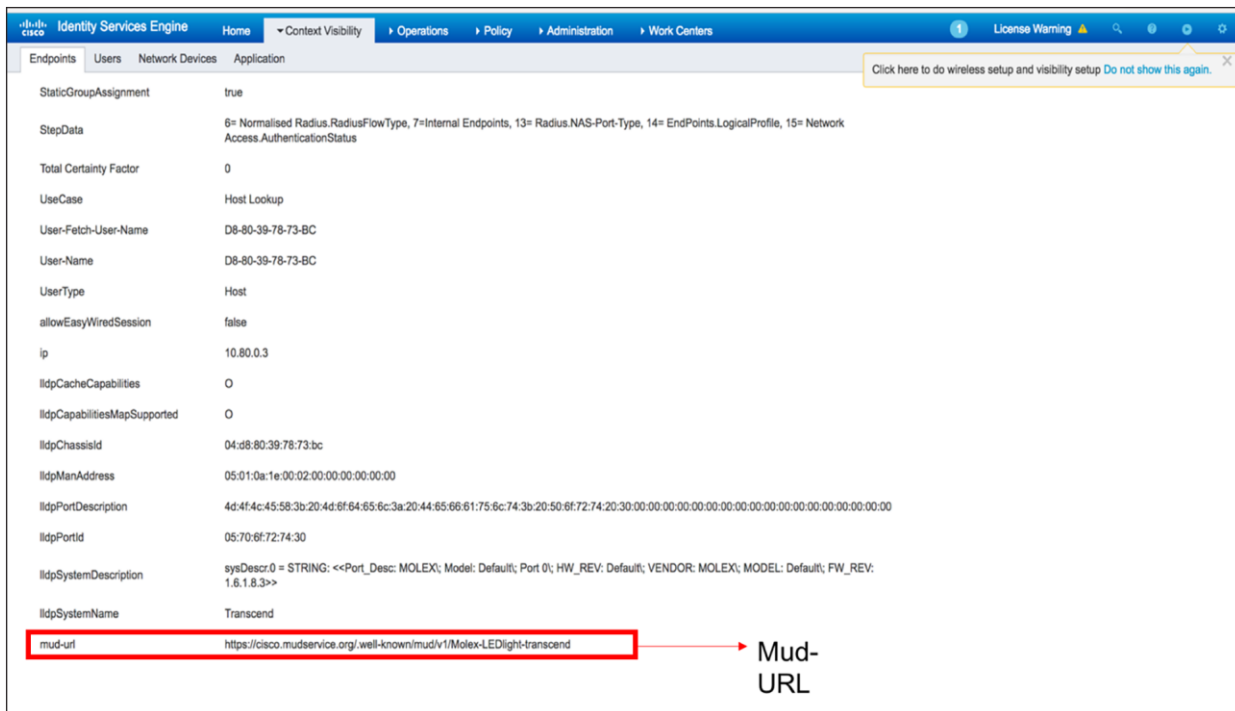


Figure 18.
Mud-URL

Network management and monitoring with Cisco Catalyst Center

Cisco Catalyst Center is a network management and automation platform that helps organizations simplify and automate their network operations. It provides a single pane of glass for managing all aspects of the network, from devices to applications to security policies. Cisco Catalyst Center provides not only network management but also Assurance with PoE analytics.

Installing the Cisco Catalyst Center appliance

- Install the Cisco Catalyst Center appliance or VM based on the following URL resources:

VM on AWS

Cisco Catalyst Center on AWS Deployment Guide:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/dna-center-va/aws/deploy/1_5/b_deploy_cisco_dna_center_va_aws_deployment_guide_1_5.html
- <https://software.cisco.com/download/home/286316341/type/286318832/release/2.3.3.7?catid=268439477>

-
2. Launch your VMware vSphere client and connect to the ESXi host or vCenter server.
 3. Create a new VM to mount the ISO file to and install Cisco Catalyst Center by following the instructions in **Create a Virtual Machine with the New Virtual Machine Wizard** at the link below:
 - https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-AE8AFBF1-75D1-4172-988C-378C35C9FAF2.html
 4. After mounting the downloaded ISO file to the VM, turn on the VM and follow the prompts from the console to complete installation and bootup of Cisco Catalyst Center.

For detailed installation instructions, refer to the “Install and Upgrade Guides” sections for the corresponding appliance and virtual deployments in the Cisco Catalyst Center Install and Upgrade Guides at the following URL:

- <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html>

Cisco Catalyst Center physical appliance installation guide:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_3_7_2ndGen.html

Onboarding devices onto Cisco Catalyst Center for management

For more details, refer to the “Discover and Manage Network Inventory and Topology” section in the **Cisco Catalyst Center User Guide** at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center_ug_2_3_7/b_cisco_dna_center_ug_2_3_7_chapter_010.html

The following are the high-level steps for adding the device to Cisco Catalyst Center:

1. Launch the Cisco Catalyst Center GUI using a web browser with its IP address.
2. Log in to the GUI with the username and password.
3. On the main menu, click **Provision > Network Devices > Inventory**.

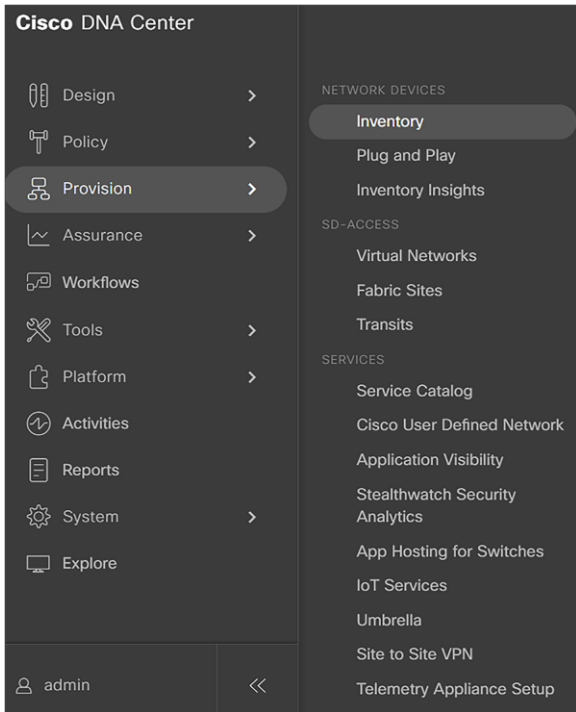


Figure 19.
Cisco Catalyst Center main menu

4. Click **Add Device** and enter the prompted values to add the device to the network architecture.

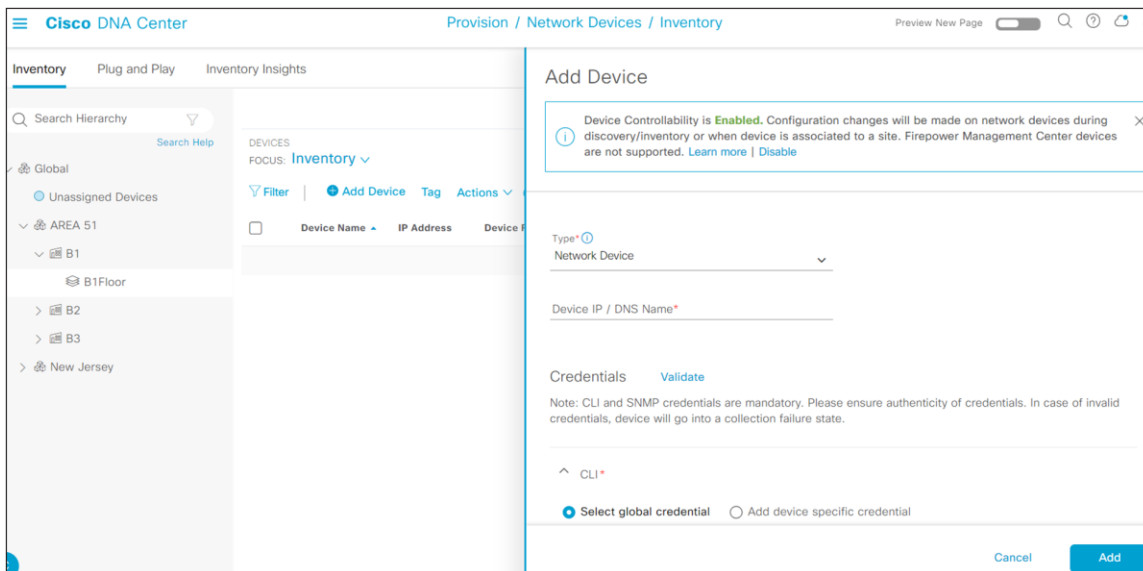


Figure 20.
Cisco Catalyst Center inventory form

5. After adding the switch to the inventory, use the Template Editor to create a specific Interface configuration template based on your design and configuration preferences.

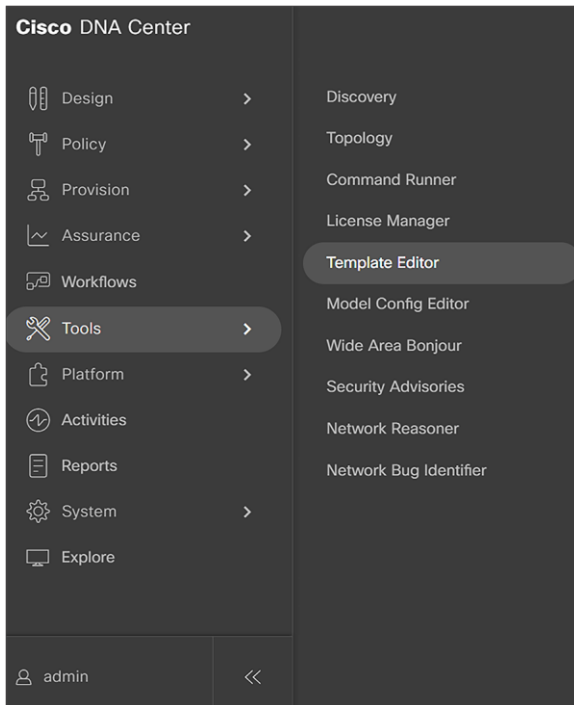


Figure 21.
Cisco Catalyst Center main menu

6. Once the desired configurations have been entered into the editor, commit the changes and apply to the switch to provision the template to the switch and thus the switch ports.

For more details, refer to the “Create Templates to Automate Device Configuration Changes” section in the **Cisco Catalyst Center User Guide** at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center Ug 2 3 7/b_cisco_dna_center Ug 2 3 7 chapter_01000.html?bookSearch=true

Managing network switch software using Cisco Catalyst Center

Cisco Catalyst Center Software Image Management (SWIM) can be leveraged to upgrade the software image on the inventory of network devices. For detailed instructions on managing and upgrading lighting network switch software images, refer to the “Manage Software Images” section of the **Cisco Catalyst Center User Guide, Release 2.3.7**, at the link below:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center Ug 2 3 7/b_cisco_dna_center Ug 2 3 7 chapter_0100.html

Available software image files can be found under **Design > Image Repository**.

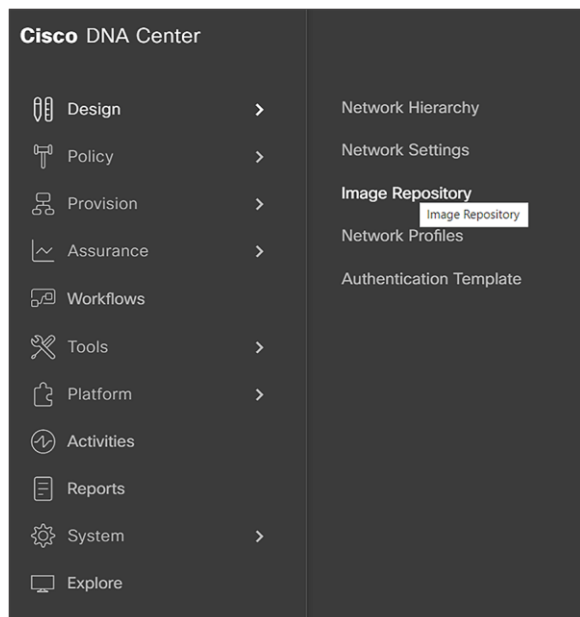


Figure 22.
Cisco Catalyst Center main menu

After the images have been imported using any of the supported protocols, they can be provisioned to a desired network device by clicking **Assign** to the right of the image filename and following through the prompts to select the network device.

Monitoring network health and PoE endpoint health using Cisco Catalyst Center Assurance

To monitor the health of network devices, enable telemetry collection on Cisco Catalyst Center for the devices from the inventory page.

Once a switch is provisioned for telemetry, it automatically sends the telemetry every 10 minutes to Cisco Catalyst Center. Cisco Catalyst Center collects the telemetry and put the data into the Assurance dashboards.

Cisco Catalyst Assurance for network health monitoring and PoE Assurance

Assurance provides a comprehensive solution to help assure better and more consistent service levels to meet growing business demands. It addresses not just reactive network monitoring and troubleshooting, but also proactive and predictive aspects of running a network and helping ensure optimal client, application, and service performance.

- In the top left corner, click the menu icon and choose **Assurance > Health**.

The overall health dashboard is displayed.

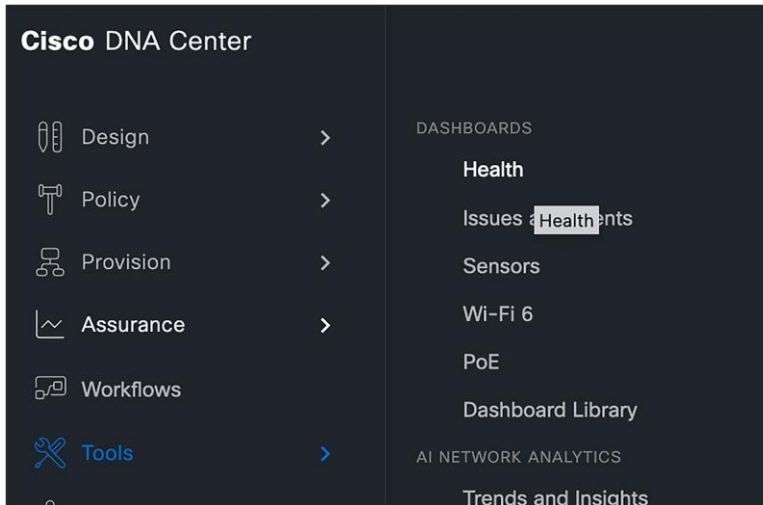


Figure 23.
Cisco Catalyst Center main menu

Cisco Catalyst Center PoE Assurance

Cisco Catalyst Center PoE-focused Assurance dashboards help to monitor and troubleshoot PoE devices in the network. They provide a multicontextual yet single pane of glass for viewing PoE-related information, such as the power budget, power used, power remaining, and power usage of PoE-powered devices.

Cisco Catalyst Center PoE Assurance can also be used to troubleshoot PoE problems, such as devices that are not receiving enough power or devices that are drawing too much power.

Here are some of the key dashboard items on Cisco Catalyst Center PoE Assurance:

- PoE statistics for each connected Powered Device (PD) on the switch
- PoE power consumption information for each switch
- View of PoE power consumption across all switches
- View of all monitored PDs with status
- View of types of PDs, along with the PoE consumption
- Insights into different capabilities of PoE, such as UPOE+, Fast PoE, compliance
- Usage load of all switches, bucketized with range

Configuring telemetry on Cisco Catalyst Center to collect PoE telemetry from the network

In the Cisco Catalyst Center GUI, click the left menu icon and choose **Provision > Inventory**.

Once the Inventory window appears, check the check boxes next to the network devices that have been set up for PoE telemetry.

From the Actions drop-down list, choose **Telemetry > Update Telemetry Settings**.

Check the **Force Configuration Push** check box. (This option causes the configuration changes to be pushed to the device.)

The PoE Assurance dashboard in Cisco Catalyst Center is located under **menu icon -> Assurance -> PoE**.

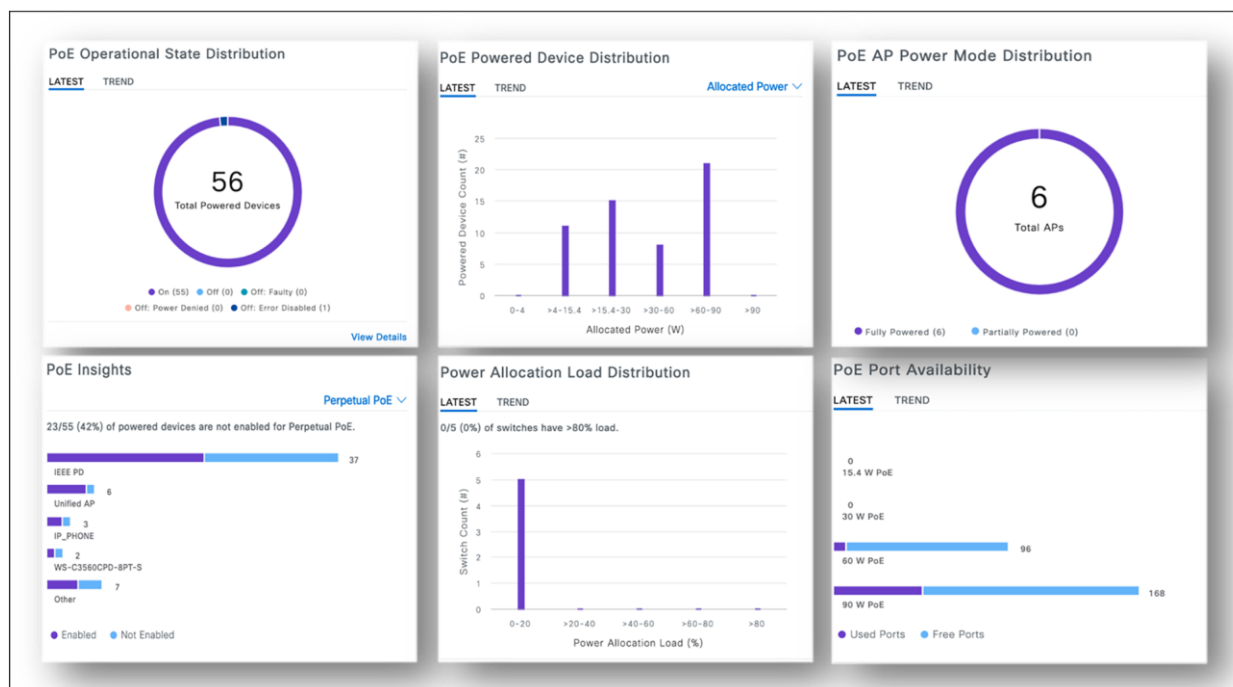


Figure 24.
Cisco Catalyst Center PoE Assurance dashboard

For detailed instructions on monitoring and troubleshooting the PoE lighting infrastructure, refer to the “Monitor and Troubleshoot Your Network” section of the **Cisco Catalyst Center User Guide, Release 2.3.7**, at the link below:

- [Cisco Catalyst Center Assurance User Guide, Release 2.3.7, Chapter: Monitor Power over Ethernet](#)

Cisco Catalyst Center PoE Assurance can generate reports on PoE usage. These reports can be used to track PoE usage over time and identify potential problems. **Reports** on the network devices are available under the Reports section from the main menu.

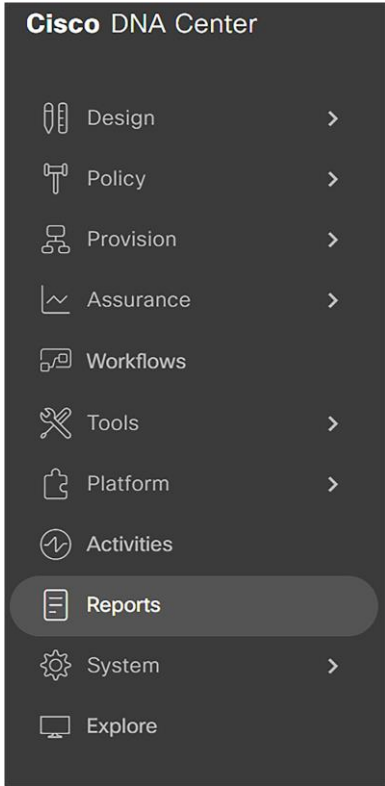


Figure 25.
Cisco Catalyst Center main menu

From the **Reports** page, click **Report Templates** to see the available reports. In the **Network Devices** section, there will be a PoE report available.

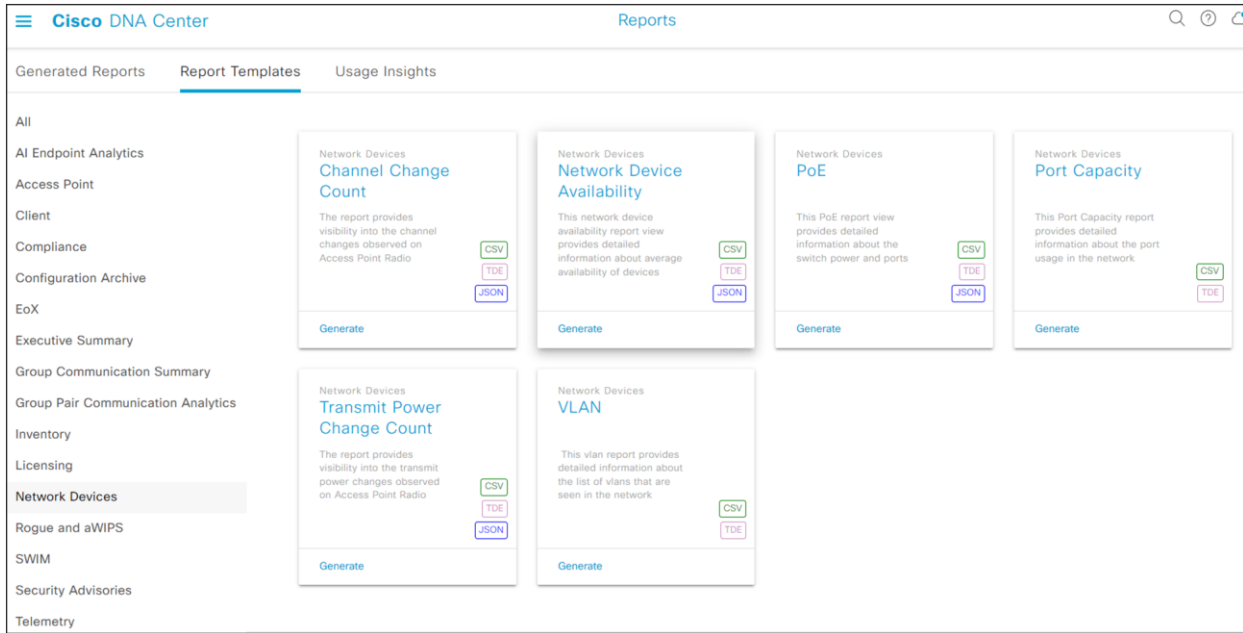


Figure 26.
Cisco Catalyst Center report templates menu

Follow through the prompts to see the option to select the scope of the reports.

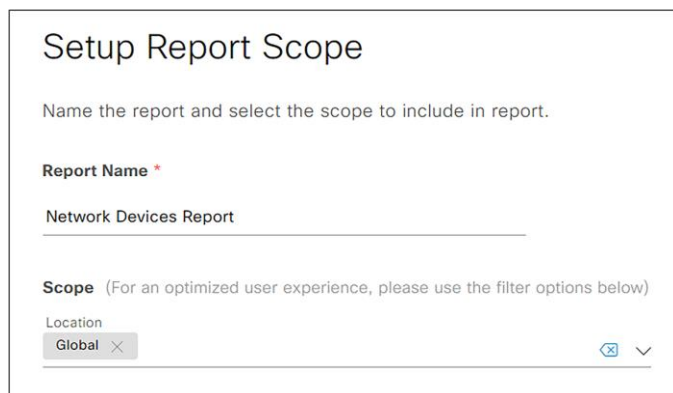


Figure 27.

Cisco Catalyst Center setup report scope form

The report generated will display the PoE-capable devices, power budget, power used, and power remaining for the network devices on the network. From this report, the network devices as well as the PoE end devices can be monitored for their functionality.

Configuring Molex CoreSync Manager services

Installation of Molex CoreSync Manager

Refer to the **Molex CoreSync Manager Installation Guide** for setting up and installing the CoreSync Manager in the data center.

Commissioning light fixtures using Molex Design Tool

Refer to the **Molex CoreSync Manager User Guide** for the detailed procedure to commission the light fixtures in the network. The following high-level steps summarize the commissioning procedure.

1. Launch the Design Tool and enter the project details.
2. Add the **Fixture Start Address** and **Sensor Start Address** details.
3. From the **Fixture** tab, double-click the map to add a light fixture.
4. Edit the **IP Address** in the right window, if required, and then choose **CoAP** from the drop-down menu.
5. On the **Sensor** tab, double-click the map to add a sensor.
6. From the right panel, choose the type of sensor you want to add.
7. Verify the **IP Address** and choose the protocol as **CoAP**.
8. From the **Zone** tab, create a zone by dragging the mouse to create a rectangular area covering the fixture and sensors.
9. Click the desired zone on the right to make the rectangular selection into your desired zone type.
10. Navigate to **File > Upload Project**.
11. Once the dialog window says **Project Upload Successful**, click **OK**.

This completes the addition of light fixtures and sensors to the Design Tool project.

Lighting control and maintenance

This section covers lighting control and management use cases using Molex CoreSync Manager, Facility Manager, and the wireless wall switch.

The steps described provide a high-level summary describing how to implement control and management of light fixture zones during commissioning. Refer to the latest documentation provided by Molex for information on provisioning and managing light fixtures.

Light fixture control using Molex Facility Manager

Connecting to the controller using Facility Manager

The light fixtures can be switched on or off or dimmed up or down using the Molex Facility Manager.

Refer to the **Molex CoreSync Manager User Guide** for the procedure to connect to the CoreSync controller.

Controlling on/off/dimming using the wireless wall switch

Alternatively, the light fixtures can be controlled via the wireless wall switch. The wall switch controls all the light fixtures of the zone to which it is added. Perform the following steps to control the light fixtures using the wall switch:

1. Pair the wireless wall switch with the EnOcean Gateway using the MoDiag tool. Refer to the **Molex CoreSync Commissioning Guide** for detailed steps to pair the wireless switch and gateway.
2. In the **Design Tool**, add the sensor with its correct IP address and choose the **ON/OFF** sensor in the sensor role from the right panel.
3. Enter the 6-digit Hex ID in the **Device ID** section.
4. Change the polling rate to something other than 0.
5. Configure it in the zone you wish to control.
6. Upload the project.
7. Press the button on the wireless wall switch to switch the lights on and off. Verify that the light fixtures turn on and off accordingly.

Configuring occupancy sensing

Refer to the **Molex CoreSync Manager User Guide** and **Molex CoreSync Commissioning Guide** for the steps to configure the Occupancy Sensing feature.

Configuring Ambient Lighting Sensing

Ambient Lighting Sensing is used to adjust the intensity of the light fixture according to the surrounding light from other light sources as well as from daylight. This helps save power.

Refer to the **Molex CoreSync Manager User Guide** and **Molex CoreSync Commissioning Guide** for the steps to configure the Ambient Lighting Sensing feature.

Selecting light scenes using Facility Manager

The light scenes can be changed in order to bring a unique experience for each collaboration. Once the project has been created and uploaded using the CoreSync Design Tool, the required light scene can be selected using the Facility Manager.

For the light scene selection procedure, refer to the **Molex CoreSync Manager User Guide**.

Ongoing maintenance for light fixtures

Replacing light fixtures

When a light fixture malfunctions, it must be replaced. Since the MAC address of the new light fixture is different from the light fixture that needs to be replaced, the DHCP IP address assignment for this newly replaced light fixture will be different from the one for the old light fixture in the same network subnet.

This requires the recommissioning of the light fixture in the Molex CoreSync Manger Design Tool and projects. Follow the commissioning procedure suggested by Molex for replacing the light fixture. The following provides a summary of steps to be performed.

Modify the light fixture in the Design Tool

The new light fixture has to be added to the project, replacing the old light fixture. This can be done in the Design Tool.

1. In the Design Tool, go to the old fixture to be replaced and change its IP address to that of the new fixture.
2. Similarly, change the IP address for the sensors added with this fixture.
3. From **File > Upload Project**, select the target networks and devices.
4. Verify that the new light fixture has successfully replaced the old light fixture by controlling it from the Facility Manager Zone.

Appendix A: Caveats

This appendix covers open issues in the system and workarounds for them, if any.

Table 12. Caveats and workarounds

Open issue	Workaround
The Fast PoE feature does not work with 2-event classification on the PoE switch port configuration.	Remove/disable 2-event classification for the Fast PoE feature from the switch port configuration.
The Fast PoE feature does not work on the Cisco Catalyst 9300 Series stack with power stacking cables connected. Molex light fixtures require 8 to 10 minutes to receive power and illuminate after the switch comes back up from a power restore in a power stack deployment.	No workaround is available for Fast PoE with the Cisco Catalyst 9300 Series Switch power stack. If Fast PoE is required, configure Cisco Catalyst 9300 Series Switches only in the data stack.
The Fast PoE feature with 2-event classification does not work as expected in this Cisco Reference Design release due to known issues.	None available.
Molex light fixtures require recommissioning if they are already commissioned for deployment and the DHCP-assigned IP address changes for the light fixture. This causes a temporary outage of the light fixtures in the building.	None available. A planned maintenance and outage notification is required if light fixture recommissioning is needed.
DHCP IP address to MAC address binding changes due to lease expiration and a change in the light fixture MAC address. If the Molex CoreSync Gateway MAC address for the light fixtures changes in later firmware versions, it is necessary to recommission the light fixture in the Molex project. Light fixture outages are introduced until recommissioning is performed.	None available. Molex should not override or change the MAC address of light fixtures upon firmware upgrades to light fixtures that are already deployed.
The Molex MoDiag application's "Extended Range" accepts a range of only 250 IP addresses at a time to enable multicast discovery control within a VLAN.	Configure a block of only 250 IP addresses in the MoDiag application. If more than 250 light fixtures exist in a VLAN, it is necessary to relaunch MoDiag for an additional block of IP addresses in the same VLAN for multicast discovery control commissioning of the light fixtures.
The PD device classification of "Light" on a Cisco Catalyst 9300 Series Switch is based on a light fixture's MAC address only, as no LLDP Type Length Value (TLV) extension-based classification is available.	The Auto SmartPort feature requires device classification as "Light," through either a MAC address or LLDP TLV extension values. Since a TLV-based device classification is still not available, MAC address-based classification of the PD is the workaround available.
The IP DHCP snooping and IP Source Guard security features described in this document do not work as expected in this Cisco Reference Design release due to known issues.	None available. You may not be required to configure these features in the switches.

Appendix B: References

This appendix, which lists the documentation used in this implementation guide, includes the following major topics:

- [Cisco documentation](#), page 62
- [Molex documentation](#), page 62
- [Third-party documentation](#), page 62

Cisco documentation

- [Low-Voltage PoE Lighting Design Guide](#)
- [Design Zone for Campus Wired and Wireless LAN](#)
- [Cisco Catalyst 9300 Series Switches Data Sheet](#)
- [Software Configuration Guide. Cisco IOS XE 17.3.x \(Catalyst 9500 Series Switches\)](#)
- [Cisco Catalyst 9300 Series Switches Hardware Installation Guide](#)
- [Stacking and High Availability Configuration Guide. Cisco IOS XE 17.9.x \(Catalyst 9300 Switches\)](#)
- [Software Configuration Guide. Cisco IOS XE 17.9.x \(Catalyst 9300 Switches\)](#)
- [Cisco UCS C240 M6 Server Installation and Service Guide](#)
- [Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide. Release 4.3](#)
- [Cisco Catalyst Center Install and Upgrade Guides](#)
- [Cisco Catalyst Center Administrator Guide. Release 2.3.7](#)
- [Cisco Identity Services Engine \(ISE\) Administrator Guide. Release 3.0](#)
- [Cisco Identity Services Engine Installation Guide. Release 3.0](#)
- [Cisco Catalyst Center Getting Started Guides](#)
- [Cisco Catalyst Center User Guide. Release 2.3.7](#)

Molex documentation (refer directly to Molex representative for the following documents)

- CoreSync Installation and Commissioning Overview Application Note
- CoreSync Manager User Guide
- Molex CoreSync Installation Guide

Appendix B: Glossary

Term	Definition
AAA	Authentication, authorization, and accounting
ACE	Access control entry
ACL	Access control list
ARP	Address Resolution Protocol
ALS	Ambient Light Sensor
BPDU	Bridge Protocol Data Unit
CT	Configuration Tool
DAI	Dynamic ARP inspection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOS	Denial of service
IPv4	Internet Protocol Version 4
ISE	Cisco Identity Services Engine
LLDP	Link Layer Discovery Protocol
NTP	Network Time Protocol
OTT	Over the top
OVA	Open Virtualization Appliance
OVF	Open Virtualization Format
PACL	Port access list
POE	Power over Ethernet
RPVST	Rapid per-VLAN spanning tree
SCM	Storm Control Manager
SSH	Secure Shell
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
SVI	Switched virtual interface

Term	Definition
TACACS	Terminal Access Controller Access Control System
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
TLV	Type Length Value
UCS	Cisco Unified Computing System
UPOE+	Cisco Universal Power over Ethernet
UDP	User Datagram Protocol
VM	Virtual machine
VLAN	Virtual local area network

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)