Cisco and Molex Digital Building Solution Implementation Guide

The Cisco® Systems and Molex® end-to-end Digital 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 Digital Building Solution Cisco Reference Design (CRD) consists of a Design Guide, which provides overall guidance on the solution design, and this Implementation Guide.

This document provides implementation details for the Cisco and Molex Digital Building Solution initial installation, migrating the lighting initial setup to a production campus network topology and on-going lighting system management and maintenance.

This *Cisco and Molex Digital Building Solution Implementation Guide* provides the implementation details for the system topologies as discussed in the "System Architecture" section of the *Cisco and Molex Digital Building Solution Design Guide*.

Note: The *Cisco and Molex Digital Building Solution Design Guide*, which is referred to frequently in this document, will be simply referred to as "*Design Guide*" going forward.

The scope of this document is limited to implementation of lighting network for initial installation, migrating 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 Molex Lighting system are covered in the *Molex Coresync Manager User Guide* that is referenced in this document, wherever applicable.

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

- http://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html#~validate

Audience

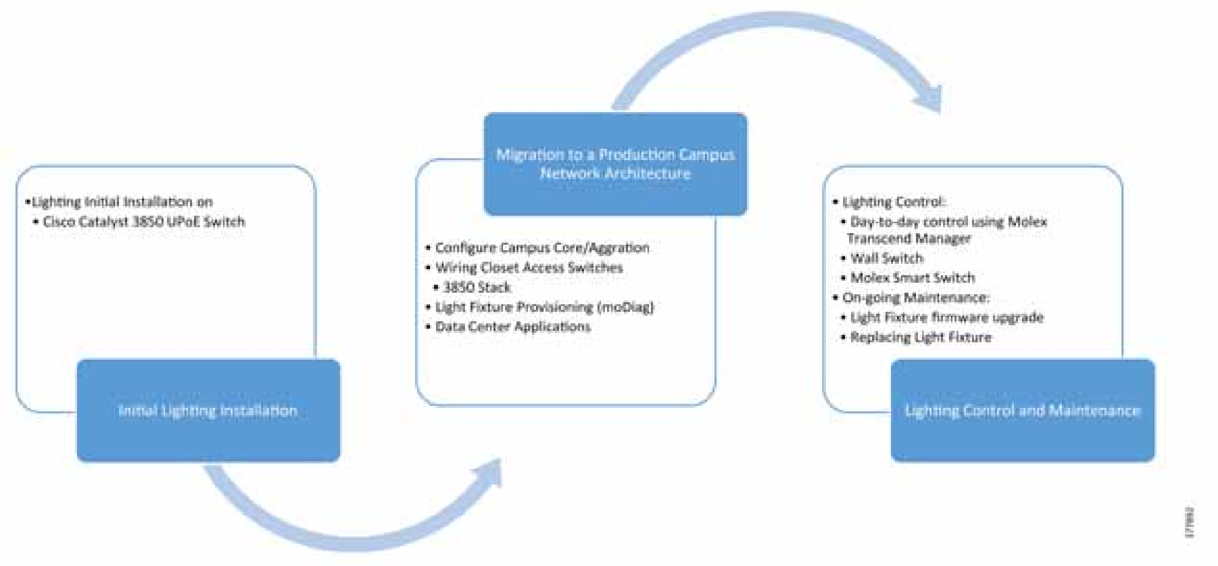
The audience of this guide comprises, but is not limited to, system architects, network/compute design engineers, systems engineers, field consultants, Cisco Advanced Services specialists, and customers who are deploying the Cisco and Molex Digital Building Solution.

Readers should be familiar with IPv4 networking concepts and protocols, Networking Layer 4 through Layer 7 services and Cisco Catalyst Series Switches, Cisco Unified Computing System (UCS), and VMware hypervisors.

Implementation Workflow

This section provides the high-level implementation flow for deploying the Cisco and Molex Digital Building Solution on a campus network topology that is described in the design guide. It is suggested to 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 Digital Building System Implementation Workflow


Migration to a Production Campus Network Architecture
•Lighting Initial Installation on
• Cisco Catalyst 3850 UPoE Switch
• Configure Campus Core/Aggration
• Wiring Closet Access Switches
• 3850 Stack
• Light Fixture Provisioning (moDiag)
• Data Center Applications
• Lighting Control:
• Day-to-day control using Molex Transcend Manager
• Wall Switch
• Molex Smart Switch
• On-going Maintenance:
• Light Fixture firmware upgrade
• Replacing Light Fixture
Initial Lighting Installation
Lighting Control and Maintenance
377992

System Overview

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

- System Topology, page 2
- System Components, page 4
- System Networking, page 5

System Topology

Different network topologies exist in which the Digital Building Solution can be deployed based on the customer's requirements when the installation will be done.

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

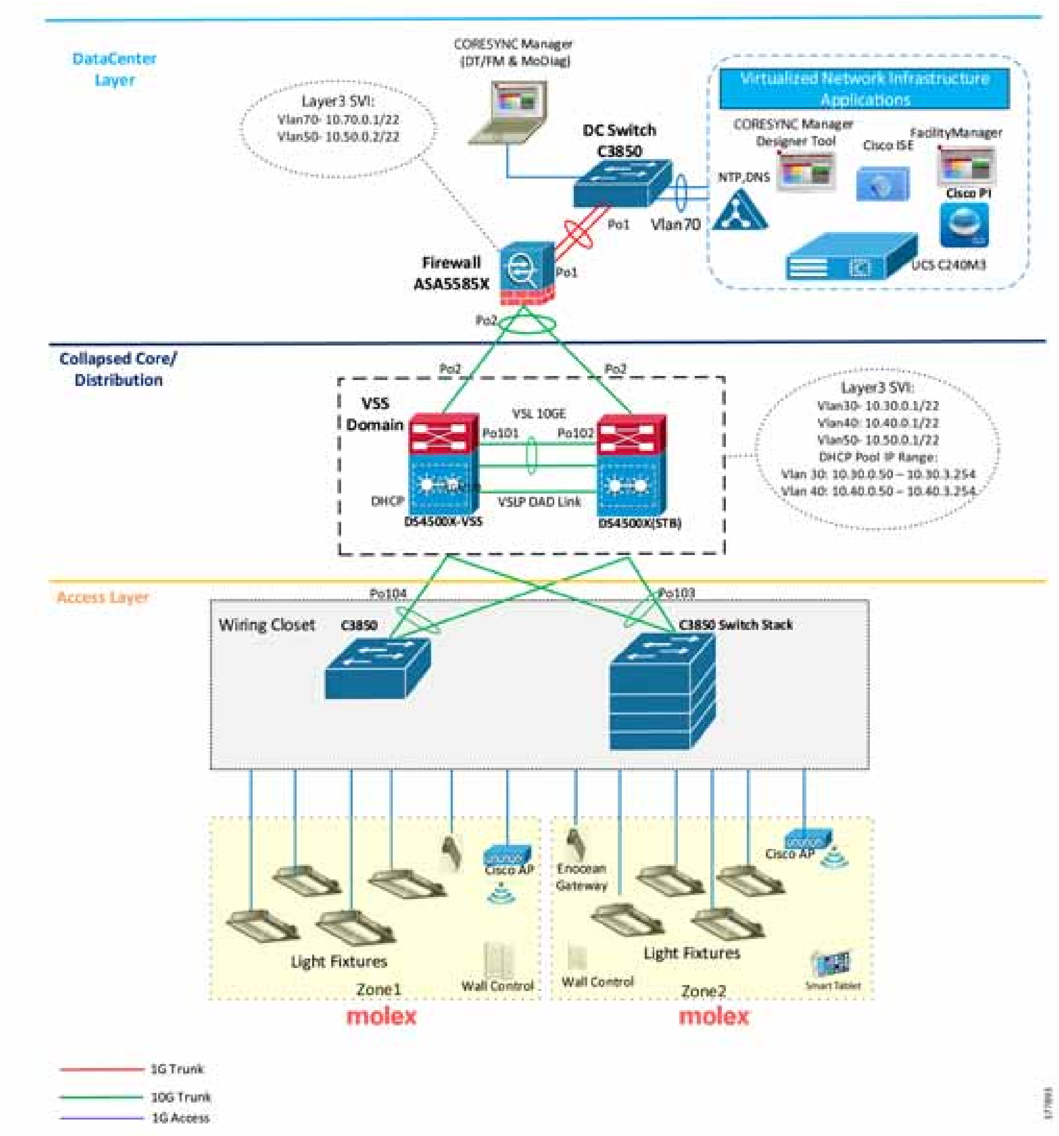
Figure 1 above show the physical network topology for a lighting network integration with a Campus Network, where wiring closet access switches (Cisco Catalyst 3850 standalone and Cisco Catalyst 3850 stack) connect to the campus network aggregation/distribution switch (Cisco Catalyst 4500-X). In this deployment, the aggregation switch aggregates 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.

Figure 2 shows the Cisco Catalyst 3850 switch as an example data center switch for the server farm's network access. However, any data center switch that is recommended or implemented in the campus data center design can be leveraged to configure network access to servers.

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 *Cisco Campus Network 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 Digital Building Solution on a Campus Network Topology with Cisco Catalyst 3850 Switches and Stack in Wiring Closet



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 3850 Switch—Wiring Closet / Access Switch	16.9.2	UPOE switch
Cisco Catalyst 4500-X Switch—Core / Distribution Switch	15.2.5 E1 (3.9.1)	Campus network Layer 3 aggregation switch
Cisco Identity Services Engine (ISE)	2.4.102.162	Terminal Access Controller Access Control System+ (TACACS+) authentication and authorization server for network devices
Cisco ASA 5585 Firewall	9.6.1	Firewall to protect server farm
Cisco Aironet 3702i Wireless Access Point	15.3.3 JD4	Wireless access point

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	1.6.1.8.4	Firmware for lighting (updated firmware version)
Molex Sensor Board Firmware	2.0.1.3.3	Firmware for sensor board
Molex Coresync Smart Tablet:		Tablet for zone control
Molex Tablet Software - ZoneID	1.0.23	Coresync Smart Tablet software
Molex Tablet Software - EUT	1.1.75	Coresync Smart Tablet software
Molex Coresync Manager	1.6.2	Coresync management application
Molex Diagnostic Tool	2.0.16.27	Molex diagnostic tool

Table 3 is the list of third party infrastructure components used in the system.

Table 3 Third Party System Components

Product	Purpose	Version
Virtualization Software for UCS	Hypervisor	VMware ESXi 5.5
Application Platform	Operating System	Microsoft Windows 10 Enterprise Release SP1

System Networking

The network-powered lighting system should deploy on a separate logical network (VLAN). It is suggested to 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 for deploying more than 500 light fixtures. Each VLAN requires the Molex MoDiag application to set the Molex Coresync Manager IP address with which light fixtures can communicate.

This section summarizes the logical network (VLAN) configuration for the Cisco and Molex Digital Building Solution network. In Table 4, which is an example list of VLANs implemented for this solution, the subnet mask “255.255.252.0” 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 Digital Building Solution. VLAN numbering will vary based on your actual deployment.

Initial Installation of Lighting Network

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

- Initial Installation with Cisco Catalyst 3850 UPOE Switch, page 5
- Light Fixture Initial Installation, page 7

During the initial installation, the electrician will install the light fixture on a wiring closet switches (Cisco Catalyst 3850) with the default factory configuration to verify the light fixture's operation.

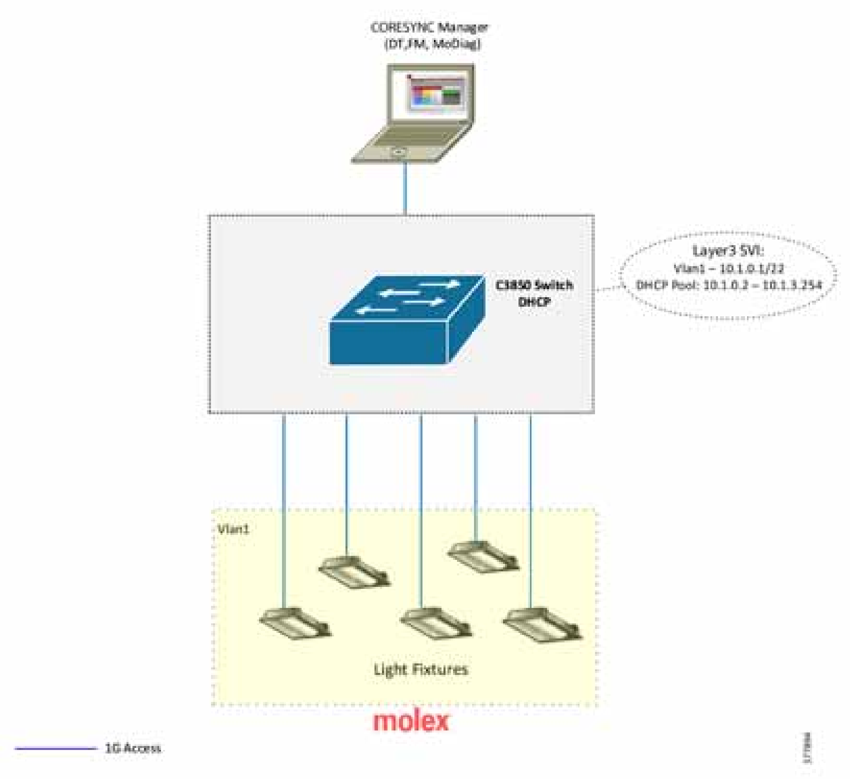
Initial Installation with Cisco Catalyst 3850 UPOE Switch

This section covers the network topology and configuration required on the Cisco Catalyst 3850 switch for the initial installation of light fixtures.

Network Topology

During the initial installation, light fixtures are connected to the wiring closet Cisco Catalyst 3850 UPOE access switch or to the switch stack, as shown in the network topology in Figure 3.

Figure 3 Cisco and Molex Digital Building Solution Initial Setup on Wiring Closet Cisco Catalyst 3850 Switch



Configuring Cisco Catalyst 3850 UPOE Switch for Initial Installation

Molex Light Fixtures Installation

A technician 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 3850 UPOE switch port, the light fixtures turn on with low brightness; this verifies the light fixtures' hardware operation.

Initial Network Setup

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

Prerequisites for Initial Installation

Perform the following prerequisite step for initial lighting network setup:

The Cisco Catalyst 3850 switch supports Perpetual and Fast PoE features (described in Lighting Migration to Campus Network Architecture, page 8) on the 16.9.1 switch IOS software release. Therefore, it is suggested to upgrade the switch IOS image to version 16.9.1 before beginning lighting network installation.

1. Enable Link Layer Discovery Protocol (LLDP) on the switch global configuration as shown below. LLDP is required to be enabled on the switch for the Molex light fixtures' power negotiation and operation.

```
3850-Switch(config)#lldp run
```

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

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

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

```
interface vlan 1
 ip address 10.1.0.1 255.255.252.0
!
```

Light Fixture Initial Installation

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

Configuring 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 application. 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 3850 access switch on 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 3850/Cisco Catalyst 4506-E

Pool Network	Excluded IP Range	Purpose
10.1.0.0/23	10.1.0.1	DHCP pool for Molex light fixtures in default VLAN 1

Configure the DHCP server on the Cisco Catalyst 3850 access switch. For example:

```
3850-Switch (config)# ip dhcp pool Molex
     network 10.1.0.0 255.255.255.0
     default-router 10.1.0.1

3850-Switch (config)# ip dhcp excluded-address 10.1.0.1
!
```

Configuring MoDiag for Light Fixture Provisioning

Perform the steps described in this section for installing and configuring the Molex Coresync Manager.

Installing Molex MoDiag

Refer to the Installation Procedure in the *Molex Coresync Manager Installation Guide* for installing Molex MoDiag.

Provisioning Light Fixtures

Refer to the *Molex Coresync Commissioning Guide* and *Molex Coresync Manager User Guide* for detailed instructions on initial provisioning of the light fixtures.

Verifying and Upgrading Light fixture Firmware

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

Refer to the *Molex Coresync Commissioning Guide* for upgrading firmware on Molex endpoints. Also, verify the firmware version after the successful upgrade by following the instructions provided in the *MoDiag User Guide*.

Lighting Migration to Campus Network Architecture

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

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

- Campus Network Core/Aggregation Switch Cisco Catalyst 4500-X, page 9
- Wiring Closet Access Switch (Cisco Catalyst 3850), page 15
- Wiring Closet Access Switch Stack (Cisco Catalyst 3850 Stack), page 22
- Provisioning Light Fixtures, page 29
- Implementing Data Center Applications for Lighting, page 29

Network Topology

During migration, the access switches in the wiring closet (Cisco Catalyst 3850 standalone or stack) connect to a production campus network core/aggregation switch with separate logical networks for Molex light fixtures, as shown in Figure 4 and Figure 5.

Figure 4 Cisco and Molex DBS on Campus Network Architecture with Cisco Catalyst 3850 Access Switch

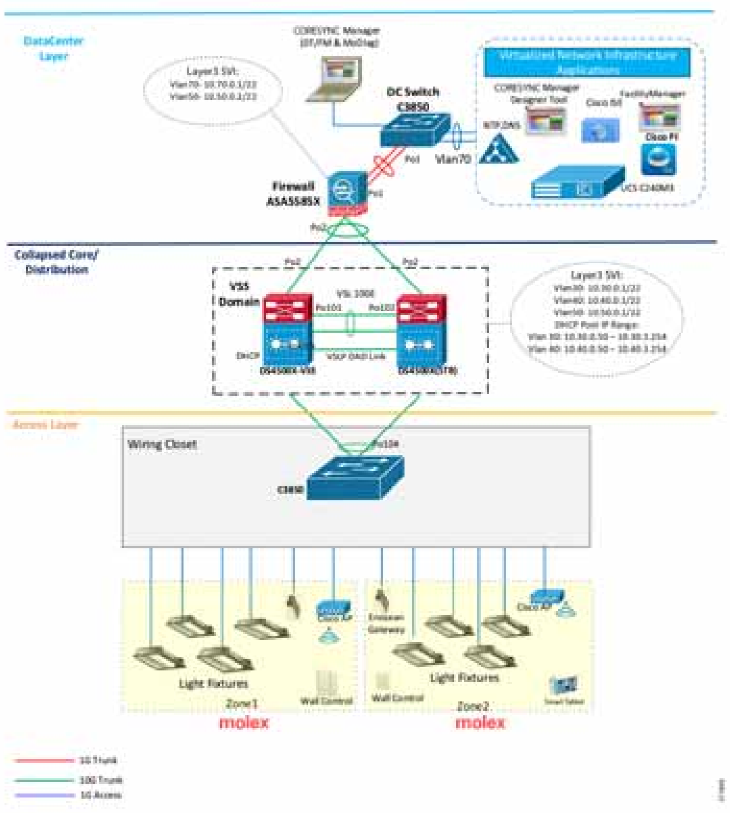
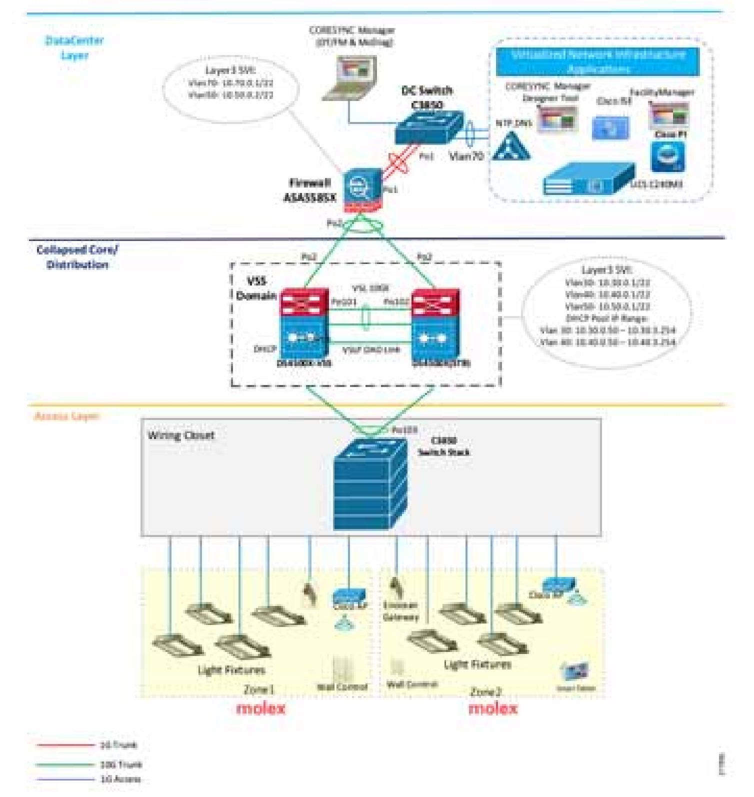


Figure 5 Cisco and Molex DBS Large Scale Deployment on Campus Network Architecture with Cisco Catalyst 3850 Switch Stack



Campus Network Core/Aggregation Switch Cisco Catalyst 4500-X

The lighting network UPOE access switches (Cisco Catalyst 3850 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 4500-X switches deployed in a pair, which provides campus network core, aggregation services, and Layer 3 routing functionalities for the lighting endpoints in the access layer. The implementation of the Cisco Catalyst 4500-X 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 Virtual Switching System

The system topology in Figure 4 above shows one of the implementations of the campus network aggregation as a collapsed core/distribution model for this Cisco and Molex Digital Building Solution. The aggregation Cisco Catalyst 4500-X switches implement Virtual Switching System (VSS) to provide network redundancy at the aggregation layer.

A VSS combines a pair of Cisco Catalyst 4500-X series switches into a single network element. The VSS manages the redundant links, which externally act as a single port channel. The VSS 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 VSS may not be required to be implemented at the network aggregation level. In this case, VSS configuration steps are not required to be performed.

For the detailed implementation of VSS on the Cisco Catalyst 4500-X switch, refer to the *Catalyst 4500 Series Switch Software Configuration Guide, IOS XE 3.9.xE and IOS 15.2(5)Ex* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-9-0E/15-25E/configuration/guide/xe-390-configuration/vss.html

Configuring Network Layer 2 and Layer 3

This section defines the implementation of VLANs and Layer 3 logical interfaces on the Cisco Catalyst 4500-X switch.

1. Configure VLANs, which must be created along with ports assignment on the Cisco Catalyst 4500-X switch:

```
CL-4500X(config)#vlan 30,40,50
```

2. Create 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 4500-X switch:

```
interface Vlan30
 ip address 10.30.0.1 255.255.252.0
 !
interface Vlan40
 ip address 10.40.0.1 255.255.252.0
!
interface Vlan50
 ip address 10.50.0.1 255.255.252.0
!
```

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

3. Create port channel interfaces on the Cisco Catalyst 4500-X to the wiring closet switches (Cisco Catalyst 3850 standalone and stack), and ASA firewall in the network as shown below:

```
interface Port-channel2
 description Etherchannel Link to ASA5585 Firewall
 switchport
 switchport mode trunk
end
!
interface Port-channel103
 description Etherchannel Link to 3850 Switch Stack
 switchport
 switchport mode trunk
switchport trunk allowed vlan 30,40,50
end
!
interface Port-channel104
 description Etherchannel Link to 3850 Switch
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50
end
```

4. Enable EtherChannel on the appropriate physical switch ports connected to the Cisco Catalyst 3850 standalone, stack, and ASA. The following configuration shows the port channel assignment to switch physical ports:

Physical links to the Cisco Catalyst 3850 switch stack in 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 3850 switch in wiring closet:

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

Physical links to the ASA 5585 Firewall switch:

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

5. The following commands add static default routes to the ASA:

```
ip route 10.70.0.0 255.255.255.0 10.50.0.2
!
```

6. Enable rapid per-vlan spanning tree:

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

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 4500-X 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 3850) that was performed on the initial lighting setup.

Table 6 shows an example DHCP pool range for Molex endpoints.

Table 6 IPv4 DHCP Address Pool on Cisco Catalyst 4500-X

Pool Network	Excluded IP Range	Purpose
10.30.0.0/22	10.30.0.1	DHCP pool for Molex light fixtures in VLAN 30
10.40.0.0/22	10.40.0.1	DHCP pool for Molex light fixtures in VLAN 40

Perform the following step to configure the DHCP server pool on the Cisco Catalyst 4500-X aggregation switch for lighting network:

Configure DHCP pools for light fixture on the Cisco Catalyst 4500-X:

```
ip dhcp pool MOLEX-VLAN30
 network 10.30.0.0 255.255.252.0
 default-router 10.30.0.1
!
!
```

```
ip dhcp pool MOLEX-VLAN40
 network 10.40.0.0 255.255.252.0
 default-router 10.40.0.1
!
ip dhcp excluded-address 10.40.0.1
ip dhcp excluded-address 10.30.0.1
!
```

Configuring Security Features

Security features in the lighting network are important to protect light fixtures from network attacks like IP address 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 4500-X. For a detailed description of the Layer 2 security features, refer to the *Cisco Catalyst 4500-X Configuration Guide* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-9-0E/15-25E/configuration/guide/xe-390-configuration/vss.html

IP DHCP Snooping (Optional)

IP DHCP snooping is needed on the Cisco Catalyst 4500-X switch only if a separate centralized DHCP server exists that is connected to the Cisco Catalyst 4500-X. In that case, the Cisco Catalyst 4500-X 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 DHCP snooping 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 4500-X 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 CRD release.

1. Configure the required port as 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 learnt on the Cisco Catalyst 4500-X 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 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 CRD release.

Perform the following step on the Cisco Catalyst 4500-X switch to configure IP Source Guard:

Configure the IP Source Guard on the downlink port channel interfaces to the Cisco Catalyst 3850 stack and standalone switches that have trusted IP-to-MAC bindings:

```
interface Port-channel103
 description Etherchannel Link to 3850 Switch Stack
 ip verify source
end
!
interface Port-channel104
 description Etherchannel Link to 3850 Switch Standalone
 ip verify source
end
```

ARP Inspection (Optional)

Since it is highly unlikely that attackers will connect to the free ports of the Cisco Catalyst 4500-X, configuring Dynamic ARP Inspection (DAI) on the Cisco Catalyst 4500-X is optional.

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.

Lights or any other devices connected on untrusted ports of the Cisco Catalyst 4500-X will be automatically 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 4500-X switch to configure ARP Inspection:

1. Configure the required port channels as an ARP Inspection-trusted port, as shown in this example configuration:

```
interface Port-channel103
 description Etherchannel Link to 3850 Switch Stack
 ip arp inspection trust
end
!
interface Port-channel104
 description Etherchannel Link to 3850 Switch Standalone
 ip arp inspection trust
end
```

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. Therefore, keeping Storm Control limits the propagation of such packets to the light fixtures and maintains proper access to the light fixtures for the SCM.

Perform the following configuration on the Cisco Catalyst 4500-X switch to configure Storm Control:

Configure the Storm Control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentage of line rates:

```
interface Port-channel103
 description Etherchannel Link to 3850 Switch Stack
 storm-control broadcast level pps 4000 3500
 storm-control multicast level pps 4000 3500
 storm-control unicast level pps 4000 3500
end
!
interface Port-channel104
 description Etherchannel Link to 3850 Switch Standalone
 storm-control broadcast level pps 4000 3500
 storm-control multicast level pps 4000 3500
 storm-control unicast level pps 4000 3500
end
```

Disabling Telnet

Since Telnet is not secure, it should be disabled for accessing the device. The following commands disable Telnet and enable only Secure Shell (SSH) access to the Cisco Catalyst 4500-X switch:

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

Configuring Network Management (SNMP)

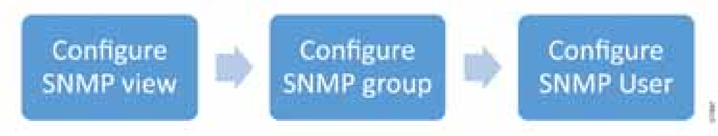
Simple Network Management Protocol (SNMP) is used in the lighting network to manage and monitor the switches in the lighting network.

SNMP traps are configured to send light fixtures ports up/down status alerts to a network management server (Cisco Prime Infrastructure 3.0) that helps monitor light fixture's port status.

Configuring Switch Network Management

The SNMPv3 protocol configuration is used on the Cisco Catalyst 4500-X switch for network management. Perform the following steps to configure SNMP v3:

Figure 6 Network Management SNMP Configuration Flow


Configure SNMP view

Configure SNMP group

Configure SNMP User

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 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 CLI:

```
CL-DS4500X-VSS#show snmp user

CL-DS4500X-VSS#show snmp group

CL-DS4500X-VSS#show snmp view
```

Wiring Closet Access Switch (Cisco Catalyst 3850)

This section covers wiring closet access switch Cisco Catalyst 3850 stack, Layer 2, Layer 3 networking, security configuration, and network management configurations.

Removing the Initial Installation Configuration

When migrating the initial lighting setup on the Cisco Catalyst 3850 switch on the wiring closet to a campus network, follow the steps below to configure the Cisco Catalyst 3850 switch:

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

```
3850-Switch (config)# no ip dhcp pool Molex
3850-Switch (config)# no ip dhcp excluded-address 10.1.0.1
```

2. Remove the IP address for VLAN 1:

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

Configuring Network Layer 2 and Layer 3

This section defines the implementation of VLANs and logical SVI for management traffic on the Cisco Catalyst 3850 switch. The LLDP and 2-event must have been already enabled in the initial installation.

1. Configure VLANs, which must be created along with ports assignment on the Cisco Catalyst 3850 switch stack. The following is an example VLAN configuration:

```
3850-switch (config)#vlan 30,40,50
```

2. Configure switch ports connecting to light fixtures/wireless gateway on appropriate lighting VLAN in access mode:

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

3. Provide **shutdown** and **no shutdown** CLI commands on the switch ports where light fixtures and Coresync gateways are connected. This enables lights fixtures to initiate DHCP requests to obtain IP addresses on the newly configured VLANs.

```
(config)#interface GigabitEthernet 1/1
(config-if)# shutdown
(config-if)# no shutdown
(config-if)# end
!
```

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

4. Create Layer 3 SVI for the management VLAN and default gateway as required. The following is an example configuration of management VLAN SVI on the Cisco Catalyst 3850 switch stack:

```
interface Vlan50
 ip address 10.50.0.4 255.255.252.0
 !
ip default-gateway 10.50.0.1
```

5. Create port channel uplink interfaces on Cisco the Catalyst 3850 to campus network aggregation switch (Cisco Catalyst 4500-X), as shown in Figure 2.

```
interface Port-channel104
 description Etherchannel Link to 4500X Switch
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50
end
```

6. Enable PortChannel on the appropriate physical switch ports connected to the Cisco Catalyst 4500-X switch. The following configuration shows the port channel assignment to switch physical ports:

Physical links to Cisco Catalyst 4500-X active and standby VSS switches:

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

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

7. Enable per-vlan spanning tree.

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

Configuring MAB and filter-spec (OPTIONAL)

Note: MAB and MAB Policy configuration is required only if we implement MUD visibility using ISE in this solution.

The Manufacturer Usage Description (MUD) URL is used to address the threats to network device in a light network to which the light communicates. The MUD-URL is sent from the light's firmware that is used to authenticate the lights. This section describes the commands that should be configured for the MUD-URL to be displayed on the switch.

The following configurations should be added on both the Cisco Catalyst 3850 switch stack and the standalone light fixture access ports. These configurations are mandatory for the visibility of the MUD-URL on the switch and on ISE.

Here access sessions are configured in order to give 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
 lldp
access-session accounting attributes filter-spec include list listA
```

MAB Policy

The MAB policy is defined as follows. Here the control class specifies the MAB authentication as default and is used here 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 the light fixtures receive power via the UPOE ports of the Cisco Catalyst 3850 switch. The switch allocates powers based on the type of connected light fixtures. Perpetual POE feature can help sustain the POE under specific circumstances where the switch may undergo a power failure or a soft reload.

The following configurations are not mandatory during migration. Perpetual POE and Fast POE features only have to be configured on those Cisco Catalyst 3850 switch access ports on which certain light fixtures need to illuminate even during a reload or if you want to them to turn on quickly after power restoration on the switch.

Perpetual POE

Perpetual POE is a POE enhancement feature on the Cisco Catalyst 3850 switch that helps enable light fixtures connected ports to continue to receive power during a soft reload of the switch.

Perform the following configuration on the Cisco Catalyst 3850 stack switch for light fixture access ports to configure Perpetual POE:

Configure the required edge port with the *poe-ha* command, which enables Perpetual POE on that port:

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

Fast POE

The Fast POE feature on Cisco Catalyst 3850 switch ports helps enable Molex light fixtures to illuminate with low brightness within 10 seconds (~15W of power given via cable two pair by switch hardware) after restoring the power on a switch/stack of switches when a power interruption caused the switch to go down. Once the switch is restored to normal state, the lights are allocated the requested power.

Perform the following configuration on the Cisco Catalyst 3850 stack switch for light fixture access ports to configure Perpetual POE:

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
```

Note: Perpetual poe-ha cli is needed to enable Fast POE in this release. Once the Fast POE issue is resolved, this can be updated.

Configuring Security Features

The Cisco Catalyst 3850 switch stack integrated security features can provide threat defense capabilities for mitigating man-in-the-middle attacks and protect 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 security configuration, refer to the *Consolidated Platform Configuration Guide, Cisco IOS 16.9.x and Later (Catalyst 3850 Switches)* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/37e/consolidated_guide/b_37e_consolidated_3850_cg.html

IP DHCP Snooping

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure IP DHCP snooping:

1. Configure the required port channel connected to the Cisco Catalyst 4500-X as 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
!
```

Note: The DHCP snooping table does not match the IP Source Guard table and, therefore, light fixtures don't receive the IP address properly from the DHCP server. This issue has been resolved in the latest CCO image release.

IP Source Guard

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure IP Source Guard:

1. Configure the IP Source Guard on the port channels which 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
!
```

Note: The DHCP snooping table does not match the IP Source Guard table and the light fixtures don't receive the IP address from DHCP server when IP Source Guard is enabled. Therefore, the IP Source Guard feature does not work as expected in this CRD release.

ARP Inspection

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure ARP Inspection:

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

```
interface Port-channel104
 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 3850 stack switch to configure ARP Rate Limiting:

Configure ARP Rate Limiting according to the maximum allowable packet rate on 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 learnt 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 one 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 address of light fixtures that are learnt on any secured port will be the only MAC address permitted on that port. If any other device is connected on that port, then it will throw a security violation alert. So if one light's MAC address is already learnt 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 learnt. If The Auto Smartport feature is enabled, then this issue will automatically be taken care of by Auto Smartport.

Perform the following step on the Cisco Catalyst 3850 stack switch to configure port security:

Configure the port security on the light fixture access ports in sticky mode with a maximum allowable number of MAC address 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 3850 stack switch to configure Storm Control:

Configure Storm Control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentage 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 Bridge Protocol Data Unit (BPDU) Guard prevents loops by moving a non-trunking port into an *errdisable* 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 BPDU Guard.

Perform the following step on the Cisco Catalyst 3850 stack switch 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 the Coresync Manager uses to communicate with light fixtures.

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure PACL:

1. Configure IP access list to permit the incoming traffic only for Layer 4 port numbers specific to communication between 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 3850 switch:

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

Configuring Auto Smartport (Recommended)

Rather than manually enabling all the commands separately, the access port configurations shown in the previous sections can be configured much more simply with the Auto Smartport feature. This also saves a great deal of time when several lights are connected on the switch.

Auto Smartport enables configuring the access ports connected to end hosts such as light fixtures. By configuring an Auto Smartport macro for a particular type of host device, the moment a port comes up with that type of host device, a macro that instantly puts a set of preconfigured commands on that access port is triggered. 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 config 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, then 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 detailed functionality of the Auto Smartport feature, refer to the *Auto Smartports Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*, which can be found at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3-2_0_se/autosmartports/configuration_guide/iosaspcg/configure.html

1. The macro needed for the light port config can be configured as 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
  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 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
    exit
   fi
  }
```

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

```
macro auto global processing
```

Configuring Network Management (SNMP)

Simple Network Management Protocol (SNMP) is used for collecting information from network devices in order to manage the network.

Refer to Configuring Switch Network Management, page 14 for configuring network management on Cisco Catalyst 3850 standalone.

Wiring Closet Access Switch Stack (Cisco Catalyst 3850 Stack)

This section covers wiring closet access switch Cisco Catalyst 3850 stack, Layer 2, Layer 3 networking, security configuration, and network management configurations.

Cisco Catalyst 3850 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*, *stand-by*, and *member*. However, all switches in the stack are operational. A switch stack always assigns one switch in active role and one in 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 stack-wide management.

In this system implementation, a stack of four Cisco Catalyst 3850 UPOE (24 UPOE ports per switch) switches are configured in the network topology according to the system requirement. Since each of those switches have 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 re-elected as the active switch if a re-election occurs.

- To install a Cisco Catalyst Switch Data Stack and Stack Manager, refer to the *Catalyst 3850 Switch Hardware Installation Guide* at the following URL:
  - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-9/configuration_guide/stck_mgr_ha/b_169_stck_mgr_ha_3850.html

- To configure a switch stack, refer to the *Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* at the following URL:
  - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-9/configuration_guide/stck_mgr_ha/b_169_stck_mgr_ha_3850/managing_switch_stacks.html

When migrating lighting initial setup on the Cisco Catalyst 3850 switch on the wiring closet, perform the following steps to configure the Cisco Catalyst 3850 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:

```
sh boot
---------------------------
Switch 3
---------------------------
Current Boot Variables:
BOOT variable = flash:cat3k_caa-universalk9.SPA.16.09.02.bin;
Boot Variables on next reload:
BOOT variable = flash:cat3k_caa-universalk9.SPA.16.09.02.bin;
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: cat3k_caa-universalk9.SPA.16.09.02.bin
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 ws-c3850-24u
switch 2 provision ws-c3850-24u
switch 3 provision ws-c3850-24u
switch 4 provision ws-c3850-24u
```

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 switch can be configured in the **Enable** mode as shown below:

```
switch 1 priority 15
```

Network Layer 2 and Layer 3 Configuration

This section defines the implementation of VLANs and logical SVI for management traffic on the Cisco Catalyst 3850 switch stack.

1. Enable LLDP on the switch stack as follows:

```
3850-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 ports assignment on the Cisco Catalyst 3850 switch stack. The following is an example VLAN configuration:

```
3850-switch (config)#vlan 30,40,50
```

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

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

5. Create Layer 3 SVI for the VLANs and default gateway as required. The following configuration is an example configuration of management VLAN SVI on the Cisco Catalyst 3850 switch stack:

```
interface Vlan50
 ip address 10.50.0.4 255.255.252.0
 !
ip default-gateway 10.50.0.1
```

6. Create port channel uplink interfaces on the Cisco Catalyst 3850 stack to the campus network aggregation switch (Cisco Catalyst 4500-X), as shown in Figure 2.

```
interface Port-channel103
 description Etherchannel Link to 4500X Switch
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 30,40,50
end
```

7. Enable port channel on the appropriate physical switch ports connected to the Cisco Catalyst 4500-X switch. The following configuration shows the port channel assignment to switch physical ports:

```
Physical links to Cisco Catalyst 4500-X active and standby VSS switches:
interface TenGigabitEthernet3/1/3
 channel-group 103 mode active

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

8. Enable the per-vlan spanning tree.

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

POE Feature Configuration

All light fixtures receive power via the UPOE ports of the Cisco Catalyst 3850 switch. Based on the type of light fixtures connected to the switch, the switch allocates powers to them. The Perpetual POE feature can help sustain the POE under circumstances where the switch undergoes a power failure or a soft reload.

The following configurations are not mandatory during initial installation. They only have to be configured on those access ports of Cisco Catalyst 3850 switch on which certain light fixtures need to illuminate even during a reload or you want to them to turn on quickly after power restoration on the switch.

Perpetual POE

Perpetual POE is a POE enhancement feature on Cisco Catalyst 3850 switch, which helps enable light fixtures connected on certain ports to continue to receive power during a soft reload of the switch. Perform the following configuration on the Cisco Catalyst 3850 stack switch for light fixture access ports to configure Perpetual POE:

Configure the required edge port with the *poe-ha* command which enables perpetual POE on that port:

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

Fast POE

The Fast POE feature on Cisco Catalyst 3850 switch ports helps enable Molex light fixtures to illuminate with low brightness within 10 seconds (~15W of power given via cable two pair by switch hardware) after restoring the power on switch/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
```

Note: Perpetual poe-cli is needed to configure Fast POE in this release. Once the Fast POE issue is resolved, this will be updated. The light fixtures are initially at low brightness within 20 seconds after power restore but then turn to full brightness after the UPOE switch is fully up and operational (approximately 6-8 minutes).

Configuring Security Features

The Cisco Catalyst 3850 switch stack integrated security features can provide threat defense capabilities for mitigating man-in-the-middle attacks and protect 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 security configurations, refer to the *Consolidated Platform Configuration Guide, Cisco IOS XE 3.7E and Later (Catalyst 3850 Switches)* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/37e/consolidated_guide/b_37e_consolidated_3850_cg.html

IP DHCP Snooping

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure IP DHCP snooping:

1. Configure the required port as 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 3850 stack switch to configure IP Source Guard:

Configure the IP source guard on the ports which have trusted IP to MAC bindings:

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

On light fixture access ports:

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

ARP Inspection

Perform the following steps on the Cisco Catalyst 3850 stack switch 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 3850 stack switch to configure ARP Rate Limiting:

Configure ARP Rate Limiting according to the maximum allowable packet rate on 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 address of light fixtures that are learnt on any secured port will be the only MAC address 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 3850 stack switch to configure Port Security:

Configure the Port Security on light fixture access ports in sticky mode with the maxi-mum 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 3850 stack switch to configure Storm Control:

Configure the Storm Control for broadcast or unicast traffic according to the maximum and minimum allowable threshold percentage 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 BPDU Guard prevents loops by moving a non-trunking port into an *errdisable* 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 BPDU check for spanning tree and, therefore, those ports can be configured for PortFast BPDU Guard.

Perform the following step on the Cisco Catalyst 3850 stack switch to configure PortFast and BPDU Guard:

Enable Portfast on the light fixture access ports as 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, filters specifically the port numbers that MA uses to communicate with lights.

Perform the following steps on the Cisco Catalyst 3850 stack switch to configure PACL:

1. Configure 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 Secure Shell (SSH) access to the Cisco Catalyst 3850 switch.

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

Configuring Auto Smartport (Optional)

Auto Smartport enables configuring the access ports connected to end hosts such as light fixtures. By configuring an Auto Smartport macro for a particular type of host device, the moment a port comes up with that type of host device, a macro that instantly puts a set of pre-configured commands on that access port is triggered. 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 config 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 config can be configured as 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
  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
  exit
 fi
 if [[ $LINKUP == NO ]]
  then  conf t
  interface $INTERFACE
  no macro description
  no switchport access vlan 30
  no power inline port 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
  exit fi
}
```

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

```
macro auto global processing
```

Configuring Network Management (SNMP)

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

Refer to Configuring Switch Network Management, page 14 for configuring network management on the Cisco Catalyst 3850 stack.

Provisioning Light Fixtures

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

During migration phase, the light fixtures are assigned IP addresses from the DHCP pool configured on the Cisco Catalyst 4500-X aggregation switch in the light fixtures' VLANs. The MoDiag application is required to set the Coresync Manager IP address for light fixtures communication with Coresync Manager. Refer to the *Molex MoDiag User Guide* for detailed steps to setting up the IP address.

A new Coresync Manager Design tool project is required to be created based on the new IP addresses of light fixtures which 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 data center application/services in a campus network required for Cisco and Molex Digital Building Solution deployment, as shown in Figure 2. It includes the following major topics:

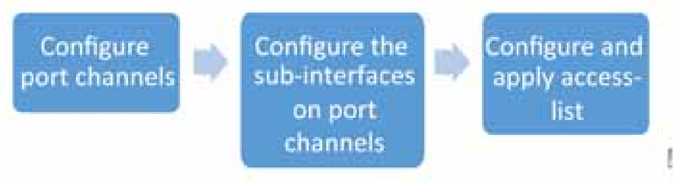
- Configuring Firewall (Cisco ASA 5585-X), page 29
- Configuring Unified Computing System, page 31
- Configuring Network Device Authentication (ISE), page 32
- Configuring Network Management (Cisco Prime Infrastructure), page 41
- Configuring Molex Coresync Manager Services, page 42

Configuring Firewall (Cisco ASA 5585-X)

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

The ASA is configured to operate in routed mode. Several tasks are required to complete ASA configuration. The workflow is shown in Figure 7.

Figure 7 Firewall Configuration Flow Diagram


Configure port channels
Configure the sub-interfaces on port channels
Configure and apply access-list

Configuring Port Channel to Network

Configure the port channel on the ASA towards the data center and towards the campus network aggregation switch (Cisco Catalyst 4500-X), as per the topology in Figure 2. The port channels can be created by performing the following steps:

1. ASA is configured with a port channel having two member links to 4500. The port channel includes the two Ten Gig interfaces available on the ASA 5585-X. No name or security-level is assigned to the port channel.

```
interface Port-channel2
description ##4500X##
```

```
!
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-channel2.50
 vlan 50
```

3. ASA is configured with a port channel having two member links to the Cisco Catalyst 3850 data center switch. The port channel includes the two Gig interfaces available on the ASA 5585X. No name or security-level is assigned.to the port channel.

```
interface Port-channel1
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 ASA Interfaces

The interfaces are configured with names, security levels, and IP addresses. Table 7 summarizes the interface configuration used along with the corresponding zones:

Table 7 ASA Interface Configuration

Zone	Interface	Security Level	Description
Inside	Port-channel1.70	100	Used to connect to 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 10.70.0.1 255.255.252.0
!
interface Port-channel2.50
 nameif outside
 security-level 0
 ip address 10.50.0.2 255.255.252.0
!
```

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

Configuring Access Control Lists

By default, ASA 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:

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

```
access-list campustodatacenter extended permit ip 10.30.0.0 255.255.252.0 10.70.0.0 255.255.252.0
access-list campustodatacenter extended permit ip 10.50.0.0 255.255.252.0 10.70.0.0 255.255.252.0
access-list campustodatacenter extended permit ip 10.40.0.0 255.255.252.0 10.70.0.0 255.255.252.0
```

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

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

Configuring Unified Computing System

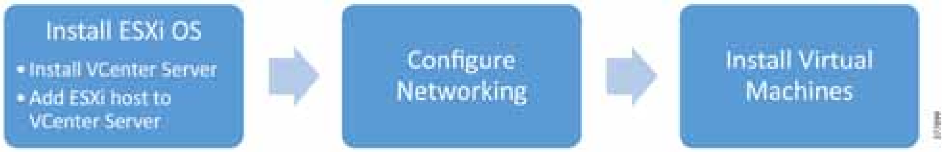
Configuring Virtualization Infrastructure

This section describes how to deploy a Cisco UCS C240 M3 server to provide the virtualized infrastructure required to deploy virtual machines (VMs), for example, Cisco Prime and Cisco ISE. Where applicable, refer to the following Cisco and VMware documentation for details:

- *Cisco UCS C240 M3 Server Installation and Service Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240/install/C240.html
- *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 2.0* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201.html
- *vSphere Installation and Setup Guide* at the following URL:
  - https://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.install.doc/GUID-A71D7F56-6F47-43AB-9C4E-BAA89310F295.html

Note: The Cisco Unified Computing System (UCS) C-Series server platform discussed in this section is used for applications, such as Network Time Protocol (NTP), Cisco Prime Infrastructure, and ISE, through server virtualization. However, any UCS server series or desktop server can be chosen for deployment based on the application's hardware requirements matching the server hardware resources.

Figure 8 Flow Diagram for Virtualization Configuration



Install ESXi OS
- Install VCenter Server
- Add ESXi host to VCenter Server

Configure Networking

Install Virtual Machines

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 UCS C-Series server platform for the data center applications such as Cisco Prime Infrastructure, 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 on the enterprise data center deployment and enable networking according to the production campus network.

To configure VMs’ ESXi networking on the UCS ESXi host, refer to *Setting Up Networking with vSphere Standard Switches* at the following URL:

- https://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.networking.doc/GUID-E198C88A-F82C-4FF3-96C9-E3DF0056AD0C.html

Configuring Network Device Authentication (ISE)

This section covers how to deploy Cisco ISE 2.0 on the UCS server platform in the data center for network devices authentication (TACACS+) and security.

Installation of Cisco Identity Services Engine

The prerequisites and the necessary information to install ISE can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/install_guide/b_ise_InstallationGuide24/b_ise_InstallationGuide24_chapter_00.html

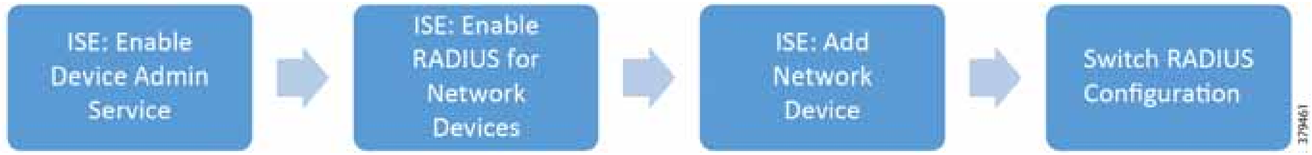
The above book describes different deployment scenarios with ISE. One should choose deployment scenario according to the use case needs.

Configuring Cisco Identity Services Engine (Optional)

Note: The deployment of ISE and AAA configurations in this solution is optional. However, it is recommended to use ISE for devices authentication and enhanced network security.

ISE 2.0 is used for providing device authentication and authorization in the network via TACACS+. ISE 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 TACACS+ communication from the management VLAN 50 to ISE.

Figure 9 AAA Configuration Flow


ISE: Enable Device Admin Service
ISE: Enable RADIUS for Network Devices
ISE: Add Network Device
Switch RADIUS Configuration
379461

Switch AAA Configuration

Perform the following steps on each switch in the network (for example, Cisco Catalyst 4500-X and Cisco Catalyst 3850 stacks and Cisco Catalyst 4506-E switches 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 switch configuration files(s) if you are using the Smart Install feature to configure the switches as described in Initial Installation of Lighting Network, page 5.

1. On the switches, configure ISE as the TACACS+ server. ISE is the name of the RADIUS defined. Any user-defined name can be used. The RADIUS server " ISE" defined 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 as shown here:

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

3. Configure login authentication, exec and console authorization using the following commands, which 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 method ABC on VTY authentication and authorization. From the above step, the different authentication groups that have been created should be attached to the respective login type.

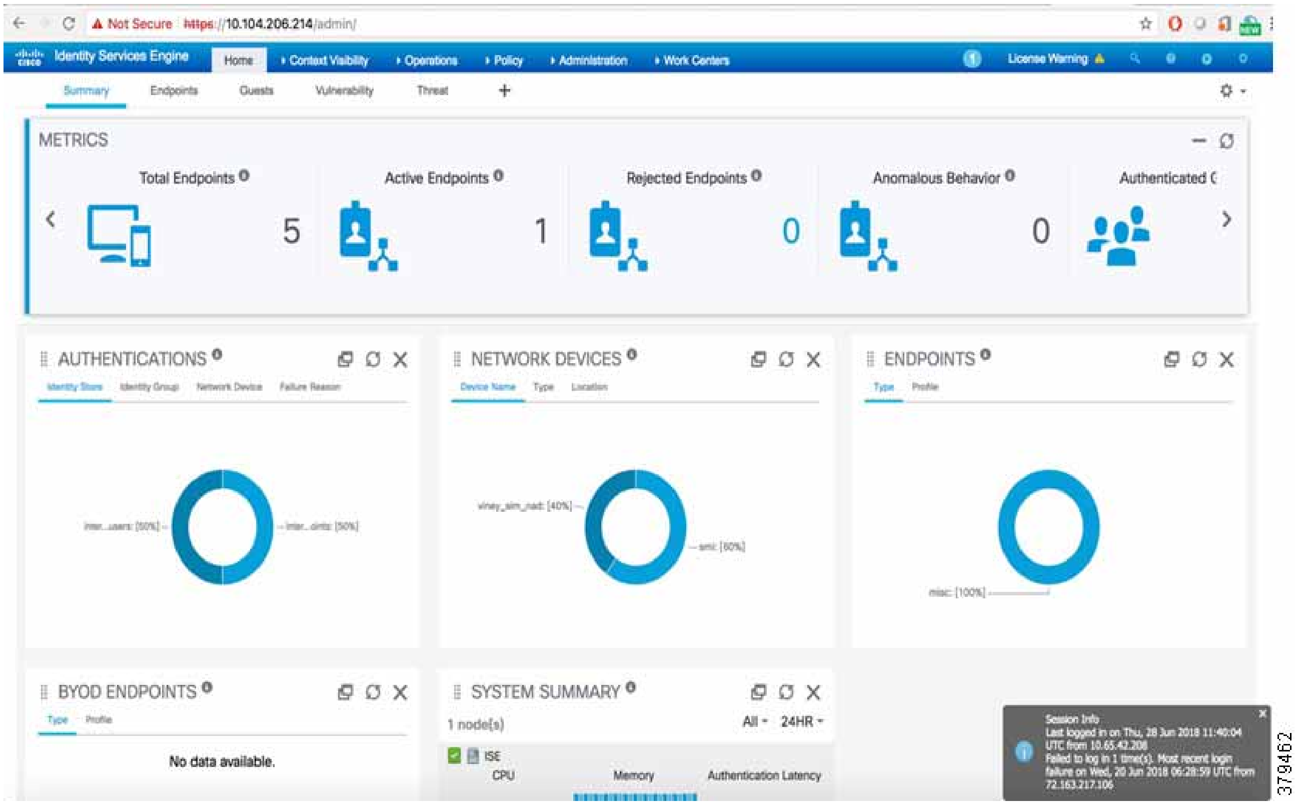
```
line con 0
login authentication SMIconsole
stopbits 1
speed 115200
    line vty 0 4
login authentication telnetConsole
    line vty 5
login authentication telnetConsole
```

ISE Configuration

Perform the following steps on the ISE server for enabling RADIUS-based device authentication and authorization:

1. Log in to ISE. Figure 10 shows the ISE summary after successful login.

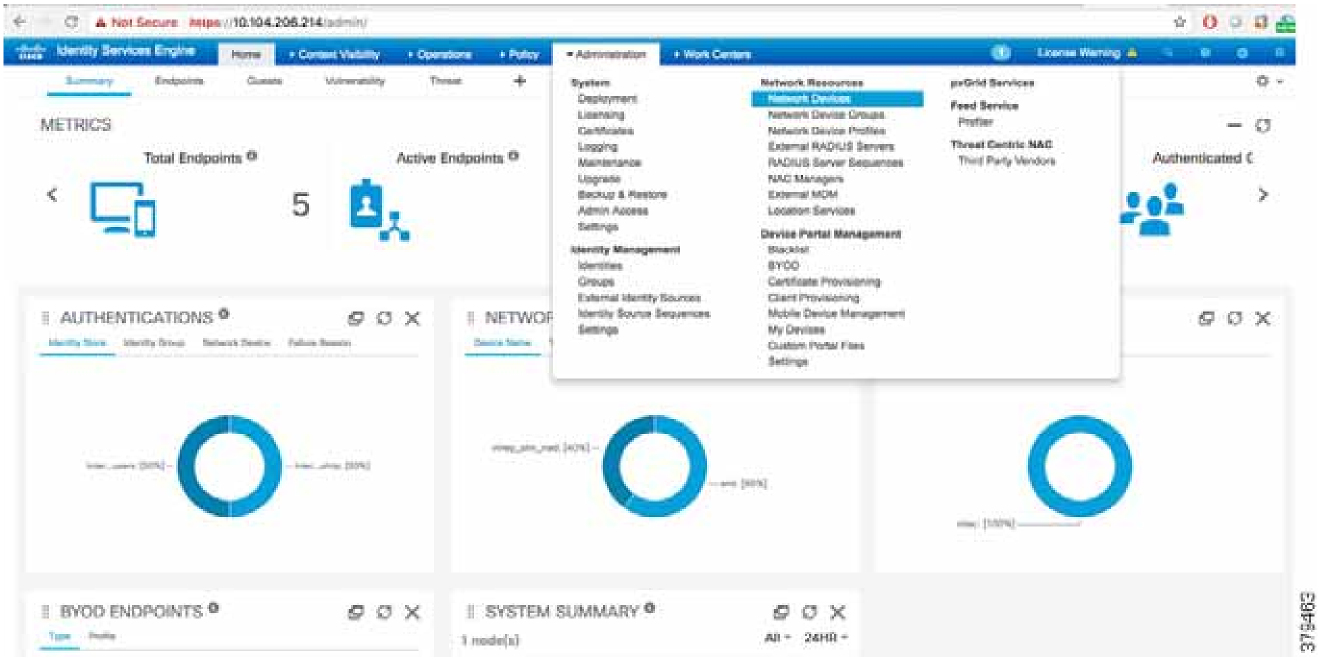
Figure 10 ISE Login Success Page



Session Info
Last logged in on Thu, 28 Jun 2018 11:40:04 UTC from 10.65.42.208
Failed to log in 1 time(s). Most recent login failure on Wed, 20 Jun 2018 06:28:59 UTC from 72.163.217.106

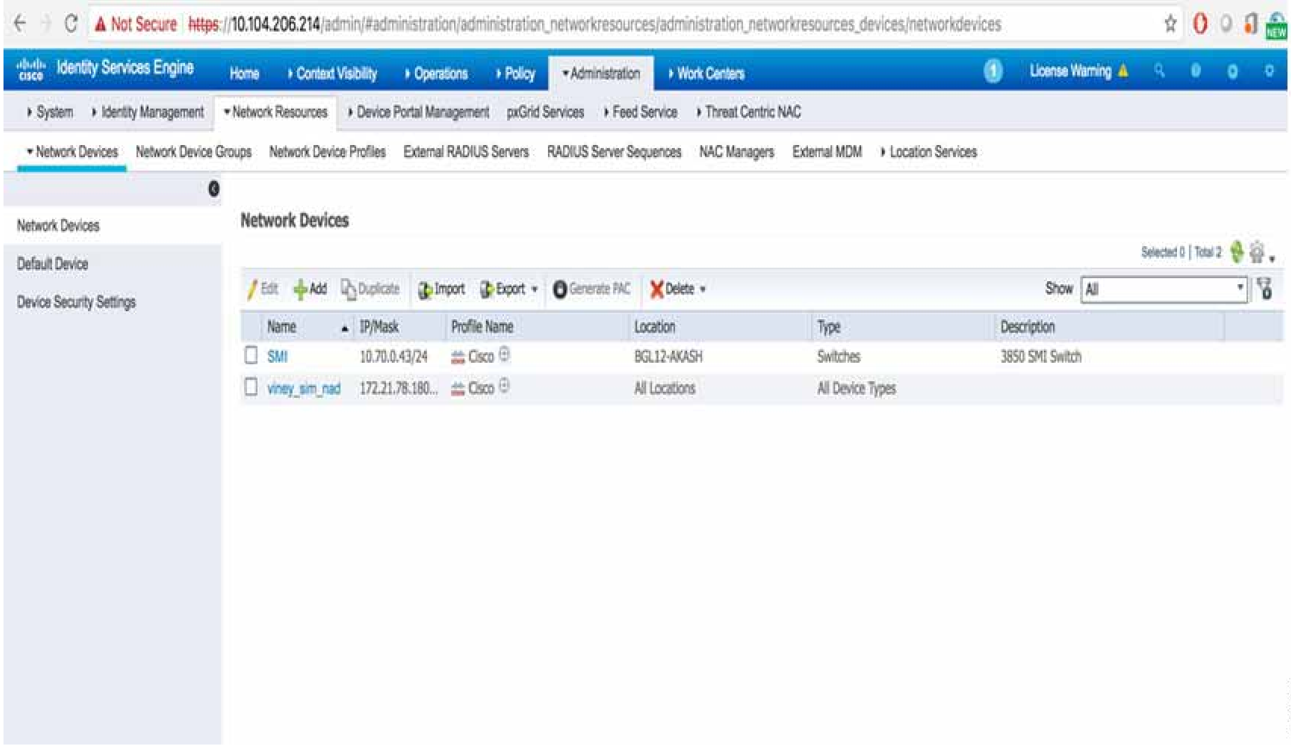
2. Add the 3850 standalone switch or the stack as a network device to ISE. To add the network device, from **Administration > Network Resources**, click **Network Devices** as shown in Figure 11.

Figure 11 Choose Network Devices in ISE



3. On choosing **Network Devices**, the page should display a list of the devices (if any) that were added.

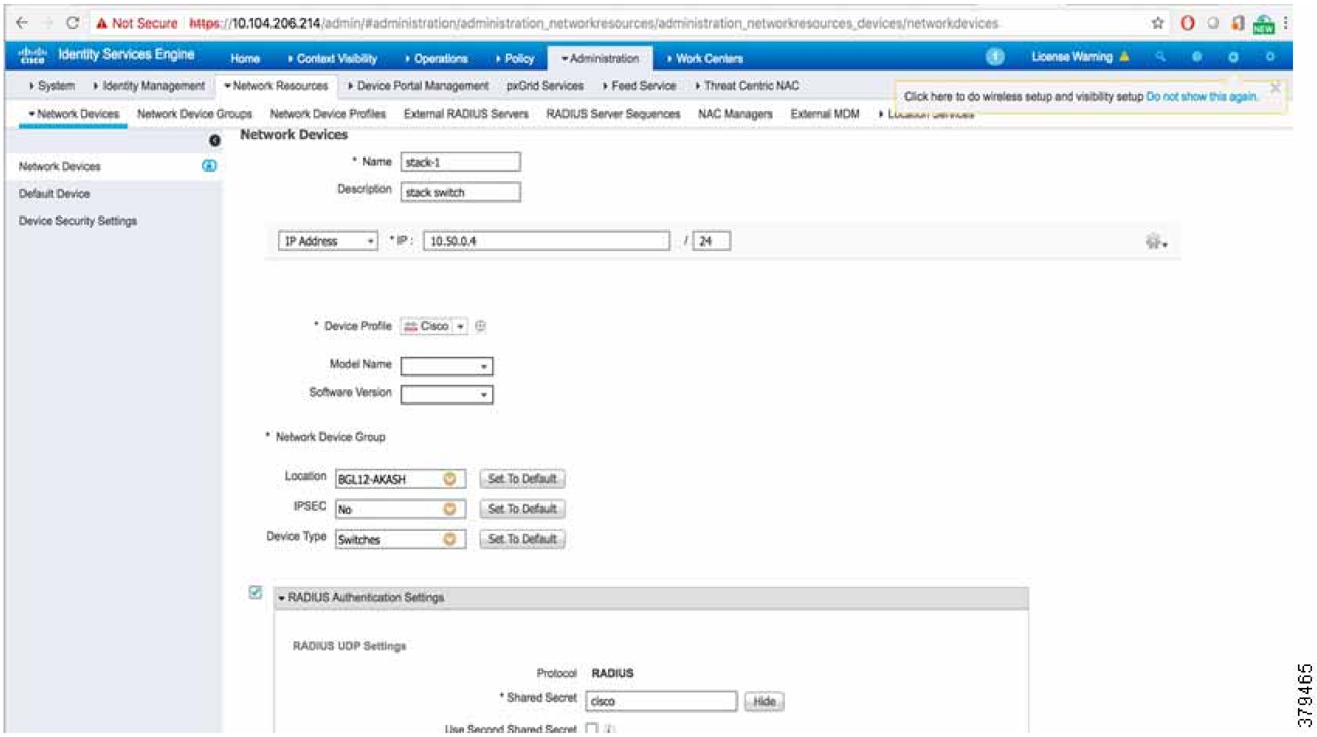
Figure 12 Network Devices in ISE



Name	IP/Mask	Profile Name	Location	Type	Description
☐ SMI	10.70.0.43/24	Cisco	BGL12-AKASH	Switches	3850 SMI Switch
☐ viney_sim_nad	172.21.78.180...	Cisco	All Locations	All Device Types	

4. To add network device to the list, click **Add**, and then 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 in ISE



Network Devices

* Name: stack-1

Description: stack switch

IP Address * IP : 10.50.0.4 / 24

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: BGL12-AKASH

IPSEC: No

Device Type: Switches

☑ RADIUS Authentication Settings

RADIUS UDP Settings

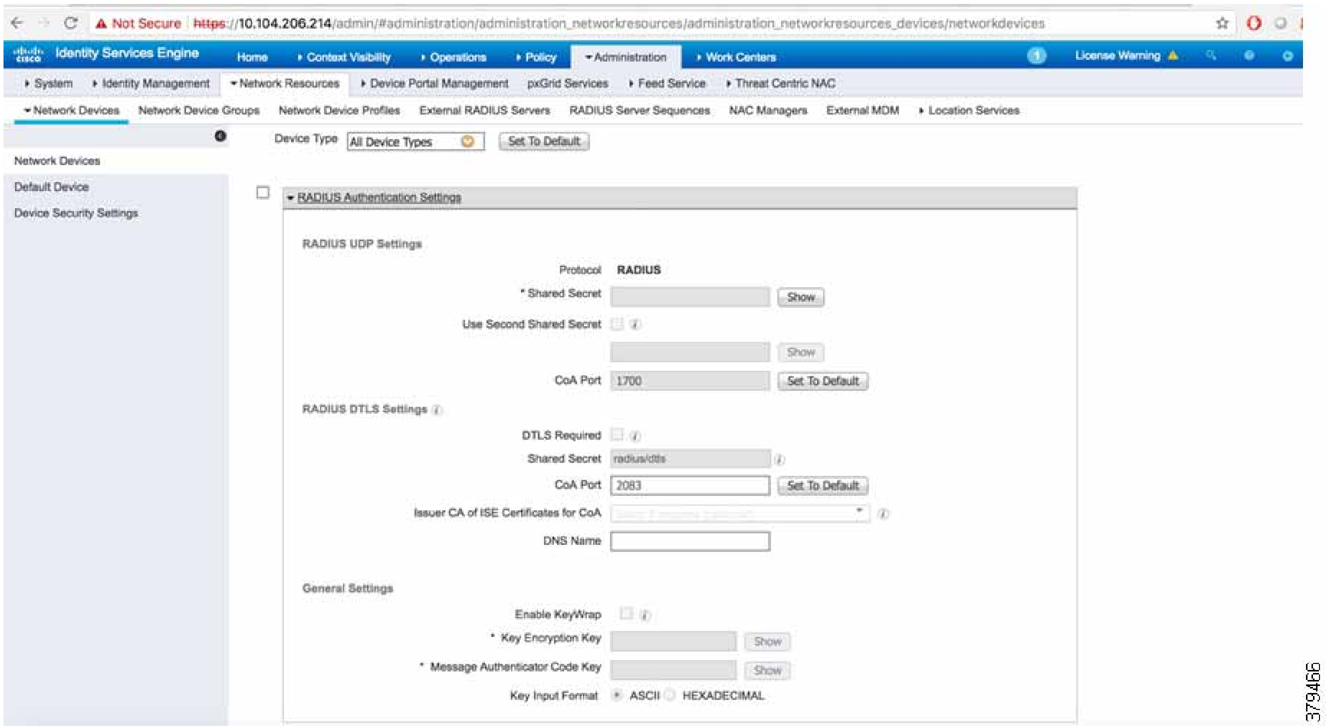
Protocol: RADIUS

* Shared Secret: cisco

Use Second Shared Secret: □

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

Figure 14 RADIUS Authentication Settings



Device Type: All Device Types

☐ ▾ RADIUS Authentication Settings

RADIUS UDP Settings

- Protocol: RADIUS
- * Shared Secret: [Show]
- Use Second Shared Secret: ☐
- CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings

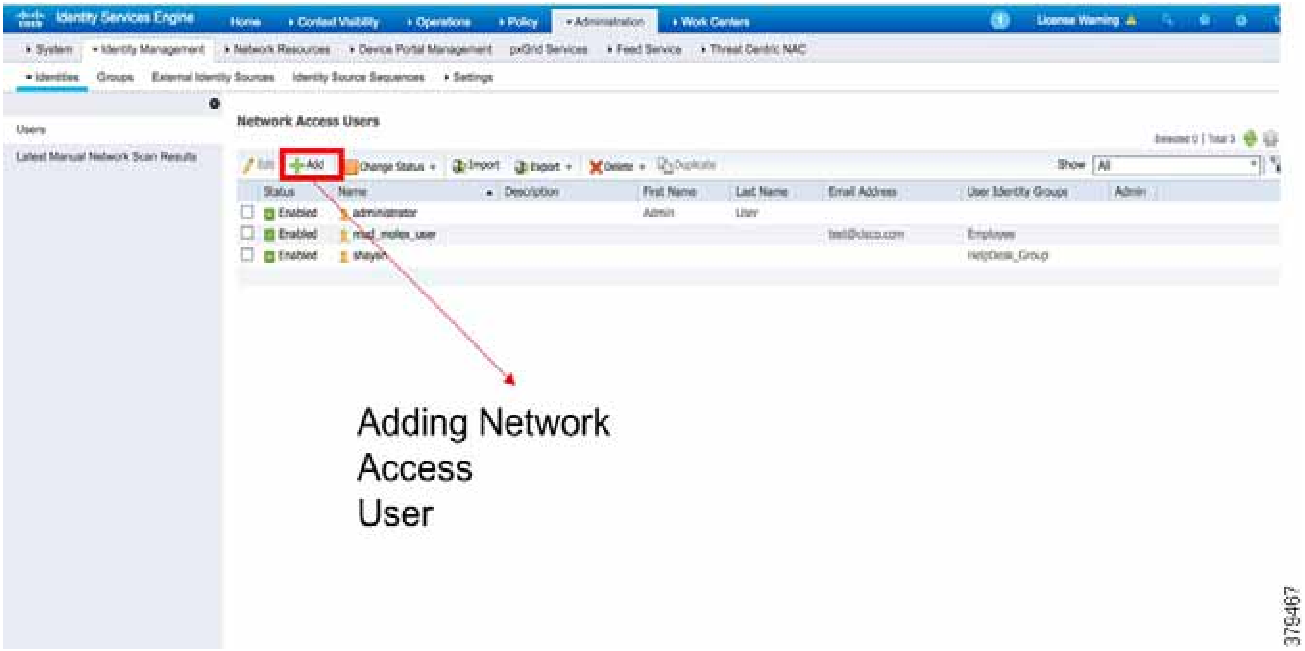
- DTLS Required: ☐
- Shared Secret: radius/dtls
- CoA Port: 2083 [Set To Default]
- Issuer CA of ISE Certificates for CoA:
- DNS Name:

General Settings

- Enable KeyWrap: ☐
- * Key Encryption Key: [Show]
- * Message Authenticator Code Key: [Show]
- Key Input Format: ● ASCII ○ HEXADECIMAL

6. 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 New User in Identity Management

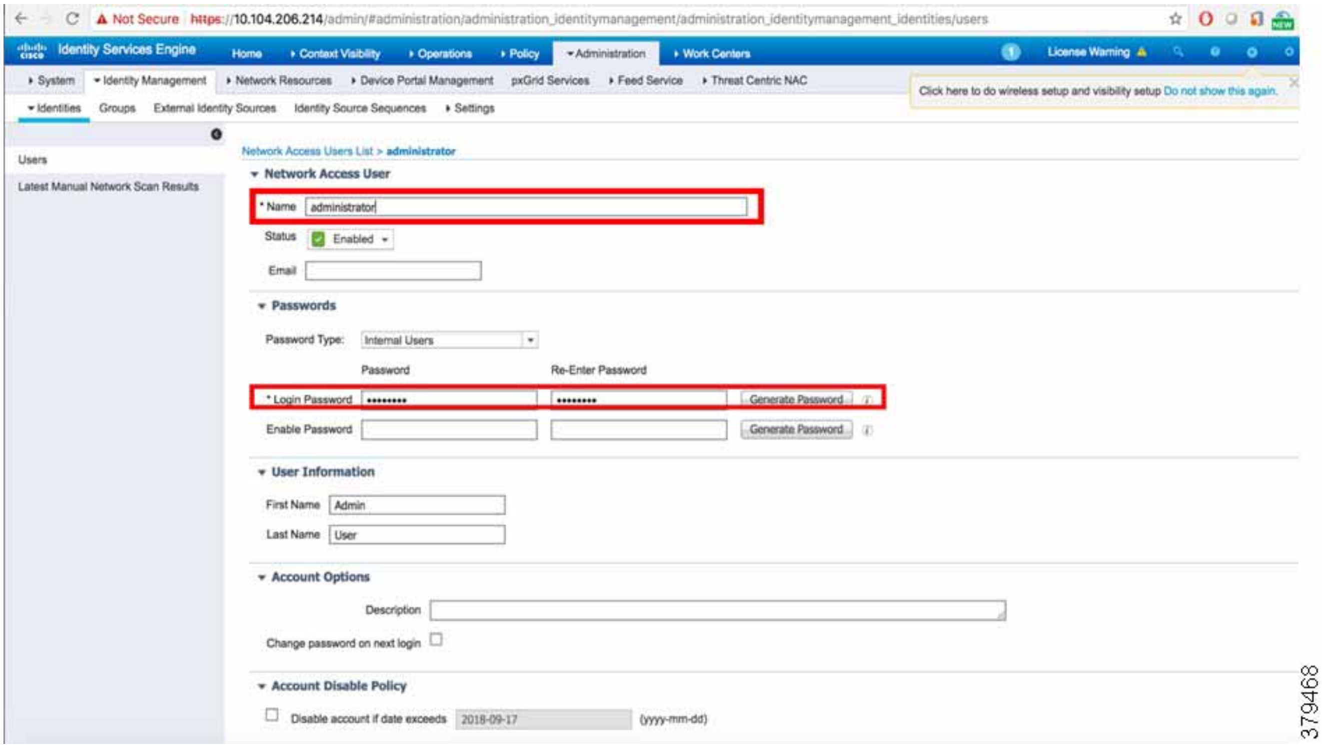


Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	administrator		Admin	User			
□	Enabled	mad_molex_user				test@cisco.com	Employee	
□	Enabled	shaysh					HelpDesk_Group	

Adding Network Access User

Figure 16 Creating a New User in Identity Management



Network Access Users List > administrator

Network Access User

* Name: administrator

Status: Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	•••••••••	•••••••••
Enable Password		

User Information

First Name: Admin

Last Name: User

Account Options

Description:

Change password on next login □

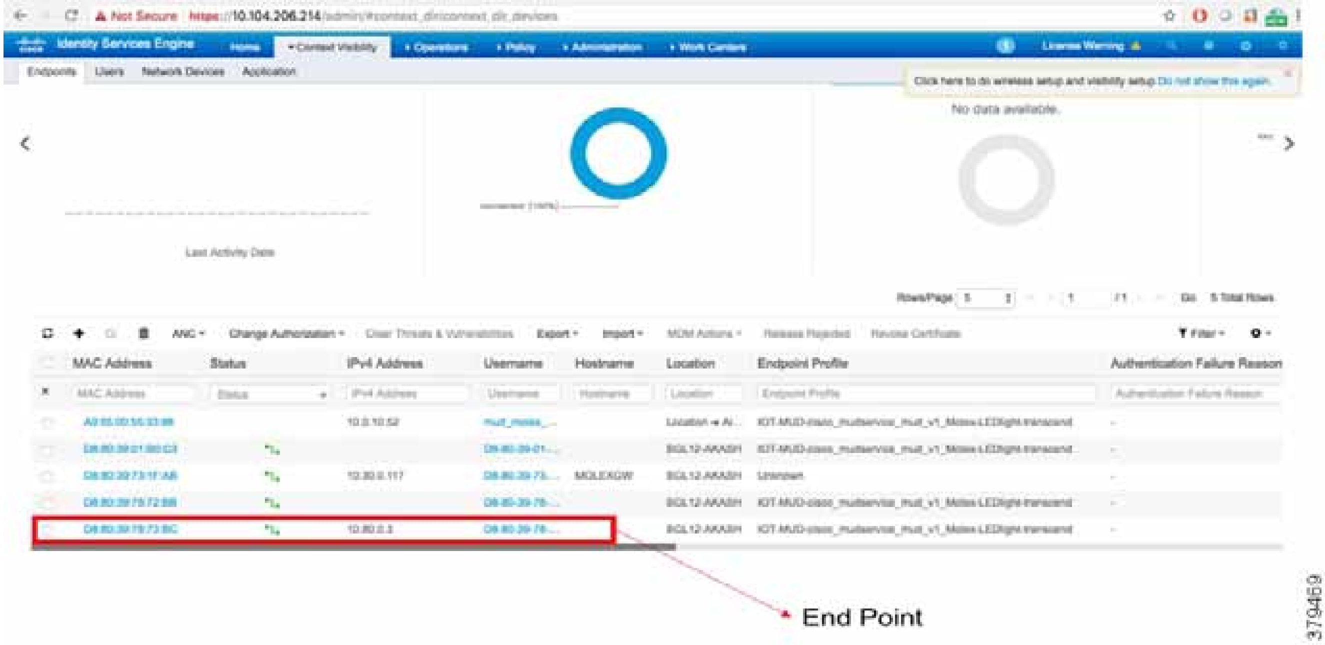
Account Disable Policy

□ Disable account if date exceeds 2018-09-17 (yyyy-mm-dd)

This completes the ISE 2.0 RADIUS configuration for network devices authentication and authorization.

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

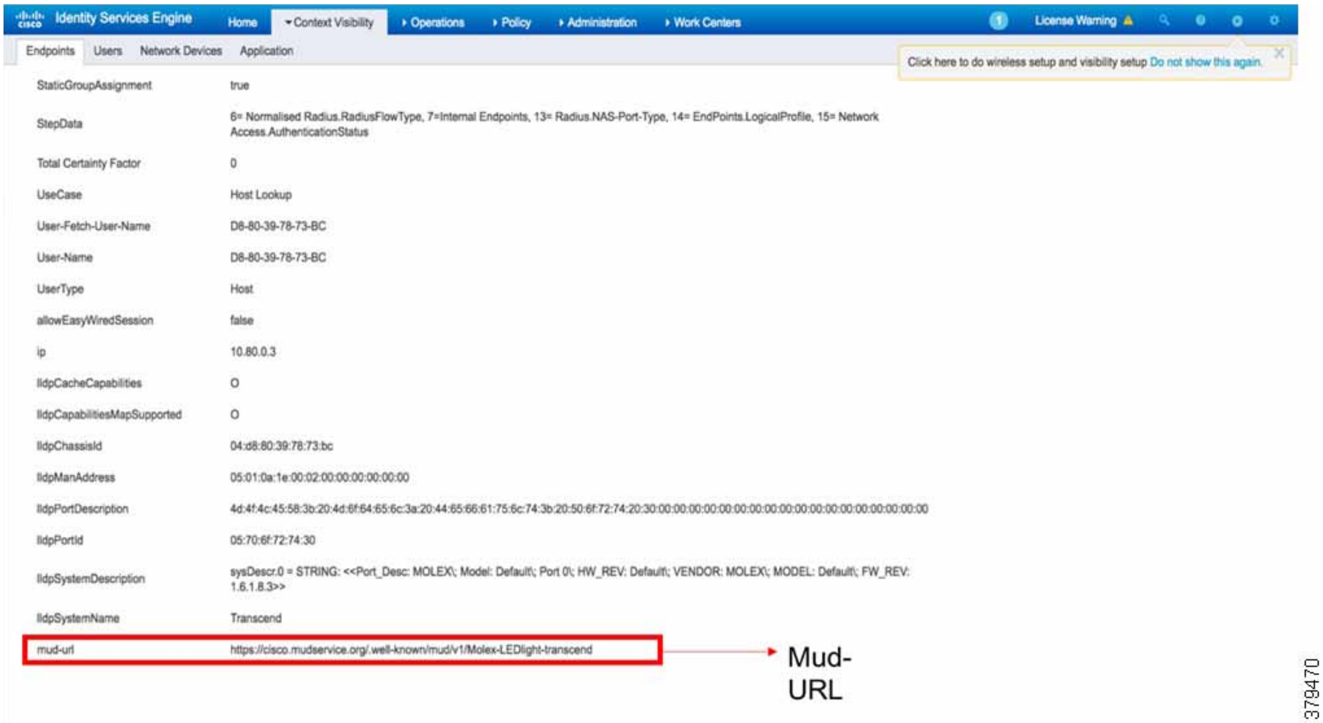
Figure 17 End Points List



MAC Address	Status	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason
A0:55:00:55:33:88		10.0.10.52	mud_molex_...		Location → Al...	IOT-MUD-cisco_multiservice_mud_v1_Molex-LEDlight-transcend	-
D8:80:39:01:80:C3			D8-80-39-01-...		BGL12-AKASH	IOT-MUD-cisco_multiservice_mud_v1_Molex-LEDlight-transcend	-
D8:80:39:73:1F:AB		10.80.0.117	D8-80-39-73-...	MOLEXGW	BGL12-AKASH	Unknown	-
D8:80:39:79:72:BB			D8-80-39-79-...		BGL12-AKASH	IOT-MUD-cisco_multiservice_mud_v1_Molex-LEDlight-transcend	-
D8:80:39:79:73:BC		10.80.0.3	D8-80-39-79-...		BGL12-AKASH	IOT-MUD-cisco_multiservice_mud_v1_Molex-LEDlight-transcend	-

8. On clicking one of the end points, choose the **Attributes** tab and then scroll to the bottom of the tab to see the MUD-URL. This is shown in Figure 18.

Figure 18 MUD-URL Visibility



Click here to do wireless setup and visibility setup Do not show this again.

StaticGroupAssignment	true
StepData	6= Normalised Radius.RadiusFlowType, 7=Internal Endpoints, 13= Radius.NAS-Port-Type, 14= EndPoints.LogicalProfile, 15= Network Access.AuthenticationStatus
Total Certainty Factor	0
UseCase	Host Lookup
User-Fetch-User-Name	D8-80-39-78-73-BC
User-Name	D8-80-39-78-73-BC
UserType	Host
allowEasyWiredSession	false
ip	10.80.0.3
lldpCacheCapabilities	O
lldpCapabilitiesMapSupported	O
lldpChassisId	04:d8:80:39:78:73:bc
lldpManAddress	05:01:0a:1e:00:02:00:00:00:00:00:00
lldpPortDescription	4d:4f:4c:45:58:3b:20:4d:6f:64:65:6c:3a:20:44:65:66:61:75:6c:74:3b:20:50:6f:72:74:20:30:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
lldpPortId	05:70:6f:72:74:30
lldpSystemDescription	sysDescr.0 = STRING: <<Port_Desc: MOLEX\; Model: Default\; Port 0\; HW_REV: Default\; VENDOR: MOLEX\; MODEL: Default\; FW_REV: 1.6.1.8.3>>
lldpSystemName	Transcend
mud-url	https://cisco.mudservice.org/.well-known/mud/v1/Molex-LEDlight-transcend

Configuring Network Management (Cisco Prime Infrastructure)

Cisco Prime Infrastructure is a network management system used to monitor and manage the devices in the network. Prime Infrastructure is also used as a syslog server.

Installation of Cisco Prime Infrastructure

1. Download the Prime Infrastructure 3.0 Open Virtualization Application (OVA) file from the Cisco website at the following URL:

   https://software.cisco.com/download/release.html?mdfid=286285348&flowid=&softwareid=284272932&release=3.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

2. Launch your VMware vSphere Client and connect to the ESXi host or vCenter server.
3. Click **File > Deploy OVF Template**.
4. Choose the OVA file downloaded in Step 1 in the **Select** window.
5. Click **Next** and then respond as per the prompt.

For detailed installation instructions, refer to the “Installing Cisco Prime Infrastructure” section in the *Cisco Prime Infrastructure 3.0 Quick Start Guide* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/quickstart/guide/cpi_qsg.html

Configuring Cisco Prime Infrastructure for Lighting

For more details, refer to the “Adding Devices to Prime Infrastructure” section in the *Cisco Prime Infrastructure 3.0 User Guide* at the following URL:

- http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug.html

The following are the high level steps to add the device to the Cisco Prime Infrastructure:

1. Launch PI User Interface using a web browser using PI IP address.
2. Log in to the GUI with the username and password.
3. In the main menu, click **Inventory > Network Devices > Add Device**.
4. Enter the SNMP and CLI credentials of the device.
5. Click **Verify Credentials**.
6. If credentials are correct, click **Add**.

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** on the right window, if required, and then choose **CoAP v1.1** from the drop-down menu.
5. From 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 v1.1**.
8. From the **Zone** tab, create a zone by dragging the mouse creating a rectangular area covering the fixture and the 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 the implementation of lighting control and management use cases using Molex Coresync Manager, Facility Manager, wireless wall switch, and Smart Tablet.

The steps described in this section provides a high-level summary of steps, to implement light fixtures control and management of zones during commissioning. Refer to the latest documentation provided by Molex for 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/OFF or dimmed UP/DOWN using the Molex Facility Manager.

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

On/Off/Dimming Control using Wireless Wall Switch

Alternatively, the light fixtures can also be controlled via the wireless wall switch. The wall switch controls all the light fixtures of a 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 Wireless Switch using the MoDiag tool. Refer to the *Molex Coresync Commissioning Guide* for detailed steps to pair the wireless switch and gateway.
2. On 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 digits of the Hex ID in the **Daisy Chain ID** section.
4. Set the polling rate to Zero.
5. Configure it in the zone that you wish to control.
6. Upload the Project.
7. Press the button on the Wireless Switch to switch the lights ON/OFF. Verify that light fixtures switch ON/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 a day light. This helps in saving power.

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

Light Scene Selection 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*.

Light Fixture Control using Coresync Smart Tablet

Molex Coresync Smart Tablet is a tool used to control a single commissioned zone available through the Coresync Smart Controller on the same network.

For more details on the Coresync Smart Tablet, refer to the *Molex Coresync Manager User Guide*.

For wireless network access, make sure to enable all required configuration on wireless access point as per the Campus network wireless access best practices described in the *Design Zone for Campus Wired and Wireless LAN*.

Installing Applications

The Smart Tablet consists of two components: the Zone ID Application for zone commissioning and the End User Tool for controlling the zone. The Smart Tablet is designed to control only one zone.

Refer to the *Molex Coresync Manager User Guide* for installing and configuring the Smart Tablet for light fixture controls.

Commissioning a Zone using ZoneID

The commissioning of the zone is done using the ZoneID application. Refer to the *Molex Coresync Manager User Guide* for the zone commissioning procedure using Smart Tablet.

Light Fixtures Ongoing Maintenance

Replacing Light Fixtures

When a light fixtures 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 old light fixture in the same network subnet.

This requires the recommissioning of the lights fixture in the Molex Coresync Manger design tool and projects. Therefore, follow through the commissioning procedure as suggested by Molex for replacing the light fixture. The following provides a summary of steps to be performed.

Modify Light Fixture in 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 the target old fixture to be replaced and change the IP address of the fixture to that of the new fixture.
2. Similarly, change the IP address for the sensors added of 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 the list of open issues in the system and workarounds for open issues.

Table 8 Caveats with Workarounds

Open Issues	Workaround
Molex light fixtures require recommissioning if they are already commissioned for deployment and DHCP-assigned IP address changes for the light fixture.	Not available. Planned maintenance and outage notification is required if light fixture re-commissioning is needed.
DHCP IP address to MAC address binding changes due to lease expiration and light fixture MAC address change. If the Molex Coresync Gateway MAC address of light fixtures changes in later firmware version(s), it is required to recommission the light fixture in the Molex project. Light fixtures will not be controllable until recommissioning is performed.	Not available. Molex should not override or change the MAC of light fixtures upon firmware upgrades of light fixtures which are already deployed.
IP DHCP snooping and IP Source Guard security features described in this document do not work as expected in this CVD release due to known issues.	Not 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 45
- Molex Documentation, page 46
- Third Party Documentation:, page 46

Cisco Documentation

- *Design Zone for Campus Wired and Wireless LAN* at the following URL:
  - http://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html#~validate
- *Cisco Catalyst 3850 Switch Data Sheet* at the following URL:
  - http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/data_sheet_c78-720918.html
- *Catalyst 4500 Series Switch Software Configuration Guide, IOS XE 3.9.xE and IOS 15.2(5)Ex* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-9-0E/15-25E/configuration/guide/xe-390-configuration/vss.html
- *Catalyst 3850 Hardware Installation Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/b_c3850_hig/b_c3850_hig_chapter_010.html

- *Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html
- *Consolidated Platform Configuration Guide, Cisco IOS 16.9.X and Later (Catalyst 3850 Switches)* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/37e/consolidated_guide/b_37e_consolidated_3850_cg.html
- *Cisco UCS C240 M3 Server Installation and Service Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240/install/C240.html
- *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 2.0* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201.html
- *Cisco Prime Infrastructure (PI) Installation and Configuration Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/quickstart/guide/cpi_qsg.html#pgfId-63672
- *Cisco Identity Services Engine (ISE) Installation and Configuration Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/installation_guide/b_ise_InstallationGuide20/Installing_ISE_on_a_VMware_Virtual_Machine.html
- *Cisco Prime Infrastructure 3.0 Quick Start Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/quickstart/guide/cpi_qsg.html
- *Cisco Prime Infrastructure 3.0 User Guide* at the following URL:
  - http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-0/user/guide/pi_ug.html

Molex Documentation

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

Third Party Documentation:

- VMware vSphere Installation and Setup

Appendix B: Glossary

Term	Definition
AAA	Authentication, Authorization and Accounting
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
ASA	Cisco Adaptive Security Appliance
ALS	Ambient Light Sensor
BPDU	Bridge Protocol Data Unit
CRD	Cisco Recommended Design
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
PI	Cisco Prime Infrastructure
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
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	Universal Power over Ethernet
UDP	User Datagram Protocol

Term	Definition
VM	Virtual Machine
VLAN	Virtual Local Area Network
VSS	Virtual Switching System