



## System Architecture

---

This chapter includes the following major topics:

- [System Topologies, page 3-1](#)
- [Design Considerations, page 3-6](#)
- [System Design, page 3-7](#)

The Cisco Digital Building Cree Solution contains Cree light fixtures, which are based on troffers and recessed downlights, and which are controlled by the SmartCast Manager application (SCM) and a wall dimmer. Cree light fixtures have advanced lighting control occupancy and daylight harvesting sensors that provide the right amount of light based on daylight conditions. The Cree lighting fixtures and SCM communicate using Cree's proprietary UDP-based SmartCast protocol.

Cree's OneButton™ Setup commissioning feature, which is part of the SmartCast® functionality, groups up to 1,000 light fixtures at a time. The OneButton Setup uses the Cree proprietary algorithms and embedded sensors to automatically form the occupancy and switch groups. The configuration tool (CT) can also be used to form or modify the groups in existing lighting networks.

In a switch group, the Cree wall dimmer controls the light fixtures so that a user can turn on, off or dim a light or group of lights. The occupancy groups are controlled by the occupancy sensor and can automatically turn a group of light fixtures on and off based on the occupancy in a room.

Each Cree light fixture has an ambient light sensor (ALS) used to enable daylight harvesting and automatically dim the lights on a sunny day or if other light sources are available.

The light fixtures are connected to the Cisco UPoE switches, which provide power to the light fixtures and access layer security with ACL configuration on the access ports that allows only SmartCast® UDP traffic on ports connected to the fixtures. Refer to [Security, page 3-9](#) for security recommendations.

## System Topologies

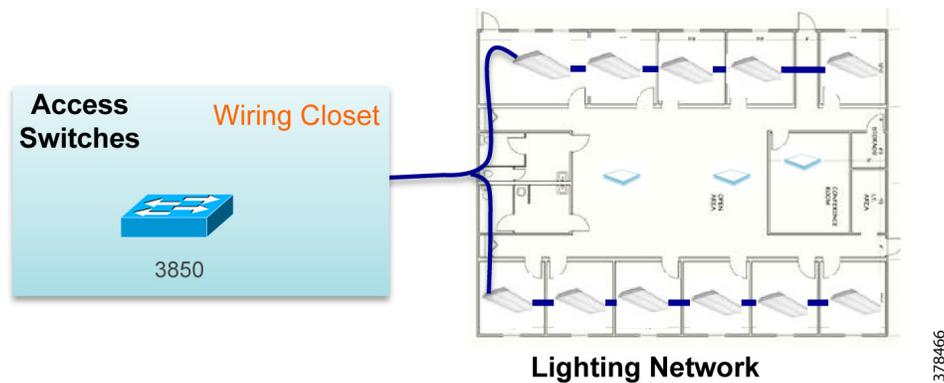
The Cisco Digital Building Cree Solution can be deployed in multiple scenarios, based on a customer's requirements. This section explains different deployment topologies.

### Initial Setup with Cisco Catalyst 3850 UPoE Series Switch

During the initial/greenfield deployment, the UPoE switch is deployed like any other LAN access switch in a wiring closet. On Day 0, the electrician will install the light fixtures, wall dimmers, and UPoE switch as shown in [Figure 3-1](#). When the light fixtures are connected to UPoE switch with default factory

configuration, the light fixtures will come up with low brightness. The customer's technology team (IT) needs to be aware that the electrician cannot test the full brightness of the lighting fixtures until static power configuration is enabled on the UPoE switch ports connected to light fixtures.

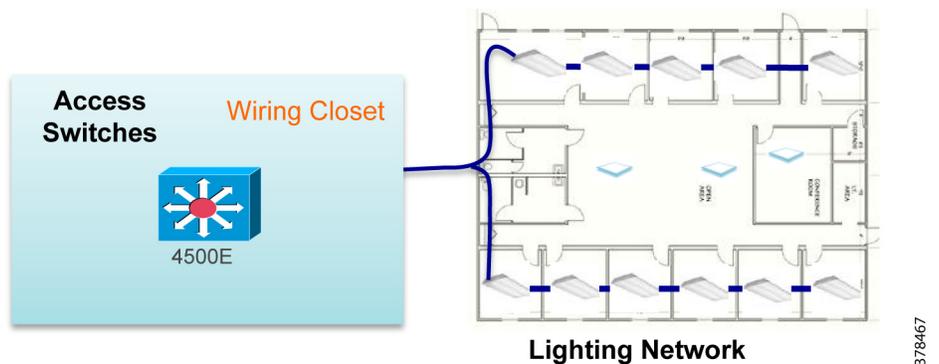
**Figure 3-1** Initial Setup with Cisco Catalyst 3850 UPoE Series Switch



## Initial Setup with Cisco Catalyst 4500-E UPoE Series Switch

A scenario exists when a customer wants to deploy this solution based on a modular switch instead of a stackable switch. The Cisco Catalyst 4500E UPoE switch serves this purpose, but it still requires separation between the light network and other shared services by having a separate VLAN for the lighting network. The initial/greenfield installation on a Day 0 remains the same on the Cisco Catalyst 4500-E UPoE switch as described in [Initial Setup with Cisco Catalyst 3850 UPoE Series Switch](#), page 3-1.

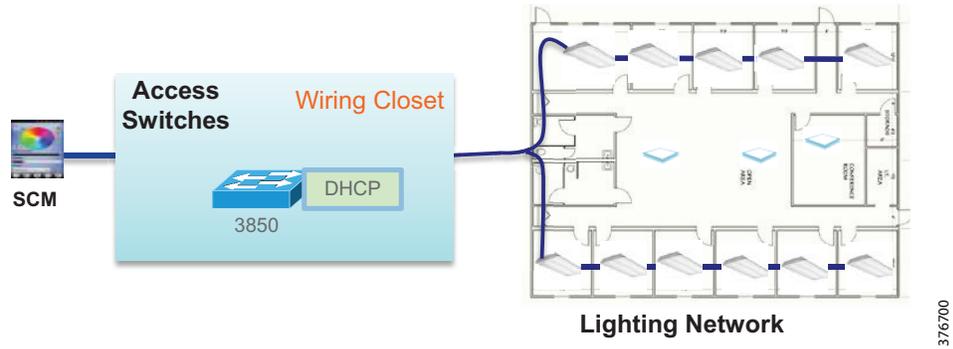
**Figure 3-2** Initial Setup with Cisco Catalyst 4500-E UPoE Series Switch



## Cisco Digital Building Cree Solution Provisioning without Uplink

When an access switch does not have an uplink connection and lighting network provisioning is required, a DHCP server needs to be configured on an access switch. Cree SCM is directly connected to the switch, as shown in [Figure 3-3](#). The SCM is required to configure, calibrate, monitor, and control the light fixtures.

Figure 3-3 Cisco Digital Building Cree Solution Provisioning with No Uplink

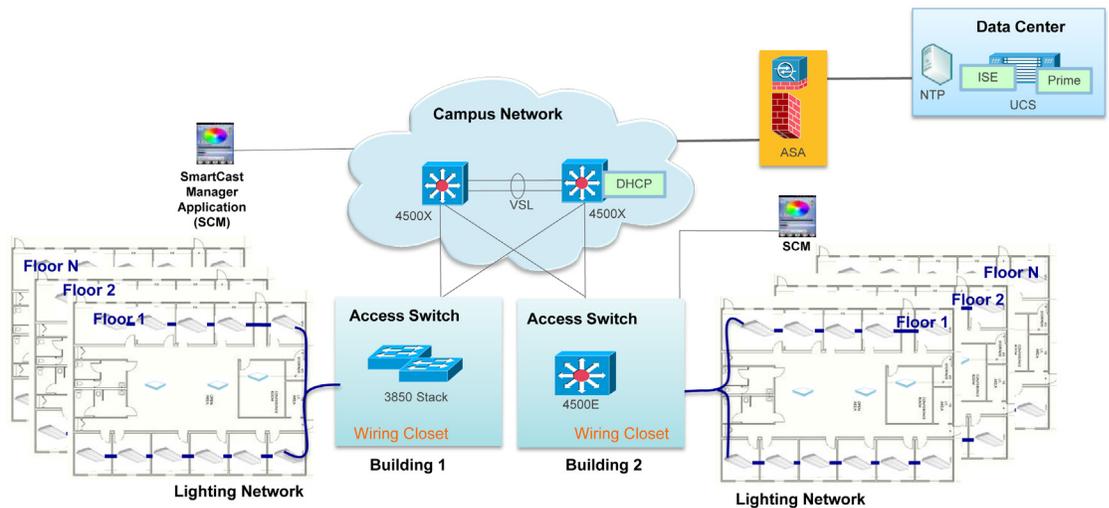


376700

## Large Scale Deployment

Figure 3-4 shows the architecture for large-scale deployment where the light fixtures are connected on Cisco Catalyst 3850 stack and Cisco Catalyst 4500-E UPoE switches. The access switches are connected to the Campus Network cloud, which is agnostic to the Cisco Digital Building Cree Solution. (The design of Campus Network is out of scope of this document.) The critical services required to manage the UPoE switches, such as Syslog, TACACS+, SNMP, and NTP reside in the data center, which is protected by the firewall. All critical services run on a separate management VLAN, which spans from the data center to the UPoE switches. The firewall blocks all other traffic except the management services on the management VLAN.

Figure 3-4 Cisco Digital Building Cree Solution Large Scale Deployment

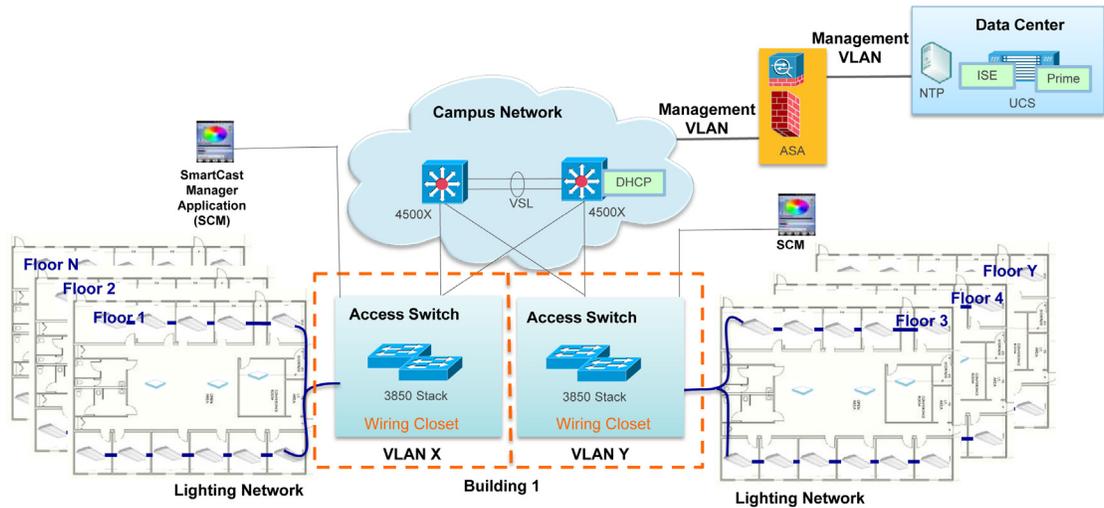


376468

# Logical Building Deployment

Cree SCM can support 1000 light fixtures in a VLAN. A different broadcast domain/VLAN is required for lighting networks containing over 1000 lighting fixtures. When more than 1000 lighting fixtures exist in a building, multiple VLANs are required to logically divide a building into different broadcast domains. The other requirement of Cree SCM is that each broadcast domain should have its own SCM. The same SCM can be used to connect to multiple VLANs, but it can manage one VLAN at a time. The location of SCM is flexible; it can be connected to any switch in the network of the managed light fixtures.

**Figure 3-5** Cisco Digital Building Cree Solution with Different VLANs

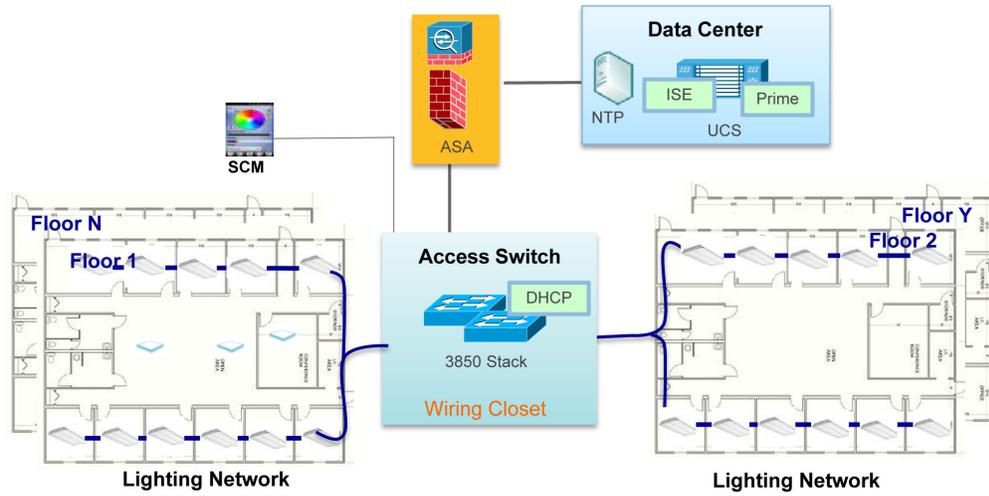


378469

# Deployment without Campus Network

When the Cisco Digital Building Cree Solution is deployed in an environment without a Core/Campus Network, the access switches are directly connected to the data center via a firewall.

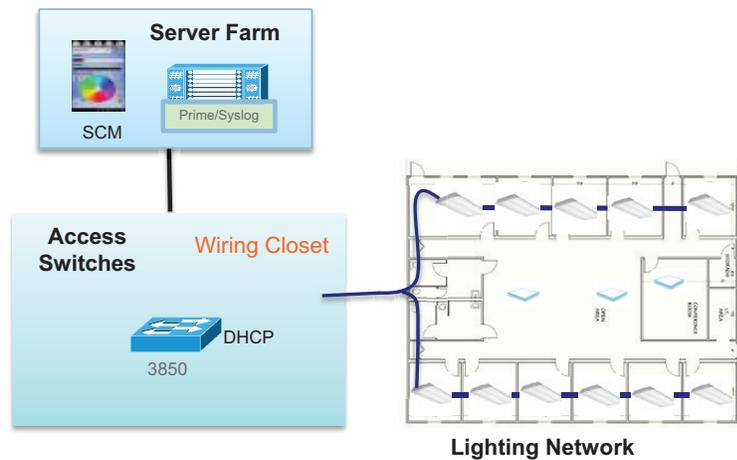
**Figure 3-6** Cisco Digital Building Cree Solution No Campus Network



# Small-Scale Deployment

When a lighting solution needs to be deployed in a small store or office that contains 20 or fewer lighting fixtures, the Cisco Catalyst 3850 UPoE switch is sufficient with all the application services, such as SCM directly connected to the switch. The DHCP server is configured on the access switch.

**Figure 3-7** Cisco Digital Building Cree Solution Small Scale Deployment





# System Design

The Cisco Digital Building Cree Solution design is fully described in this section. Topics include:

- Lighting End Points
- SmartCast Manager Application
- Network Infrastructure
- Security
- Power Management
- High Availability

## Lighting Fixtures

Cree SmartCast light fixtures are shipped from the factory with advanced lighting control sensors and embedded intelligence, which provides the right amount of light based on changing daylight conditions. The light fixtures share data with each other from their integrated occupancy and daylight sensors and use their embedded intelligence, which is based on the Cree proprietary algorithm, to provide precisely the right amount of light at the right time, based on changing conditions within the building. The light fixture will automatically synchronize with rest of the group for state, mode, and settings on power cycle/reset and during rejoining the network.

The different models of Cree fixtures require different amounts of power for the full brightness, which is reflected in [Table 3-1](#). The light fixtures will come to full brightness when static power is configured on the UPoE switch.

The Cree CR series light fixtures feature field-tunable color temperatures from 3000 Kelvin to 5000 Kelvin. The Cree KR series is offered in two fixed color temperature variants at 3500 and 4000 Kelvin.

For more details about the Cree lights, refer to the following link:

- <http://lighting.cree.com/products/controls/cree-smartcast-technology>

## SmartCast Manager Applications

The SCM provides system control, monitoring, maintenance, firmware upgrade, and reporting for the lighting network. The SCM's OneButton Setup feature provides automatic discovery, calibration, and grouping of the fixtures. The auto-grouping is formed by LightCasting, which lets fixtures know what devices are nearby. Once SCM does the OneButton commissioning, users can modify or customize their grouping and setting requirements very easily. The configuration tool can be used to form or modify the groups in existing lighting networks.

The OneButton setup process creates two types of groups: an occupancy group and a switch group.

- Occupancy groups form a set of fixtures that work in unison when someone enters the space and triggers an occupancy event.
- The switch group forms a set of light fixtures controlled by wall dimmers.

For both types of groups, light fixtures automatically turn off when vacancy is detected. A light fixture can only reside in one switch group and one occupancy group.

The SCM automatically detects a connected physical network interface that contains Cree light fixtures and provides a selection option if multiple network interfaces are found that have Cree light fixtures. The SCM use SNMP discovery mechanism to gather the information of the switch ports on which the Cree light fixtures are connected and provide users access to control these ports.

The SCM also displays the power savings and usage metrics for the network of commissioned light fixtures. SCM is installed on a PC and then connects to the local lighting network. It provides the following features:

- Power Visualization Savings: Bar Chart
- .csv File Export Features/Control of Power and OCC data storage
- Network Interface Selection
- Network Access Code Support (refer to the security section)
- Basic Fixture health monitoring

## Network Infrastructure

### Addressing

The Cree light fixtures supports IPv4 only. The DHCP server will dynamically assign IP addresses to light fixtures.

The DHCP server is configured on the aggregate switch to reduce the overhead of administering IP addresses.

However, in a scenario where the light fixtures are connected to an access switch that does not have an uplink connection, the DHCP needs to be configured on the access switch in order to provision the light fixtures. After the commissioning phase, DHCP configuration can be migrated to the aggregate switch to reduce the overhead of administering and managing DHCP service on access switch. In that case, keep the IP address pool the same during the migration.

### UPoE Switch Features

The Cisco Catalyst 3850 and Cisco Catalyst4500-E series switches used in this solution support the following general features:

#### **Cisco Catalyst 3850:**

- Universal Power over Ethernet (UPoE) with 60W power per port in 1 rack unit (RU) form factor.
- Enterprise-class stackable switch.
- Dual redundant, modular power supplies and three modular fans providing redundancy.
- Power Stacking allows the power supplies to share the load across multiple systems in a stack.
- The Cisco Catalyst 3850 provides power in constant mode with two enhanced features for light solutions as described below:
  - Perpetual PoE—Perpetual PoE power to Power Devices (PD) during reloads. POE power delivered to PDs must be uninterrupted during a control plane reboot.
  - Fast PoE—The switch on a recovery after power failure provides power to the connected light fixtures within 10 seconds, before even the IOS forwarding starts up. In this release, the fast PoE feature is only available for PoE. This release does not support the fast UPoE feature.

**Cisco Catalyst 4500-E:**

- Universal Power over Ethernet (UPoE) switch.
- Provides up to 60W per port.
- 1 + 1 supervisor engine redundancy (4507R+E and 4510R+E).
- 1 + 1 power supply redundancy.
- In-Service Software Upgrade (ISSU) ensures continuous packet forwarding during supervisor engine switchover to help ensure high availability and uninterrupted power to light fixtures.

**Cabling Considerations**

- CAT5E / CAT6 / CAT6A (AWG 23 - AWG 22)—A larger wire gauge allows more efficient power distribution which drives the 23 to an AWG recommendation.
- U/UTP CAT6, CAT5e cables (or better)—Can be used for connecting UPoE switch uplink ports to the wiring closet access switches with a maximum length of 100m (according to IEEE 802.3).

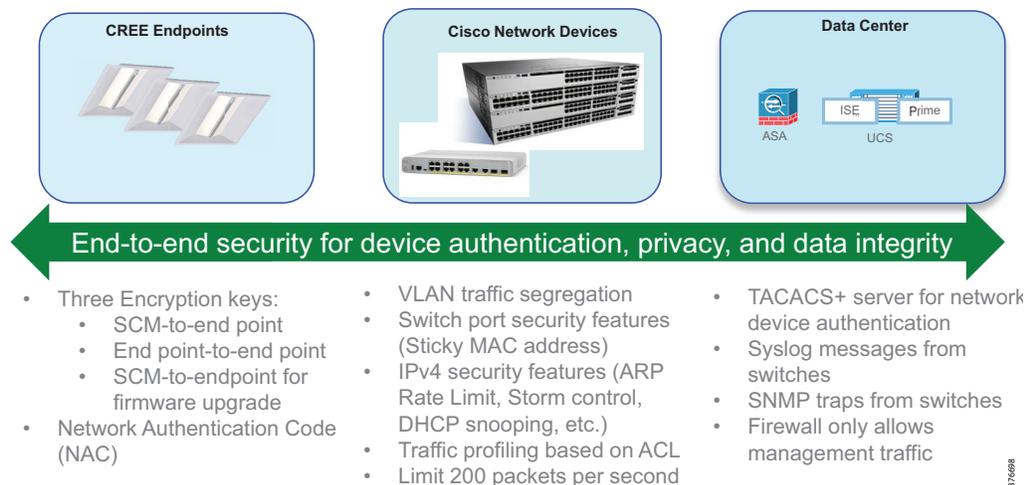
**Table 3-1 Lighting Fixture Power Requirement and Cable Length**

Light Fixture	Power Consumption	Maximum Cable Length from Light Fixture to POE Switch
CR22	32 W	100 meters
KR6	28 W	100 meters
Wall Dimmer	1.5 W	100 meters

**Security**

The end-to-end security is broken down into three major parts, as shown in [Figure 3-9](#):

- Endpoints security
- Network Infrastructure security
- Data Center security

**Figure 3-9 Cisco Digital Building Cree Solution End-to-End Security**

376698

## Endpoint Security

### Cree Endpoints

Cree's SmartCast lighting system implements encrypted communications between the SCM and the endpoints (light fixtures and wall dimmers). The system uses the Elliptic-Curve Diffie-Hellman (ECDH) key exchange algorithm to establish a secure communication channel, which is then used to exchange symmetric keys for subsequent communications.

Three types of symmetric keys are used, depending on the type of communication:

- SCM to Endpoint (operating mode)
- SCM to Endpoint (firmware update mode)
- Endpoint to Endpoint

On startup, the SCM checks the endpoint keys, and issues new keys to the endpoints if necessary. Endpoints store their keys in volatile or non-volatile (persistent) memory, depending upon the type of key.

### SmartCast Manager Application Security

It is strongly recommended that the SCM is deployed on a machine that is compliant to the IT policy of the customer, which should include the update policy of the standard (OS) components.

The SCM uses UDP ports 55004 and 55007 for inbound and outbound communication with lights. It also uses the SNMP protocol to discover the directly-attached switches. The IT policy should allow these ports for proper communication. It is recommended to remove SCM from the network after commissioning the lights fixtures for security concerns. The caveat is customers will lose SCM power saving and monitoring functionality.

The NAC feature provides basic protection when users try to view/modify a lighting network. Light fixtures internally maintain a network status flag, indicating if they belong to a protected network. While responding to SCM's device discovery command, the light fixture will send information about this flag. SCM will save this information about every fixture in its local application cache. When a user tries to access any light fixture, SCM will first check its network status flag value. If it is true, the user will be asked to enter its NAC when accessing the light network. Only after successful verification of NAC will the user be given access to that fixture.

## Network Infrastructure

### Lighting Network VLAN

The light fixtures use broadcast packets to advertise themselves on the lighting network. When the light fixture powers up, it will go through a device initialization process. The fixture will broadcast a device initialization packet on the lighting network. With this received packet, the SCM will detect that a new device has entered into the lighting network. The broadcast will hit every endpoint within a single broadcast domain. To protect other devices on the network, it is recommended to create a separate VLAN for the lighting network.

## UPoE Switch Security

The security on the UPoE switch is provided by allowing only SmartCast protocol traffic on the ports connected to the light fixtures, plus restrict only one light fixture per port.

A port-based access control list (ACL) lets the switch automatically allow or block packets, based on traffic policy, between the SCM and light fixtures, plus between light fixtures. The Cree light fixtures communicate with each other over the UDP protocol. It is strongly recommended to create an ACL that only allows UDP traffic for 55004 and 55007 ports.

The port security features restrict input to an interface by limiting and identifying MAC addresses of the fixture that are allowed to access the port. It is recommended to use a sticky MAC address that will allow a particular light fixture MAC address learned on a specific port.

To protect against denial-of-service (DoS) attacks, restrict 200 packets per second on ports connected to light fixtures.

It is also recommended to implement the standard Layer 2 security features on switch ports, such as the following:

- Storm control
- DHCP snooping
- BPDU Guard
- IPSource Guard
- Dynamic ARP Inspection
- ARP rate limiting

## Data Center

The management services reside in the data center on a separate management VLAN that is protected by the firewall, which allows only management traffic from switches to the application servers in the data center. The secure access to the switches is provided via TACACS+ and SSH/HTTPS protocols. The Syslog and SNMP traps are used to monitor and troubleshoot the switches. It will monitor the events, such as light fixture port security violations and port up/down status.

## Power Management

The UPoE switch provides the power to lighting fixtures depend on which type of lighting fixture is connected to the port. [Table 3-1 on page 3-9](#) shows that different lighting fixtures use different watts of power.

The Cisco Catalyst 3850 UPoE switch has two power supplies per system, allowing the power load to be split between them or provide redundant power supply. In addition, the stacking switch supports power stacking, which allows the power supplies to share the load across multiple systems in a stack. By connecting the switches with power stack cables, the user can manage the power supplies of stack members as one large power supply, which provides power to all switches and to the powered devices connected to switch ports.

The following are reasons for connecting individual switches into a power stack:

- If the power supply fails and enough spare power budget exists in the rest of the power stack, the switch can continue to function.
- A defective power supply can be replaced without having to shut down all powered devices in the systems.

The following are two modes for power stacking:

- **Power-Sharing Mode** (the default)—All input power is available to be used for power loads. The total available power in all switches in the power stack is treated as a single large power supply, with power available to all switches and to all powered devices connected to UPoE ports. In this mode, the total available power is used for power budgeting decisions and no power is reserved to accommodate power supply failures. If a power supply fails, powered devices and switches could be shut down (load shedding).
- **Redundant Mode**—The power from the largest power supply in the system is subtracted from the power budget, which reduces the total available power, but provides backup power in case of a power-supply failure. Although less available power exists in the pool for switches and powered devices to draw from, the possibility of having to shut down switches or powered devices in case of a power failure or extreme power load is reduced.

The Cisco Digital Building Cree Solution can be deployed with different types of light fixtures that require different power consumption as shown in [Table 3-1 on page 3-9](#). A light fixture uses a maximum power of 40 watts. It is recommended to configure 24 ports switch with 1100/715 pair power supplies and 48 ports switch with the 1100/1100 pairs power supplies. The switch allocates 880 watts of power out of 1100 watts to the UPoE/PoE light fixtures.

Select the mode based on the power available; for example, configure 48 port standalone switch in redundant mode when total power consumption of all light fixtures is less than 880 watts. Similarly, configure a unit of stacks in redundant mode when the total power available is more than the power required by light fixtures. For example, if four units exist in a stack and each unit has dual 1100 watts of power, the total number power supplies will be eight, out of which one power supply is reserved for redundant mode. The remaining seven power supplies will provide a total of 6160 watts of power (880 per power supply time X seven power supplies). The reserve power supply will provide enough power when a single power supplies fail.

If the power consumption of all light fixtures is more than the allocated power budget, then configure power stacking in the power-sharing mode. In this case, the switch also needs to be configured with power priority, to allocate power to the lighting fixtures during the failover scenario. The high and low priority on the port determines the order in which devices are shut down, in case of a power lost and load shedding. Configure different priority values, which will limit the number of lighting fixtures shut down at one time during a loss of power. For example, if multiple light fixtures exist in a room and configure few light fixtures with high priority to avoid the darkness in a room; similarly provide the high priority to the light fixtures installed at critical places.

Even if one power supply is reserved on redundant mode, configuring port priority to that will provide dual power failure protection. After one power supply failure, the redundant mode automatically changes itself to power-sharing mode, since no additional reserve power exists for another failure. In this case, having the port priority will provide power to high priority light fixtures.

## High Availability

It is recommended to deploy the infrastructure in a redundant mode and follow the Campus Network best practices to minimize the service outage as much as possible even during the upgrade and migration process.

Typically, the network components at the access layer are considered non-critical assets. These assets, such as general lighting equipment and UPoE switches, do not require UPS backup.

When deploying the light fixtures and UPoE switches, an option is to connect the lights in an area to two UPoE switches to minimize the outage or different units on stack switches. If one UPoE switch fails, half of the lights in one area can keep up, so the area won't become completely dark. This option may increase cabling complexity in the deployment, and potentially, increase the cable length and cost.

Emergency lighting equipment, such as exit signs and emergency light fixtures, is required to always be available, and is not in scope of this phase of architect design.

The Cisco Catalyst 3850 UPoE switches have dual power supply for redundancy and also support the power stacking. This is where the number of power supplies from different switches in a stack act as one large power supply, which provides power to all switches and to the powered devices connected to switch ports. Additionally, a Cisco Catalyst 3850 UPoE switch provides high availability through enhanced PoE features such as Perpetual PoE and Fast PoE.

The Cisco Catalyst 4500-E UPoE switch provides several features to minimize planned and unplanned outages. It has two power supply bays that support two of the same supplies in a redundant mode or in a combined power-sharing mode. The In-Service Software Upgrade (ISSU) provides the means to upgrade or, if needed, downgrade the Cisco IOS Software in a redundant Cisco Catalyst 4500 E-Series system, without incurring a service outage.