Overview of Cisco Catalyst Digital Building Solution – Deployment, Switch Management, and Security

1. What you will learn

This white paper will provide an overview of various deployment models for different aspects of a digital building. It will also provide an overview of various management options, such as the Cisco® DNA Center, Cisco Configuration Professional for Catalyst (CCPC), and the ‘Digital Building – Installer’ mobile app. The paper will also talk about the security aspects of Cisco Catalyst® Digital Building Series switches and Cisco Catalyst 9300 Series switches and how they can help digitize buildings securely.

2. Prerequisites

Basic networking concepts.
3. Introduction

Buildings, be it offices, hotels, hospitals, schools, or retail stores, are at the verge of a revolutionary transformation as technology pushes for convergence of subsystems such as lighting, HVAC, security, and audio-video systems. Enterprise building managers constantly seek greater control in management, monitoring and security.

While the rest of the industry dabbles with this problem of convergence, the Cisco Digital Building Solution offers the complete backbone for supporting the digital building ecosystem. This solution is driven by Cisco Catalyst Digital Building Series switches, which not only efficiently powers building systems, but also greatly simplifies the deployment, management, and control of these subsystems. This low-voltage switch can power devices up to 60W on every port, covering a host of applications ranging from charging electronic devices to lighting and surveillance. We will look at lighting as one of its use cases throughout this paper.

4. Key Business Drivers for Digital Buildings

4.1. Security

Security in buildings is an ever-growing concern and requiem. Both facets of physical and network security are immutable drivers for business growth. A host of PoE-enabled solutions address physical security aspects such as access control and surveillance. Network security threats by hackers or malicious sources need a robust horizontal architecture solution for enabling IoT components in enterprises.

Figure 4.1. Current vertical BMS structure VS horizontal approach for BMS

The new intuitive network can provide identity-based segmentation with device profiling, built-in visibility and granular policy control and dynamic endpoint management.
4.2. Experience
Tenants constantly seek more personalization and better experiences in their work environment. Some ways in which this can be achieved through different PoE use-cases are as follows:
- Scene management in lighting systems to preset ambient lighting conditions
- End-user temperature control through a PoE-based HVAC system
- Wayfinding services in buildings for ease in finding specific rooms/locations
- Smart seat-allocation and meeting room nameplates for hot-seat and agile workspaces
- Automated elevators and biometric door locks for easier tenant access

4.3. Asset and energy utilization
With the increasing demand of real estate in urban city centers, enterprises need to find new and innovative ways to ensure that buildings are efficiently utilized, and also monitor energy usage of end-points.

4.4. Building codes
In many locations across the world, building regulatory codes are progressively becoming stricter, calling for higher efficiencies and safety standards. This is another driver that is in favor of PoE-based solutions as they are inherently designed for the future connectivity needs.

4.5. Cost
Cost overruns are one of the biggest risks in constructing and managing buildings – building managers constantly seek to reduce costs through various methods – some such enablers are convergence of different subsystems, cable consolidation, reduction of high voltage labor categories etc. A PoE-based system touches upon all of the aforesaid parameters.

5. Key value propositions – Catalyst Digital Building Series switches

5.1. Simplicity
Cisco Catalyst Digital Building Series switches was designed for a variety of target applications, so it comes packaged with simplicity in installation and overall architecture, which are essentially key pillars for a scalable solution.

5.1.1. Installation simplicity
For a smart building foundation, we’ve made it really easy for customers to adopt our system. Solutions like the Network Plug and Play can help with the deployment of 100s of devices with ease. The ‘Digital Building – Installer’ mobile app ensures that Operational Technology (OT) personnel can install Catalyst Digital Building Series switches with ease. However, beyond that, Catalyst Digital Building Series switches have been built to have flexibility with mounting and powering of the switches. More info on mounting and powering options can be found in Catalyst Digital Building Series Switch Hardware Installation Guide.

5.1.2. Architecture
Historically, Building Management Systems have always functioned as silo’d vertical systems. With the Catalyst 9000 and Digital Building Series switches enabling the IP convergence all the systems within the BMS can interact with each other so that the building Managers can extract maximum value out of their assets.

Cisco Catalyst 9300 Series switches and Cisco Digital Building Series switches supports open standards like COAP (Constrained Object Application Protocol) which enables communication between various endpoints in the building and provides a platform for the future that can be leveraged endpoint management.
5.2. Security
SD-Access Extension - New IoT devices coming on the network poses a security threat and are vulnerable for a network attack. SD-Access Extension can provide Intuitive identity-based segmentation with device profiling, Built-in visibility and granular policy control and dynamic endpoint management.

5.3. Savings
- Higher power efficiency of the LED lights and Catalyst Digital Building Series switches result in significant lower OpEx
- Catalyst 9000 switches can provide next generation capabilities like containers that provides the app hosting capabilities taking computing right to the edge device as opposed to the data center
- The Digital Building ecosystem is growing exponentially and provides the platform for future innovations

6. Use cases
6.1. Building efficiency and collaboration tools
Indoor Enterprise lighting is one of the primary use cases of the Digital Building Solution.
Digital Building solution can provide
- Enhanced client experience and services
- Effective and Efficient facility and resource utilization through automation and analytics
- Flexible infrastructure to take advantage of future technology for better organizational performance through e.g. digital workplace solutions

The whitepaper Alpiq InTec- Making Buildings Smarter with Enterprise IoT talks about it in detail.

6.2. Classroom lighting
Implications of access to daylight can have an effect on the productivity of the students. Cisco Digital Building solution can allow the educators to control the lights in the classrooms to improve student productivity. Check out the Miami Dade Schools Case Study

6.3. Hospitality and retail
Cisco Digital Building solution can provide indoor lighting solutions for the Hospitality and Retail Vertical and enhance the customer experience. Check out how Sinclair Holdings is Establishing Digital Competencies for Tomorrow’s Hospitality Industry

7. Deployment models
The Digital Building solution can be deployed in multiple topologies, based on your requirements and the time duration of the installation.

7.1. Centralized deployment with the Cisco Catalyst 9300 Series switches
Some important considerations for centralized deployments are –
- Longer cable runs: Each Internet of Things (IoT) endpoint will be connected to the network by a cable running from an access layer switch such as WS-C9300-48U switch stack in the Intermediate Distribution Frame (IDF).
- Heat dissipation would be centralized (in the IDF), since the AC-DC conversion happens at the switch
- Higher resiliency (power and data) is possible due to high-availability features (Perpetual UPOE, Fast UPOE, 2-event classification) with the Catalyst 9300 Series switch stack

Figure 7.1 shows a physical network topology for a large-scale lighting network integration with a campus network, where a stack of Cisco Catalyst 9300-48U switches in the wiring closet connect to a campus network aggregation/distribution switch pair of Catalyst 9500 Series switches. In this centralized deployment, the 9300-48U stack can provide IP addressing to light fixtures using Dynamic Host Configuration Protocol (DHCP).

The aggregation switch in the campus network collapsed core/distribution layer connects to a data center. The data center hosts various campus infrastructure servers such as DNA Center, Cisco Identity Services Engine (ISE), Cisco Stealthwatch®, the building management system, etc., enabling services for ease of deployment and security.
7.2. Distributed deployment model with the digital Building Series switches

Some important considerations in distributed deployments are -

- Shorter cable runs that are cheaper: Each IoT endpoint will be connected to the Digital Building Series switch for power and data, and only one cable would run from the IDF to the switch.
- Heat dissipation would be distributed, since the AC-DC conversion would happen at the Digital Building Series switch at various deployment points.
- The Digital Building Series switch ideally sits in the plenum area, powering endpoints in spaces such as audio privacy rooms, conference rooms, team rooms, sections of a floor, etc. However, this architecture can also be implemented with the Digital Building Series switches in the wiring closet, in which case the cable runs will be roughly the same as those in a centralized architecture.

Figure 7.2 shows a physical network topology for a large-scale lighting network deployment in which the Cisco Catalyst Digital Building Series switches are used to provide network connectivity to the endpoints and power them with PoE. In this star topology, the Catalyst 9300 stack or the Digital Building Series switches can provide IP addressing to light fixtures using DHCP. All Digital Building Series switches have an upstream network connectivity to the Catalyst 9300 stack. Each Digital Building Series switch can power up to eight PoE+ or Cisco Universal Power over Ethernet (Cisco UPOE®) endpoints, depending on the switch model deployed (CDB-8P/U). The Catalyst 9300 stack connects to an aggregation switch in the campus network collapsed core/distribution layer, which connects to the data center.
Figure 7.2. Distributed deployment (Star topology) for digital building

Figure 7.3 shows another way to deploy a distributed topology. In this topology, the Digital Building Series switches can be daisy-chained. The first switch has the uplink connectivity to the Catalyst 9300 stack, which in turn has connectivity to a data center. All considerations mentioned earlier for the star topology apply to this topology. In addition, it’s important to understand that there is a 1 Gigabit Ethernet (1G) uplink connection from the first Digital Building Series switch in the daisy chain to the Catalyst 9300 Series-switch stack. As all the traffic from the downstream Digital Building Series switches will go through this 1G link, the number of switches in the daisy chain should be planned carefully so that the link is not oversubscribed. Cisco recommends limiting the number of Digital Building Series switches in the daisy chain to five.
To increase resiliency, lights in the same area (for example, a room) can be connected to different nearby switches, as shown in Figure 7.4 and Figure 7.5. However, note that cable runs will be slightly longer than usual in this approach.
Figure 7.4. Distributed deployment (Star topology with lights distributed on different switches) with digital building
8. Manageability

The Cisco Catalyst Digital Building Series switches can be managed in multiple ways. Table 8.1 summarizes the various methods.

Table 8.1. Digital building switches manageability options

<table>
<thead>
<tr>
<th>Management</th>
<th>Uplink needed</th>
<th>Scope of configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA-C</td>
<td>Yes</td>
<td>Network level</td>
</tr>
<tr>
<td>Cisco Configuration Professional for Catalyst</td>
<td>No</td>
<td>Switch level</td>
</tr>
<tr>
<td>Cisco Digital Building App</td>
<td>No</td>
<td>Switch level</td>
</tr>
<tr>
<td>Cisco Prime™ Infrastructure</td>
<td>Yes</td>
<td>Network level</td>
</tr>
</tbody>
</table>

Let’s dive deeper into some of these management techniques.
8.1. DNA Center – Network Plug and Play

Cisco DNA Center can manage your end-to-end network from the campus, branch, and WAN to the cloud. It runs on Cisco’s Software-Defined Networking (SDN) controller, the Cisco Application Policy Infrastructure Controller–Enterprise Module (APIC-EM).

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new branch or campus rollouts, or for provisioning updates to an existing network. The solution provides a unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless devices with a near zero touch deployment experience.

Cisco Digital Building Series switches run a Plug and Play agent, making them easy to deploy and manage with limited human intervention. The switches support Network Plug and Play right out of the box.

Figure 8.1 shows how the Network Plug and Play functionality can be used to deploy Digital Building Series switches at scale, with ease and without compromising security.

Figure 8.1. DNA-C Network Plug and Play workflow

More information on Network Plug and Play can be found here.

More information on Network Plug and Play specific to the Cisco Digital Building Series switches is given in section 8.2.2.
8.2. Cisco Configuration Professional for Catalyst

Cisco Configuration Professional for Catalyst (CPC) is a web-based graphical user interface that allows one to install, configure, maintain, and troubleshoot Cisco Catalyst switches with ease.

Cisco CPC makes it possible to set up a new factory default Digital Building Series switch without the need for a console cable, as long as a PC is connected to the switch. Critical information such as PoE budget and critical logs and health of the switch can be made visible on a single screen. Troubleshooting connectivity issues and switch health becomes easier, and outputs are also easily readable. Maintenance activities on the switch, such as Cisco IOS® Software upgrades can be performed with just a click of a button.

Cisco CPC has context help that explains in more detail the field and the input required.

System requirements

Table 8.2: Cisco CPC System Requirements lists the system requirements for Cisco CPC.

<table>
<thead>
<tr>
<th>System Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Either of the following:</td>
</tr>
<tr>
<td></td>
<td>Mac OS 10.9.5</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Version 7</td>
</tr>
<tr>
<td>Browser</td>
<td>Cisco CPC can be used with the following browsers:</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 52 and later</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 48 and later</td>
</tr>
<tr>
<td></td>
<td>Apple Safari 9 and later</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11 and later</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>1280 x 800 or higher</td>
</tr>
</tbody>
</table>

8.2.1. Connecting to a Digital Building Series switch through Cisco CPC via bluetooth

Cisco CPC comes preloaded on the Digital Building Series switch. No commands are required to get CPC up and running on these switches. Follow these steps to connect to a Digital Building Series switch via Cisco CPC.

1. Power up the switch.
2. Insert the Bluetooth dongle into the USB slot of the switch.
3. Pair a laptop with the switch via Bluetooth.
4. After a successful pairing, click "Connect to network," so that the laptop you are using gets an IP address from the switch (Figure 8.2).
5. The switch has a default IP address of 172.16.0.1/24 on the Bluetooth interface.
8.2.2. Performing a factory reset on a Digital Building Series switch with Cisco CPC

Cisco Catalyst Digital Building Series switches come preloaded with a default configuration for ease of deployment. The configuration file is located at flash:/dc_profile_dir/day0.cfg.

The default configuration includes:
- Bluetooth interface IP
- Bluetooth DHCP IP pool
- 2-event classification on all ports
- Perpetual UPOE/PoE on all ports
- Fast UPOE/PoE on all ports
- Constrained Application Protocol (CoAP) proxy server
- Bridge Protocol Data Unit (BPDU) guard on all downlinks

The “Factory Reset” option at Configuration → Troubleshooting → Switch Reboot, as shown in Figure 8.3, will restore the switch to the default configuration. Network Plug and Play and Smart Install can work when the switch is in this mode.
The “Connect to controller” option at Configuration → Troubleshooting → Switch reboot will write-erase the switch and remove all configurations it was shipped with. However, the Network Plug and Play agent will still kick in. If the Network Plug and Play process is not interrupted and there is uplink connectivity to the controller (for example, DNA-C), the switch can be deployed using Network Plug and Play.

8.2.3. Monitoring
Cisco CPC shows the health of the switch on a single pane of glass. You can:

• Check port status
• Check power consumption on the ports
• Check critical logs
• Check the temperature of the switch

8.2.4. Configuration
The Configuration tab of Cisco CPC allows the configuration of general switch parameters. Clicking on the port allows you to configure port parameters such as speed, duplex, VLAN associated with the port, and other parameters.

8.2.5. Software upgrade
The software associated with a switch can be upgraded with the simple click of a button. However, the image must be downloaded from Cisco.com before the switch Cisco IOS® and CPC software can be upgraded. To upgrade the switch, browse to the download location on the user PC.

8.2.6. User privilege
Distinct users can be created with varied privilege levels so that write and read access on the Cisco CPC can be restricted.

8.3. Mobile phone app
Ease of management is a critical aspect of Digital Building Series switches. The mobile phone app helps novice network users configure and deploy the switch with ease.

The Digital Building Installer’ mobile app can connect to the switch via Bluetooth. This can help the deployment personnel to deploy the switch easily even when there is no uplink connectivity and make the Day 0 deployment very easy. The deployment personnel don’t have to network savvy and the ‘Digital Building Installer’ phone app can help them through the deployment.

8.3.1. Connecting via bluetooth

• Insert the Bluetooth dongle in the USB slot of the Digital Building Series switch.
• The Android app connects to the switch using classic Bluetooth, and the iPhone app connects to the switch using Bluetooth Low Energy. (Instructions for connecting with an iPhone are given below.)
• Ensure that Bluetooth is enabled on the mobile device being used.
• Open the Cisco Digital Building app (Figure 8.4), and it will list all the switches that have Bluetooth enabled.
• Select the switch you want to manage or deploy (Figure 8.5).
Figure 8.5. Switch discovery

Steps for using the Catalyst Digital Building App on an iPhone are fairly similar. Below is the summary.

- Insert the Bluetooth dongle in the USB slot of the Digital Building Series switch.
- Ensure that Bluetooth is enabled on the mobile device being used.
- Open the Cisco Digital Building app, and it will list all the switches that have Bluetooth enabled.
- Select the switch you want to manage or deploy.
- When you click Connect, the phone will prompt you to enable a personal hotspot. Tap Yes.
- The iPhone will pair with the Digital Building Series switch.
- Go back to the app, and again tap Connect. The app should connect to the switch this time.
- The Cisco Digital Building app will connect to the switch automatically if the credentials are set to the defaults. If the credentials have been modified, it will take you to the login screen.
- On successful connection to the switch, the dashboard is launched, and from here you can use the various features provided by the app.

Figure 8.6. Dashboard

9. Security

As the wave of digitization transforms buildings and enables unsecure endpoints to converge on the IP network, it creates tremendous business value, but also increases the attack surface for hackers, thus exposing enterprises to new risks. In this state, security becomes paramount, and a holistic approach to securing endpoints and enterprises becomes critical.

9.1. Software-Defined Access

Cisco Software-Defined Access (SD-Access), built on the principles of the Cisco Digital Network Architecture (Cisco DNA™), provides a transformational shift in building and managing networks: faster, easier and with improved security. By decoupling network functions from hardware, SD-Access helps ensure security policy consistency across the network.

Many medium-sized to large businesses want to consolidate multiple networks into one management plane while having the ability to segment the network into either lines of business or functional blocks.
Cisco Software-Defined Access provides not only the ability to macro segment the network by defining constructs like Virtual Network but also provide micro segmentation capabilities in the form of Group based end to end policies.

In the past adding and securing devices was done by manually by creating VLANs based on IP addresses and manually dealing with policies, user and device policy violations. This let threats to go unnoticed or threats that entered via encrypted traffic go unseen. Cisco is changing that with Software Defined Access that simplifies segmentation and policy across the network fabric. By creating logical groups of similar "IoT devices" (IOT Virtual Network), the administrator can create a single policy that states “IoT devices do not have access to sensitive company data.” This policy is then applied throughout the network that is part of the fabric - to make sure that malicious activity such as ransomware cannot access critical data thwarting potential risk. As new IoT devices are added they are automatically added to the “IoT devices” group meaning that the manual process of adding these devices in minimized.

As shown in Figure 9.1, Catalyst 9300 Series switches can be deployed as the Fabric Edge Nodes and the Catalyst Digital Building Series switches can be deployed as a SD-Access Extension in the SD-Access architecture. SD-Access Extension will allow a variety of endpoints like the lights, cameras, vending machines, HVAC, IP Phones, desktop machine, laptops, etc. to be connected to the SD-Access Extension and get segmented with the correct security policies.

Figure 9.1. DNA SD-Access extension node architecture

Note:
Fabric edge nodes – A Fabric device (e.g. Access or distribution) that connects Wired endpoints to the SD-Access fabric
SD-Access extension – A switch that connects to the Fabric edge nodes
Virtual Network – Virtual Network maintains a separate routing & switching instance for each VN; For Simplicity - Virtual Network = VN = VRF
IoT devices connected to the CDB SD-Access Extension can be segmented into a VN e.g. IoT as shown in Figure 9.2.
Software-Defined Access provides Network architects and administrators with all the tools to orchestrate key business functions, such as user mobility, secure segmentation, user onboarding, Internet of Things (IoT) integration, guest access, context-based troubleshooting and data center and cloud integration.
9.2. Security with Cisco IOS
Cisco Catalyst Digital Building Series switches run the Cisco IOS® operating system and natively inherit its security features. A safe and secure network infrastructure mandates establishing security as the foundation of the network. As a critical component of the Cisco network, Cisco IOS Software delivers a sophisticated set of security capabilities for a comprehensive, layered security approach throughout the network infrastructure. Cisco IOS security technologies help defend critical business processes against attacks and disruption, protect privacy, and support policy and regulatory compliance controls. Cisco Digital Building Series switches support a comprehensive suite of security features, some of which are listed in Table 9.1.

Table 9.1. Security features of Cisco Catalyst Digital Building Series switches

<table>
<thead>
<tr>
<th>Auto Security</th>
<th>IPv6 Security</th>
<th>Port Based Security</th>
<th>Cisco COAP Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DHCP Snooping</td>
<td>• IPv6 Multicast Listener Discovery (MLD) snooping</td>
<td>• 802.1x</td>
<td>• RawPublicKey supporting asymmetric keys without certificates</td>
</tr>
<tr>
<td>• Dynamic ARP</td>
<td>• IPv6 Device tracking</td>
<td>• MAC address filtering</td>
<td>• Certificate based support for asymmetric keys using x.509 certificate</td>
</tr>
<tr>
<td>inspection</td>
<td></td>
<td>• Access lists (ACLs)</td>
<td></td>
</tr>
<tr>
<td>• Port security</td>
<td></td>
<td>• VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Storm control:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TACACS+, AAA</td>
<td></td>
</tr>
</tbody>
</table>

9.3. Trust Anchor Technologies
Cisco Trust Anchor Technologies provide a highly secure foundation for Cisco products.

**Image signing:** Cryptographically signed images help ensure that the firmware, the BIOS, and other software is authentic and unmodified. As the system boots, the signatures are checked, ensuring the integrity of the system’s software.

**Secure boot:** Secure boot takes image signing to the next level. It gives the network administrator stronger assurance about the integrity of the hardware and software that perform image checks and other critical system functions. It does this by anchoring the boot sequence chain of trust to immutable hardware. It also helps assure that a system’s foundational state and the software to be loaded cannot be modified regardless of a user’s privilege level.

Image signing effectively mitigates persistent attacks. Secure boot makes that protection even more robust. A device with these features offers a network administrator the ability to prevent man-in-the-middle replacements of software and firmware. In addition, Secure Boot provides layered protection against the persistence of illicitly modified firmware.

**Hardware authenticity assurance:** Special hardware is included to uniquely identify the product so that its origin can be traced to Cisco, providing assurance that the product is genuine.

The Trust Anchor module enhances hardware authenticity assurance by using an industry-standard unique identification in a tamper-resistant, strong-cryptographic, single-chip solution.

10. Summary
In summary, the Cisco Digital Building Solution can be deployed in a secure way in various topologies depending on the needs of the customer. Cisco Catalyst Digital Building Series switches come with a range of options designed to provide ease of management. In case of questions regarding the solution, reach out to digitalceiling@cisco.com. For questions on Digital Building Series switches reach out to ask-cdb-pm@cisco.com.