Simplifying Physical Access Control with Cisco UPOE: Unleash the Power of Your Network

Cisco® physical security solutions provide broad networkcentric capabilities in video surveillance, IP cameras, electronic access control, and innovative technology that converges voice, data, video, and physical security in one unified solution. Our connected physical security solution enables customers to use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge their physical security infrastructures operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between other IP-centric systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

What You Will Learn

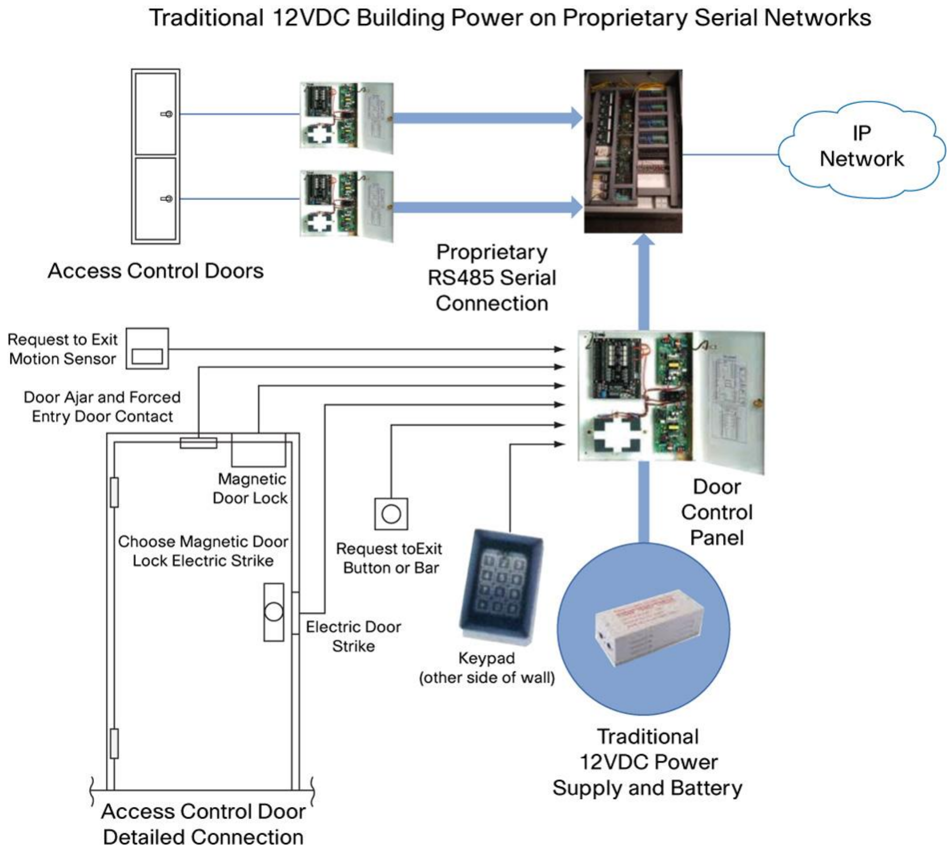
Cisco Universal Power over Ethernet (UPOE) is a technology that extends the IEEE 802.3 PoE standard to provide the capability to source up to 60W of power over standard Ethernet cabling infrastructure. The maximum power sourcing capability as defined by the IEEE 802.3 standard is limited to 30W.

Cisco UPOE is being introduced on the Cisco Catalyst® 4500E Series Switches, the most widely deployed modular access switching platform in the industry. The platform has time and again demonstrated leadership in this space, specifically with PoE+, where the Cisco Catalyst 4500 was the first enterprise-class switch to deliver PoE+ compliant switches, two years prior to the introduction of the IEEE PoE+ standard. With UPOE, Cisco Catalyst 4500E takes inline powering technology to a new level by dramatically increasing the power sourced by the switch to 60W. UPOE helps extend the benefits of power resiliency, power management, and power efficiency to a wider range of devices.

Cisco is also introducing a UPOE splitter device that can work in conjunction with Cisco UPOE-capable Cisco Catalyst 4500 switches to address several use cases that can benefit from inline powering. This splitter has UPOE as the input and provides two output interfaces: an IEEE 802.3-compliant Ethernet PoE port and an auxiliary 12V DC interface. The Cisco UPOE power splitter can provide up to 30W of inline power on the Ethernet port and up to 50W of power over the auxiliary 12V DC interface.

One area that can use the Cisco UPOE technology is traditional building management and security systems. Today these systems have analog CCTV cameras, building management controllers, serial access control door controllers, and traditional door locking equipment. Most of these devices run on 12 VDC and have a centralized collection point that connects to the IP network. Figure 1 shows a traditional physical access control system with door locking hardware.

Figure 1. Traditional Access Control System


Traditional 12VDC Building Power on Proprietary Serial Networks
IP Network
Access Control Doors
Proprietary RS485 Serial Connection
Request to Exit Motion Sensor
Door Ajar and Forced Entry Door Contact
Magnetic Door Lock
Choose Magnetic Door Lock Electric Strike
Request toExit Button or Bar
Electric Door Strike
Keypad (other side of wall)
Door Control Panel
Traditional 12VDC Power Supply and Battery
Access Control Door Detailed Connection

This document focuses on how Cisco UPOE technology can be used to rearchitect building management and physical access control security applications by using network power to deliver unprecedented value in terms of device consolidation and reducing the total cost of ownership (TCO).

Challenge

Traditional building management and security systems are built like silos using proprietary networks and communications protocols. Traditionally these systems don’t talk to one another or integrate well with each other. Businesses are demanding integration and operational efficiencies. Integration means having the HR system, IT network access system, building management, and security system work over the corporate network. Delivering this experience requires building managers, security managers and IT to give careful consideration to the network design. In addition to providing integration, companies need to account for emergency backup power and maintenance of the network.

Business Benefits

Shifting physical access control from analog proprietary serial communications to IP provides five main benefits:

- Protecting access control data
- Responding to alarms more quickly
- Helping business keep going if the network goes down
- Simplifying operations

- Reducing total cost of ownership (TCO) with network power

Reason 1: Protect Access Control Data

Analog physical access control systems make it relatively easy for someone with a little knowledge and widely available tools to create a working card to impersonate an employee. Most card data is not encrypted, either over the air or from the reader to door-control panels. Someone who taps the link can read badge data. A related issue is that most analog door controllers use the Wiegand protocol, which is one way only from reader to door-control panel. That means the card reader can’t tell whether it’s connecting to a legitimate door-control panel or a snooping device.

IP physical access control systems use digital encryption technologies to help protect identity information, making physical access control systems less vulnerable to attacks. For example, new IP-based controllers support a challenge-response function, a highly secure way to protect card data sent over the link. When you present your card for access, the card does not immediately turn over its data. Instead, it first authenticates to the system by sending a public key and listening for a signed response from system. The system signs the credential and sends it back to the card. Only after receiving verification that the system at the other end of the connection is legitimate, not an imposter, does the card transmit its encrypted data to the reader.

New standards in access control interoperability will increase security and interoperability while driving down system costs. One is the U.S. Federal Information Processing Standards (FIPS) 201 for personal identity verification (PIV). FIPS 201 defines a back-end public key infrastructure (PKI) system to manage public keys and user identities through a certificate authority. Other standards include Physical Security Interoperability Alliance (PSIA) and the Open Network Video Interface Forum (ONVIF). Physical Access Control companies, in turn, are moving toward adopting an encryption standard to protect data traveling over the wireless and wired interface.

Reason 2: Quickly Respond to Alarms by Integrating with Video Surveillance and Incident Response Systems

Traditionally, a security officer who receives a forced-door alarm on door 47 has to turn to another console to view video feed, look up which camera monitored that door, and then spend valuable time finding the relevant alarm video. Meanwhile, an intruder could cause harm or flee the property.

The process is more efficient when the physical access control and video surveillance systems are tied together. Integrating physical security systems is far simpler than analog systems, because all servers and endpoints connect to the same network.

For example, suppose someone kicks in an exterior door. An IP-based access control system can transmit the forced-door alarm to the IP-based incident response system. Receipt of the alarm invokes predefined policies, such as sending an alert to a security officer’s preferred device - say, a handheld device - along with real-time video or video associated with the alarm. This saves valuable minutes compared to the security officer weeding through alarm screens searching for the right video cameras. In addition, instead of being tethered to the desk, security officers can receive alerts on mobile devices while patrolling the property, helping to prevent crime or fear of crime.

The benefits multiply if you add an IP dispatch system. Multiple agencies or teams - physical safety, local police, human resources, and others - can join a virtual talk group on any device, including desk phone, mobile phone, or any type of radio.

Another use case illustrating the value of integration comes from a school district in Texas. Video surveillance cameras now do double duty after hours as motion detectors. If motion is sensed after 5 p.m., the motion alert triggers the access control system to notify appropriate personnel on their laptops, phones, or smartphones. The notification includes real-time video or alarm video so that the person can determine whether to investigate, contact police, or conclude that the alarm was caused by a cat, for example.

The same school district also uses the IP-based physical access control system to automatically lock classroom doors one minute after bell rings. The result: 25 percent fewer tardies.

Reason 3: Help Business Keep Going If Network Goes Down

When physical access control is essential to business continuance, the traditional physical access control system might be the weak link: if the proprietary network goes down, so does the ability to let authorized people in and keep others out. Business continuance is especially urgent for governments and critical infrastructure organizations such as energy plants.

IP physical access controls give you options to increase availability. For example, instead of placing the intelligence in a central server that connects to all of your doors over the WAN, you can place intelligence at the network edge. This helps the business keep going even if the WAN goes down because of hurricane, tsunami, power outage, or another disaster.

For even higher availability, implement redundant physical access control management servers, either one of which can take over from the other. The servers share a common IP address and are continuously synchronized. This practice is much cleaner than implementing tiered databases - for example, at the local, regional, and national levels.

Reason 4: Simplify Operations by Integrating with IT or HR Database

Many organizations separately maintain databases for network access, HR records, and physical access control. The drawbacks are data duplication and redundant processes. Separately maintaining the database used for employee access control can also create unsafe situations if terminated employees or vendors with limited-time access are not promptly removed from the system.

With an IP-based physical access control system, changes made to your central Microsoft Active Directory or SQL databases can be automatically propagated to the access control system.

Here, too, IP gives you choices. One option is to implement one-way Enterprise Data Integration communication between the central database and Cisco physical access manager which allows both databases to be synchronized on a periodic basis. The other is using a web services API which allows dynamic integration into the physical access control system. A public university in the Southern United States uses a web services API to allow building administrators to set their own lock schedules on a webpage. The API is also useful for organizations that give out large numbers of one-day visitor badges.

Reason 5: Reduce Total Cost of Ownership (TCO) with network power

Traditional physical access control systems require bringing power, both primary and backup, to each door reader and lock. With UPOE this can be replaced by using IP gateway readers, door locks, and readers that are all connected and powered over a standard Cat5e/Cat 6 cable. This can reduce installation costs by up to several hundred dollars per door.

A single unified physical infrastructure and managed cabling system can also increase availability, negating the requirement to provide both primary and backup power to these end devices. The backup power can be consolidated (commercially available uninterruptible power supplies) and moved into the wiring closet or data center to power the UPOE capable switches. This consolidated backup power supply eliminates the need to install batteries by each door.

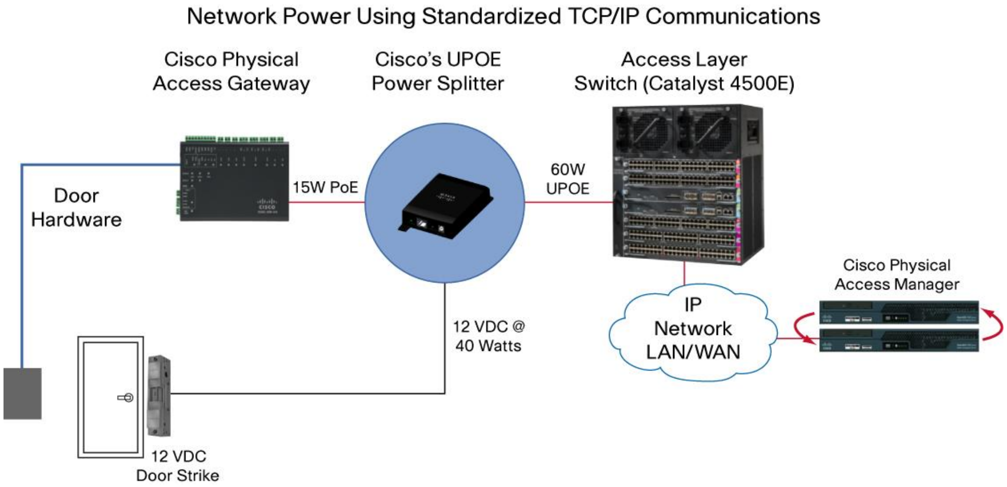
Cisco UPOE Redefining Physical Access Control Solution

New buildings as well as upgrades for traditional access control solutions can use the Cisco Catalyst 4500 Series Switches delivering Cisco UPOE to power the Cisco Physical Access Gateway devices, badge readers, and physical door strikes that are responsible for locking/unlocking the doors. The Cisco Catalyst 4500 has a bulletproof architecture in terms of data/power resiliency and high availability. In addition to the power resiliency offered by UPOE, the platform offers full system-level redundancy and software enhancements such as Nonstop Forwarding (NSF) with Stateful Switchover (SSO) to make sure that a single hardware-level failure does not cause downtime to the network. Furthermore, the platform also supports a true In-Service Software Upgrade (ISSU) feature to enable change management without incurring any network downtime.

The overall Cisco Physical Access Control solution has four components: the Cisco Physical Access Gateway, Cisco UPOE splitter, Cisco Catalyst 4500E switch, and Cisco Physical Access Manager.

Figure 2 shows the physical access control architecture in detail. The Cisco Physical Access Gateway and the Cisco UPOE splitter mount above the doors or are placed in IT closets near the door. A standard copper Ethernet cable connects and powers the Cisco Physical Access Gateway and the Cisco UPOE splitter. The gateway can power the downstream badge reader. Similarly, the 12V DC auxiliary output powers the door strike. A standard Cat5e/6 copper Ethernet cable is yet again used to the UPOE splitter with the Cisco Catalyst 4500E switch, which connects to the Cisco Physical Access Manager over a standard IP network.

Figure 2. Cisco UPOE Solution with Cisco Physical Access Control Products


Network Power Using Standardized TCP/IP Communications
Cisco Physical Access Gateway
Cisco's UPOE Power Splitter
Access Layer Switch (Catalyst 4500E)
Door Hardware
15W PoE
60W UPOE
Cisco Physical Access Manager
IP Network LAN/WAN
12 VDC @ 40 Watts
12 VDC Door Strike

UPOE benefits

- Scalable Modular Architecture, easily integrated with corporate network
- Emergency power from UPS not unchecked batteries at the door
- Less expensive and simplified Cat 5/6 cable runs to the door
- Convenient splitter can be installed when 803.3 af (15W) won't power the door
- Splitter can power most door strikes/magnetic locks

In summary, here are the primary advantages of using Cisco Physical Access Control with Cisco UPOE:

- Power all the access control end devices over standard Cat 5e/6 cable and provide resilient power, eliminating the need for backup batteries near the door
- Upgrade legacy access control system to IP-based systems using network UPOE power
- Achieve operational efficiencies through database integration
- Integrate the HR database, IT database, and security database into a single point of entry

Ordering Information

Cisco UPOE is being introduced on the Cisco Catalyst 4500E, the most widely deployed modular access platform. Cisco UPOE is supported on Supervisor Engine 7-E (or later) based Cisco Catalyst 4500E switches with UPOE-capable line cards. The UPOE splitter WS-UPOE-12VPSPL works with UPOE-capable Cisco Catalyst 4500E switches.

Table 1 shows UPOE compatibility on the Cisco Catalyst 4500E platform.

Table 1. Cisco UPOE Network Switches

Chassis	Supervisor	Line Card	Power Supply
WS-C4503-E **WS-C4506-E** **WS-C4507R+E** **WS-C4510R+E**	WS-X45-SUP7-E	WS-X4748-UPOE+E	PWR-C45-1300ACV PWR-C45-2800ACV PWR-C45-4200ACV PWR-C45-6000ACV

Table 2 shows part numbers for the Cisco physical access manager and Cisco physical access control hardware that can be used in conjunction with Cisco UPOE.

Table 2. Cisco Physical Access Control

Physical Access Manager Hardware	Physical Access Manager Software	Physical Control Hardware	Door Strikes, Card Readers, Request to Exit Sensors
CPS-MSP-1RU-K9 **CIVS-HDD-1000** **CIVS-CAB-16-xx**	CIAC-PAME-M1X-K9 CIAC-PAME-BD= CIAC-PAME-HA= CIAC-PAME-M64= CIAC-PAME-M128= CIAC-PAME-M512= CIAC-PAME-M1024= CIAC-PAME-EDI= CIAC-PAME-WSAPI=	CIAC-GW-K9 CIAC-GW-RDR CIAC-GW-IP10 CIAC-GW-OP8	Parts depend on door and access control card and reader technology. Consult a Cisco Physical Access Control ATP partner.

For more information about Cisco Catalyst 4500E switches and Cisco Physical Access Control, refer to the following URL.

For more information, visit:

- UPOE White Paper
  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_white_papers_list.html
- Cisco Catalyst 4500E Datasheet
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_data_sheets_list.html
- Cisco Physical Access Manager
  http://www.cisco.com/en/US/products/ps9688/index.html
- Cisco Physical Access Control Gateway
  http://www.cisco.com/en/US/products/ps9687/index.html
- Cisco Physical Security
  http://www.cisco.com/en/US/products/ps6712/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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