Network Architecture and IT Guidance Technical Guide

LumaWatt Pro

This document is intended for Lighting Control Systems and IT professionals

Important: Engage appropriate network security professionals to ensure all lighting control system hardware and servers are secure for access.

Network security is an important issue. Typically, the IT organization must approve configurations that expose networks to the Internet. Be sure to fully read and understand customer IT Compliance documentation.

Powering Business Worldwide

Table of contents

Network and IT Considerations

LumaWatt Pro Network Topology Options

The feature that most differentiates LumaWatt Pro Lighting Control from other wireless, networked building management solutions is the autonomy of LumaWatt Pro Smart Sensors. Each LumaWatt Pro Sensor is a full-fledged computing and communications device that controls light levels locally. With the bulk of control instructions transmitted over a wired connection to the control unit and ballast, traffic on the LumaWatt Pro wireless network is kept to a minimum.

Wireless networking is used mainly for data gathering and transport of energy, environmental and occupancy data to the central LumaWatt Pro Energy Manager™ appliance. This appliance provides an interface to the sensor network, simplifying configuration and management of lighting behavior, as well as data monitoring and reporting.

LumaWatt Pro Smart Sensors communicate to the LumaWatt Pro Energy Manager through the LumaWatt Pro Gateway using the IEEE 802.15.4 wireless communication protocol that includes AES encryption to ensure secure links.

The LumaWatt Pro Energy Manager is (typically) mounted in a wiring or electrical closet and can be on the IT network or a stand-alone network. The LumaWatt Pro Energy Manager's intuitive graphical user interface can be accessed via a standard secured browser connection. The figure below shows an example of an LumaWatt Pro Energy Manager installation in an office environment.

The section below explains the Dedicated and Network installation methods.

LumaWatt Pro Enterprise Network

- The wireless gateway and Energy Manager connects to the building IT network via PoE switch or power injector and must have access to the building DHCP server.
- At the discretion of the building IT personnel the LumaWatt Pro system may be setup on a separate lighting network or VLAN.
- Smart devices and computers should be able to connect to the building Wi-Fi network and have access to the Energy Manager on the building IT network or VLAN.
- Connecting the LumaWatt Pro system to the building IT enables certain features such as BACnet® integration or future smart building integration features.

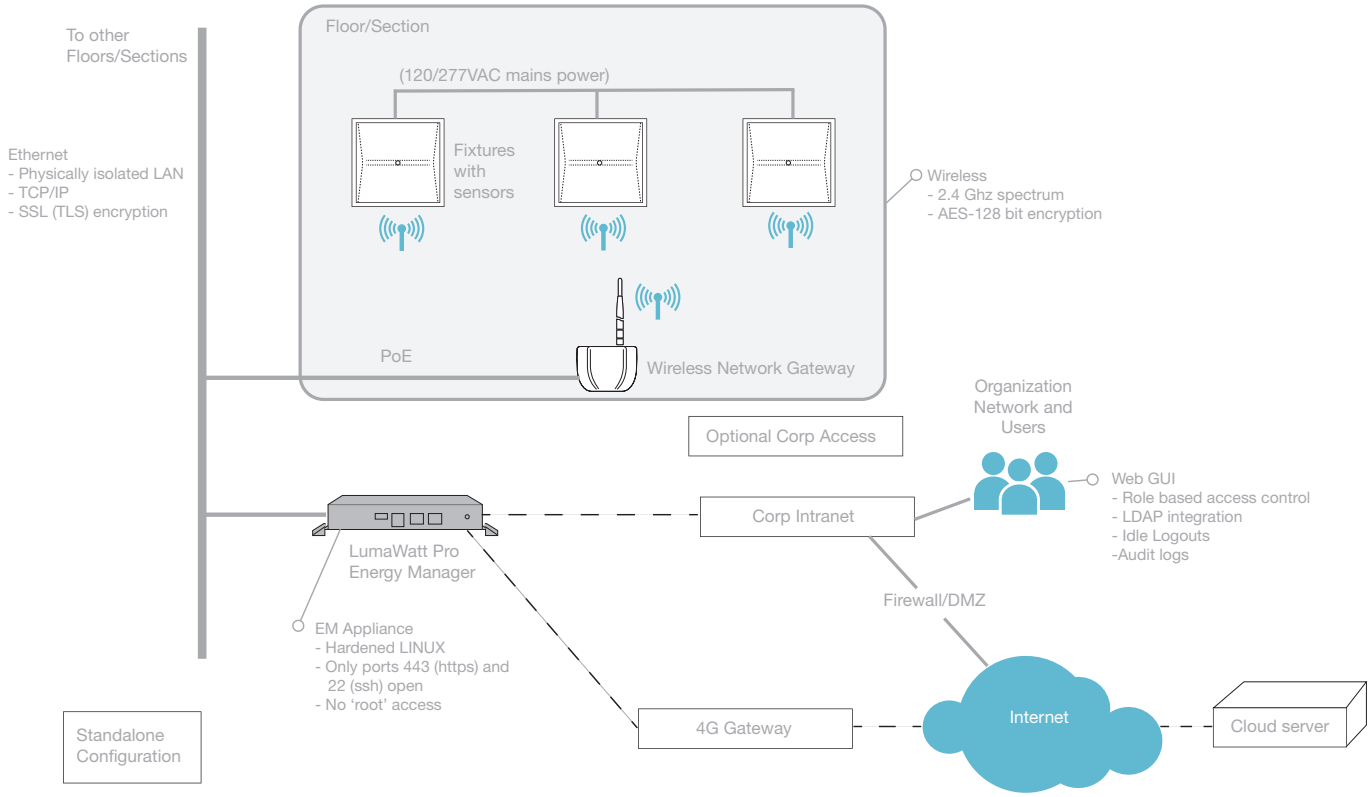
LumaWatt Pro Device IP Address Assignment (DHCP or Manual)

Table 2: IP Address Assignments

Device	Dynamic Addressing	Static Addressing	Notes
Energy Manager	Supported	Supported (default) 192.168.100.1 (default)	• Web interface to monitor, manager and analyze energy savings and data. • Manages up to 1,500 sensors and up to 3,500 BACnet points.
Midrange Energy Manager	Supported	Supported (default) 192.168.100.1 (default)	• Web interface to monitor, manager and analyze energy savings and data. • Manages up to 5,000 sensors and up to 7,000 BACnet points.
Enterprise Energy Manager	Supported	Supported (default) 192.168.100.1 (default)	• Web interface to monitor, manager and analyze energy savings and data. • Manages up to 10,000 sensors and up to 18,000 BACnet points.
Wireless Gateway	Supported	Not Supported	• DHCP address provided by IP network • The Wireless Gateway separates the IT and OT networks • The Wireless Gateway communicates data from sensors to the Energy Manager

System Overview

The LumaWatt Pro Wireless Network is based on the IEEE 802.15.4 standard and operates in the 2.4 GHz ISM spectrum. The chief concern with deploying IEEE 802.15.4 networks is the potential impact on existing Wi-Fi deployments. Both Wi-Fi (802.11) and IEEE 802.15.4 have the IEEE 802 family of wireless standards in common and share the same radio spectrum. For an 802 standard to be approved, a Co-existence Assurance document must be approved which ensures that the proposed standard will coexist with existing 802 standards when operating at the same time. Figure 1 shows more details about the LumaWatt Pro Wireless Network setup.



Product Overview

- Wireless (Gateway)

  IEEE 802.11

  IEEE 802.15.4
- Energy Manager (Midrange Energy Manager, Enterprise Energy Manager)

  IEEE 802.3
- Wireless Wallstation (Manual lighting and scene control)

  IEEE 802.15.4
- Two-Wire Fixture-Mount Sensor (Fixture integrated occupancy sensor, ambient light sensor and control)

  IEEE 802.15.4
- Compact Flush-Mount Sensor (Tile-mount occupancy sensor, ambient light sensor and control)

  IEEE 802.15.4
- Two-Wire Compact Sensor (Tile-mount occupancy sensor, ambient light sensor and control)

  IEEE 802.15.4
- Smart Sensor (Ceiling mount occupancy sensor, ambient light sensor and control)

  IEEE 802.15.4
- Ruggedized Sensor (Outdoor or Industrial application occupancy sensor, ambient light sensor and control)

  IEEE 802.15.4
- Wireless Plug Load Controller (Relay plug load control)

  IEEE 802.15.4

System backbone IT information

Network Ports and Usage

To ensure proper system operation the network ports and protocols listed below must be available to the LumaWatt Pro System and the building IT infrastructure.

Protocol	Port	LumaWatt Pro Device	Usage	Description	Security
TCP	80	Energy Manager	Redirects to Configuration Webpages	Always Open	TLS 1.2
TCP	443	Energy Manager	Configuration Webpages	Always Open	TLS 1.2
TCP	52725	Energy Manager	SSL secured CAPI web services	Always Open	

Network LAN and WAN

LumaWatt Pro was designed so only Gateways and Energy Manager devices with the interface directly with the LAN or WAN within the building. All LumaWatt Pro devices must communicate to the Gateway to maintain proper network separation and security.

VLAN

Multiple LumaWatt Pro Gateways can be installed on a VLAN within the building IT network using Layer 2 or Layer 3 network switches. When implementing a VLAN you must ensure the mobile devices used to configure and manage the LumaWatt Pro system also have access to that VLAN.

VLAN's are not required for the LumaWatt Pro system to work, however they can be implemented on sites that have the IT support and require separation of networks for additional security..

Wireless Network Overview

LumaWatt Pro uses a low duty cycle, narrow-band, IEEE 802.15.4 Zigbee® HA1.2-based 2.4 GHz wireless protocol that is not known to interfere with 2.4 GHz Wi-Fi or other systems. Each LumaWatt Pro Gateway and associated mesh network (typically up to 150 wireless devices) can also be configured via internal web pages to use a specific IEEE 802.15.4 channel to avoid co-channel interference with other installed 2.4 GHz equipment. IEEE 802.15.4 channels 11-26, corresponding with 5 MHz-wide frequency bands from 2.405 GHz to 2.480 GHz may be assigned to specific wireless mesh networks. The wireless communication is secured and encrypted using AES 128-bit encryption.

Other Notes:

Radio:	2.4GHz
Standard:	IEEE 802.15.4
Transmitter Power:	+7dBm
Range	50m (150ft) LOS
# of Walls	2 interior walls standard construction

The wireless mesh network does not support integration with non-LumaWatt Pro wireless devices.

Coexisting with Wi-Fi

The LumaWatt Pro wireless network employs three techniques to either eliminate or drastically reduce its impact on Wi-Fi networks in the building:

- Channel Selection: This technique involves identifying LumaWatt Pro wireless network IEEE 802.15.4 communication channels that do not overlap with the current Wi-Fi deployment.
- Low Airtime Consumption: LumaWatt Pro is designed to reduce wireless communications during steady state operation, greatly reducing the probability of collision with Wi-Fi traffic.
- Interference Tolerance: LumaWatt Pro is designed to work reliably despite encountering some interference, by detecting if communications packets are lost and retransmitting if needed.

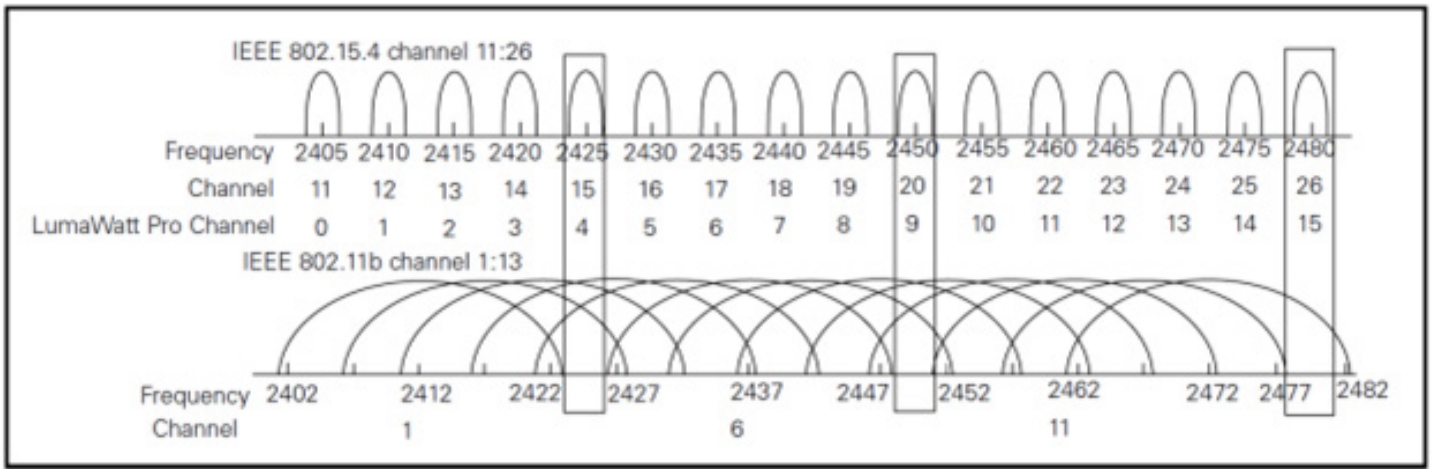
Channel Selection

LumaWatt Pro uses IEEE 802.15.4 channels, which are within the same 2.4 GHz frequency channel that IEEE 802.11 Wi-Fi operates within. Since devices communicating on the same channel can cause interference, the devices need to be set on channels that do not overlap.

If we overlay the most frequently used channels used by IEEE 802.15.4 (LumaWatt Pro) and IEEE 802.11 (Wi-Fi) on the chart below, you can see there is no overlap.

Wi-Fi uses channels 1, 6 and 11 by default, and IEEE 802.15.4 devices should be set to use channels 15, 20, 25 and 26 by default which fall within the gaps of the Wi-Fi channels. For IEEE 802.15.4 channels 15 and 20 are typical and allow us to prevent overlap that can lead to potential signal interference.

Ultimately this means that IEEE 802.11 Wi-Fi and IEEE 802.15.4 wireless devices can co-exist in the same space without interference if they are properly set with the correct channels.



Low Airtime Consumption

LumaWatt Pro recognizes that it is not always possible to select non-overlapping channels. Many Wi-Fi access points aggressively use all available spectrum to maximize performance. To coexist with such solutions, LumaWatt Pro is designed to send two messages every five minutes per sensor. The following example shows the airtime consumption for a 50,000 square foot installation.

- Airtime Consumption = # sensors*msgs_per_sensor*airtime_per_msg/5mins*100%
- 50,000 square feet = 500 sensors
- 1.5 ms of airtime per message
- Airtime Consumption = 500 * 2 * 1.5ms/5mins * 100%
- Typical Airtime Consumption = 0.5%

With such low airtime consumption, the LumaWatt Pro system will easily coexist with Wi-Fi networks whether or not non-overlapping channels are used.

Interference Tolerance

In addition to ensuring that there is no impact on Wi-Fi installations, the LumaWatt Pro wireless network must be tolerant of interference by other Wi-Fi and IEEE 802.15.4 networks. The selection of non-overlapping channels serves to avoid the potential problem. In addition, LumaWatt Pro is designed to be loss tolerant. The LumaWatt Pro communications increase transmission reliability through the use of acknowledgments and packet retransmission. As a result, when a packet is lost, the loss is detected and corrected through retransmission. Additionally, LumaWatt Pro is designed to perform lighting control without requiring network communication at all. Lighting control will continue to operate in the event of a complete wireless failure.

Potential causes for signal disruption

As stated above LumaWatt Pro should be able to co-exist in the building with Wi-Fi installations, however there are many causes of interference and degradation that go beyond the scope of this document. Some basic things that can be addressed during the design phase that may aid in preventing issues include.

1. Review the network range and the distance between the devices. It is just a fact of how signals work that the further the distance between devices, the lower the signal strength. Both IEEE 802.15.4 wireless and IEEE 802.11 Wi-Fi have a maximum unobstructed "line of site" range of 100 meters. However, we also need to factor in obstacles which are prevalent in our indoor spaces.
   a. Of special consideration are the quantity and materials of walls and other obstacles that are between transmitting and receiving devices. Wireless signals can have trouble communicating through these solid objects reducing the wireless range.
   b. Transmitter and end device placement planning during the design phase is critical to ensure proper coverage range and proper device functionality. Manufacturers may have specific recommendations for ranges for their devices that are important to pay attention to.
2. Review the location of the transmitters. Placing two transmitters within the same space, even if they are on different frequencies and channels can lead to disruption if they are too close together.
   a. If too close together, they may increase their signal to "shout" over the other transmitters in the space. If both transmitters are shouting, devices cannot hear or respond. Commercially available wireless products often state in their instructions to maintain at least a 5 to 10 foot airgap between other wireless transmitters to prevent this type of interference by proximity.
3. The quantity of devices on the network can also be a factor of signal degradation. Different network types may support different quantities of nodes. In addition, depending on the design, the quantity of devices may slow or degrade the signal. It is important to review recommendations of device limitations described by the wireless system manufacturers and incorporate this into the design.

Administration and Maintenance

Configuration and Management tools

LumaWatt Pro uses internal webpages within each Energy Manager to manage the LumaWatt Pro wireless network. The internal webpages are accessed by connecting to the Energy Manager IP address via your browser and allow for network configuration.

Internal web pages

The Energy Manager Dashboard and internal web pages permit the following configuration and management settings::

- Time synchronization
- User management
  - Administrator - user name and password
  - User – username and password
- Certificate management
- Backup/Restore
- Network management
  - DHCP/Static
  - WLAN access
    - SSID
    - Password
- Firmware update of WAC and all connected devices
- EULA
- Device placement, management, and control

Certificates

LumaWatt Pro uses SSL Certificates by default that are installed with the system and ensure secure communications.

At the building IT departments discretion custom certificates can be created and installed on the LumaWatt Pro wireless network to provide additional security

User management, roles and access

User authentication is required for administration and user access to the LumaWatt Pro wireless network.

Backup and Restore

LumaWatt Pro supports backup and restore process through the Energy Manager in the event of a product failure and it needs to be replaced.

Backups should be done periodically to ensure you have the latest backup. It is recommended that you perform a temporary backup of data prior to doing a firmware update to the system, in the event something should be updated incorrectly. Once the firmware update has completed successfully a permanent backup can be done, and stored per standard building IT processes.

Firmware and Software updates

LumaWatt Pro supports firmware updates to all wireless devices. These updates include a digital signature to ensure they are valid prior to being installed on the wireless devices.

Firmware updates are uploaded to each Energy Manager which manages the distribution and installations to all wireless devices.

Firmware and software updates are typically released on a quarterly basis for normal activities. Major improvements and feature enhancements are scheduled for a yearly release.

If your LumaWatt Pro system is registered with Eaton Lighting Solutions the registered user will get an automatic notification of firmware and software updates. Additional information will be provided through website information.

Remote support

For some configuration and diagnostics purposes our technical services staff may offer remote access services. This may be accomplished in several ways depending on the customer's network configuration and IT requirements. Most often temporary access is provided by the customer's network system administrator and any required 4G modem installation, VPN access, port opening and/or credentials are revoked upon completion of the required support service.

Special service programs could be arranged through the Eaton Service and Support Group.

Eaton's Lighting Division has a dedicated team within the Eaton Service and Support Group.

This support team is required to go through standard ethics, Global Internet security and other courses yearly and are subject to a background check as part of Eaton employment.

Firewalls (packet filtering, stateful inspection, proxy gateways)

These items should be handled as needed by the local building IT department. The implementation of these security features would be the responsibility of the IT network architect and would not interfere with the standard operation of the lighting system as that is occurring on the OT network.

Redundancy and power failure

The LumaWatt Pro wireless network allows for complete system backup capabilities. Redundant PoE power to the LumaWatt Pro Gateways and Energy Manager are the responsibility of the building IT department.

In the event of loss of communications with the LumaWatt Pro wireless network due to communications failure or power failure the LumaWatt Pro devices will continue to maintain their current light level and wallstation control. The LumaWatt Pro system is designed to be able to be compliant with UL924 emergency lighting standards as long as the appropriate devices are included in the system design.

Third party integration

The LumaWatt Pro wireless network can interface with other systems via IP connection to the Energy Manager. Third party communications must be approved and verified by Eaton Lighting Solutions during system design phase.

Currently supported integration

BACnet is currently supported through an IP connection into the Energy Manager.

API's

LumaWatt Pro supports an API for integration however it does not provide the ability to change software programming of the system. API's are used for status and override of current state.

Cloud connectivity

LumaWatt Pro does not require cloud connectivity to support any lighting control functionality. The system was designed to be supported completely on premises.

Cloud connectivity is required to support value added applications and data storage such as the Space application. The lighting control functionality will always be maintained on premises

Security

Eaton views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the LumaWatt Pro wireless network employs current industry best practices to reduce, identify, contain and manage security risks. LumaWatt Pro has been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Eaton Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the implementation of LumaWatt Pro and offers Eaton customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain Eaton product solutions in a secure environment. More information on the Eaton PCCoE can be found at www.eaton.com/cybersecurity

The LumaWatt Pro System uses a multi-tiered approach to addressing industry best practices for security risk management and utilizes guidelines promulgated by the Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) and industry standards organizations to achieve a secure and adaptable lighting control platform.

Physical security

LumaWatt Pro sensors are a hardened environment and thus even if removed from the ceiling, they cannot be broken. The key information stored in a sensor cannot be retrieved by direct inspection of the persistent storage in the sensor or by tracing the execution logic. The LumaWatt Pro Energy Manager is typically installed in a physically secure location, and the LumaWatt Pro communication network is physically isolated from IT networks.

Onsite network security

All wired communication in the LumaWatt Pro system utilizes strong encryption techniques. Communication between the Energy Manager and the Gateway utilize SSL (TLS) encryption. Communication between the Energy Manager and web clients is HTTPS.

Wireless communication security

To prevent intrusion from external networks and being used as an intrusion point, the LumaWatt Pro Wireless Network is isolated from all IT-managed networks. The LumaWatt Pro Energy Manager maintains a strict separation between the wireless network and any external, IT-managed networks. No LumaWatt Pro Wireless Network traffic is ever routed to the IT networks, and no host on the IT network can communicate with sensors on the LumaWatt Pro Wireless network.

In addition to isolation from IT networks, the LumaWatt Pro Wireless Network provides security against tampering through the wireless network itself. All LumaWatt Pro Wireless Network traffic is AES128 encrypted to prevent snooping and tampering. The commissioning process of the wireless network assigns a network key and network ID. The value of both the network key and network ID must be known (as well as the wireless 802.15.4 channel) to be able to communicate with commissioned devices in an LumaWatt Pro wireless network. Thus, it is not possible to take a commissioned sensor from one LumaWatt Pro wireless network where the network ID and key are known and use it in another LumaWatt Pro wireless network where the network ID and key are not known. Additionally, the likelihood of tampering with the LumaWatt Pro Wireless Network is low due to the lack of availability of 802.15.4 interfaces for laptops and hand-held devices.

Multi-site security

LumaWatt Pro supports very large campuses consisting of multiple buildings and energy managers. These can be viewed and administered seamlessly at the campus level viewed via the Global Energy Manager. There are two commonly used architectures. These are listed below as Options A and B. All communication between nodes uses SSL (TLS) or Secure Shell encryption. Communication between the Global Energy Manager and web clients is HTTPS. Further, there is an on-premises option for customers who wish to connect their LumaWatt Pro System to their BMS for monitoring and/or advisory HVAC Control.

Cybersecurity reporting and mitigation plans

Eaton's Cybersecurity Center of Excellence (COE) involvement and guidance is key as part of all current and future development to ensure our product incorporate industry and governmental network security best practices.

Eaton considers latest available best industry practices (DHS, NIST, FIPS) to reduce, identify, contain and manage risks: Deter, Protect, Detect, React, Recover

The COE also provides a publically accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

See www.eaton.com/cybersecurity for more detail.

Cybersecurity or functionality issues and reporting

Issues found in the field can be reported to Eaton service and support group, who will attempt to replicate the issue. If the issue can be replicated it is reported through internal issue tracking software which assigns the issue to the engineering team for resolution.

Depending on the severity and priority of the reported issue, this could include standard firmware or software updates published to the website or a proactive service visit by Eaton service and support group.

Eaton's view on cybersecurity

Eaton views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the all Eaton connected lighting systems employ current industry best practices to reduce, identify, contain and manage security risks. These systems have been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Eaton Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of each system and offers Eaton customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain Eaton product solutions in a secure environment. More information on the Eaton PCCoE can be found at www.eaton.com/cybersecurity

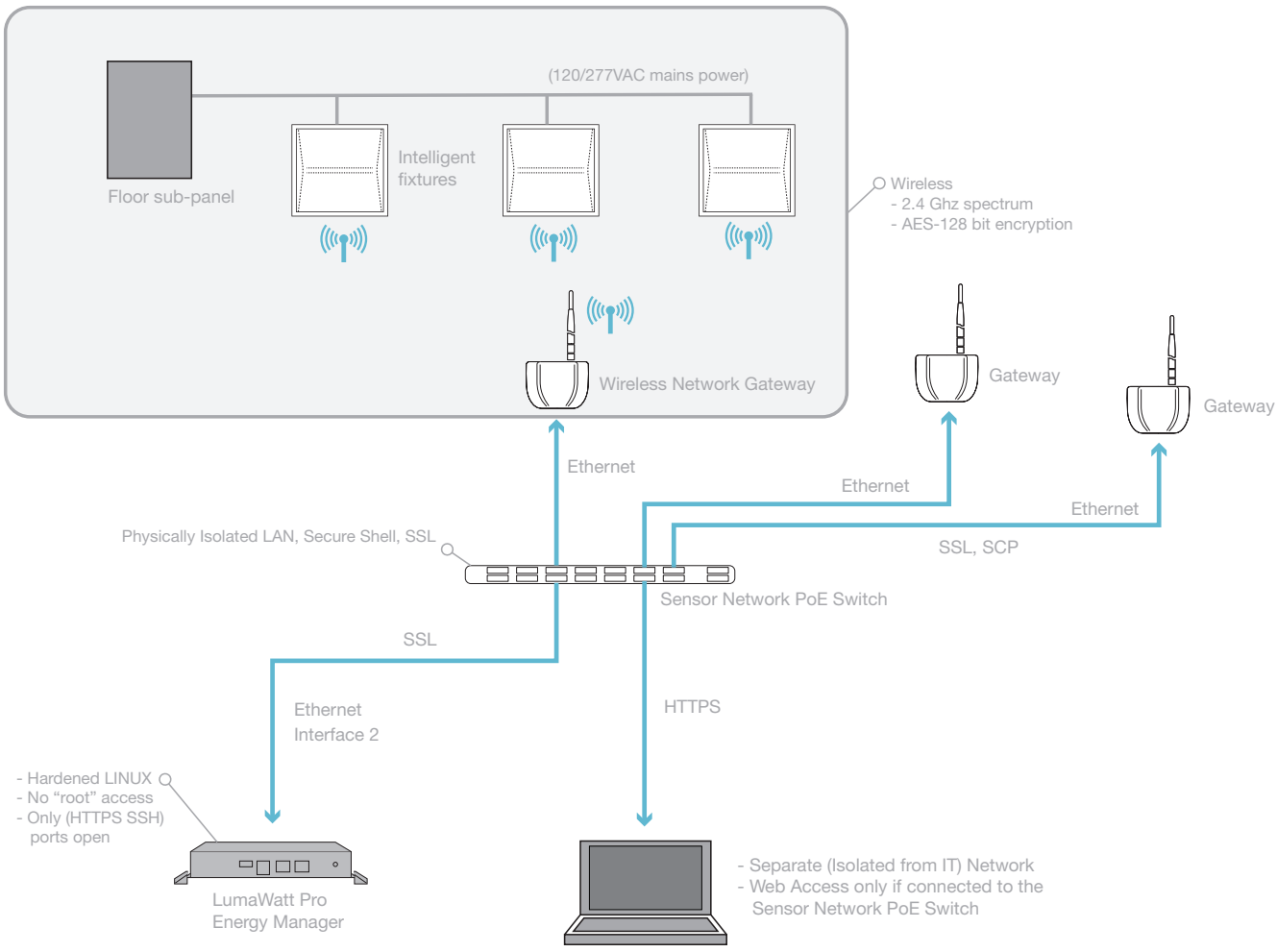
Network topology options

The LumaWatt Pro network provides the following topology options:

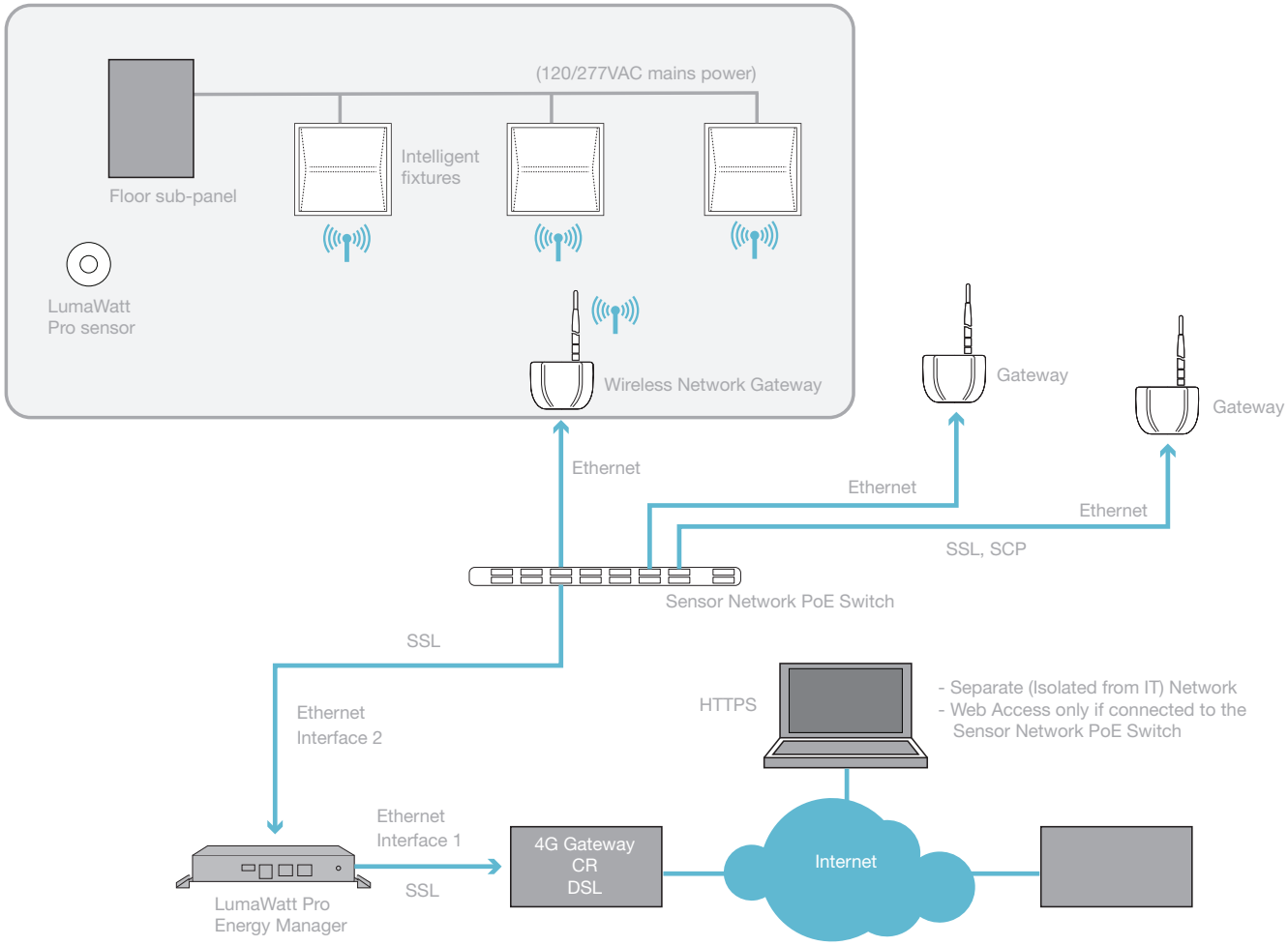
1. Gateways on Separate Secure Network, on premise - IT does not want the system on the corporate LAN
2. Cloud Connected Secure Connections, (multiple sites) - Provides secure access to multiple locations - Provides secure access to multiple locations
3. Corporate LAN Deployment with L2 VLAN - Lighting network exists on a Layer 2 VLAN - Lighting network exists on a Layer 2 VLAN
4. Corporate LAN Deployment with BMS Connection – Mode 1
5. Corporate LAN Deployment with BMS Connection – Mode 2
6. Enterprise Energy Manager Deployment with BMS Connection

Each topology is explained in detail in the following sections.

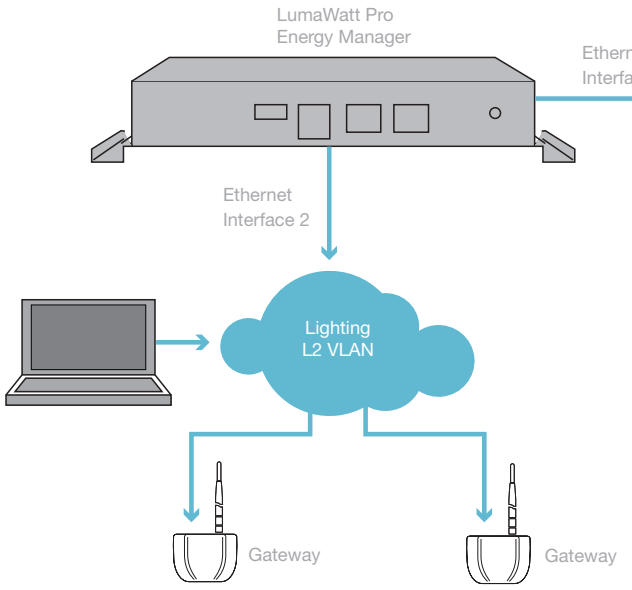
Option 1: Gateways on Separate Secure Network, on premise



Option 2: Cloud Connected Secure Connections (Multiple Sites)



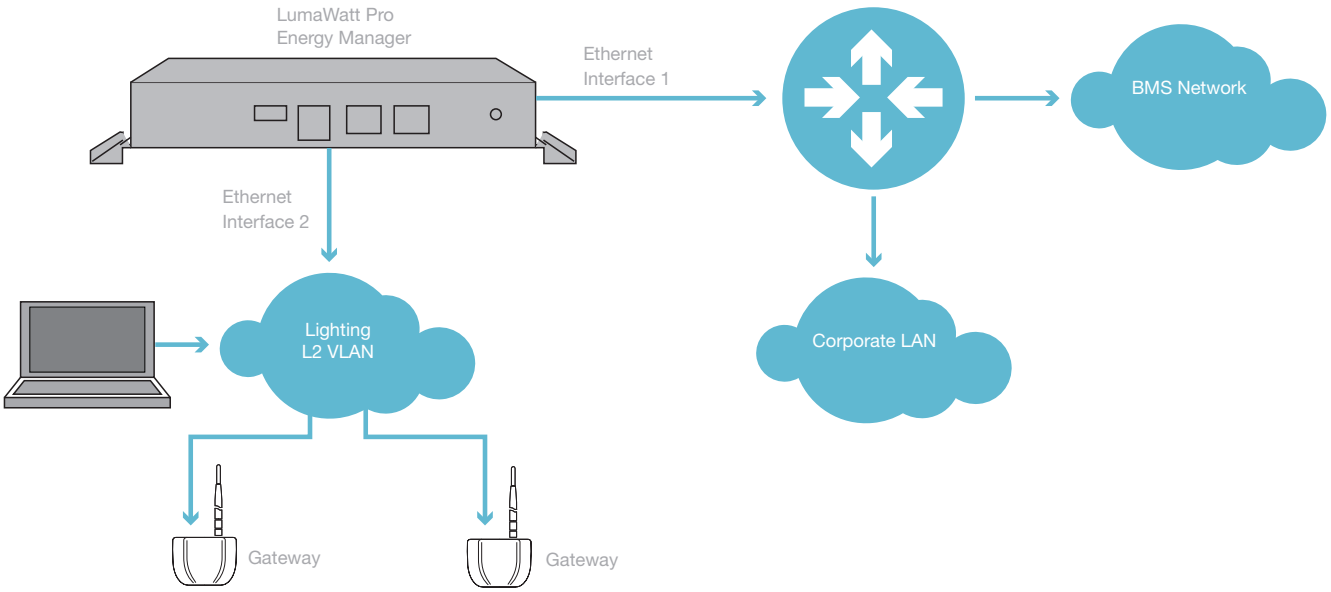
Option 3: Corporate LAN Deployment with L2VLAN



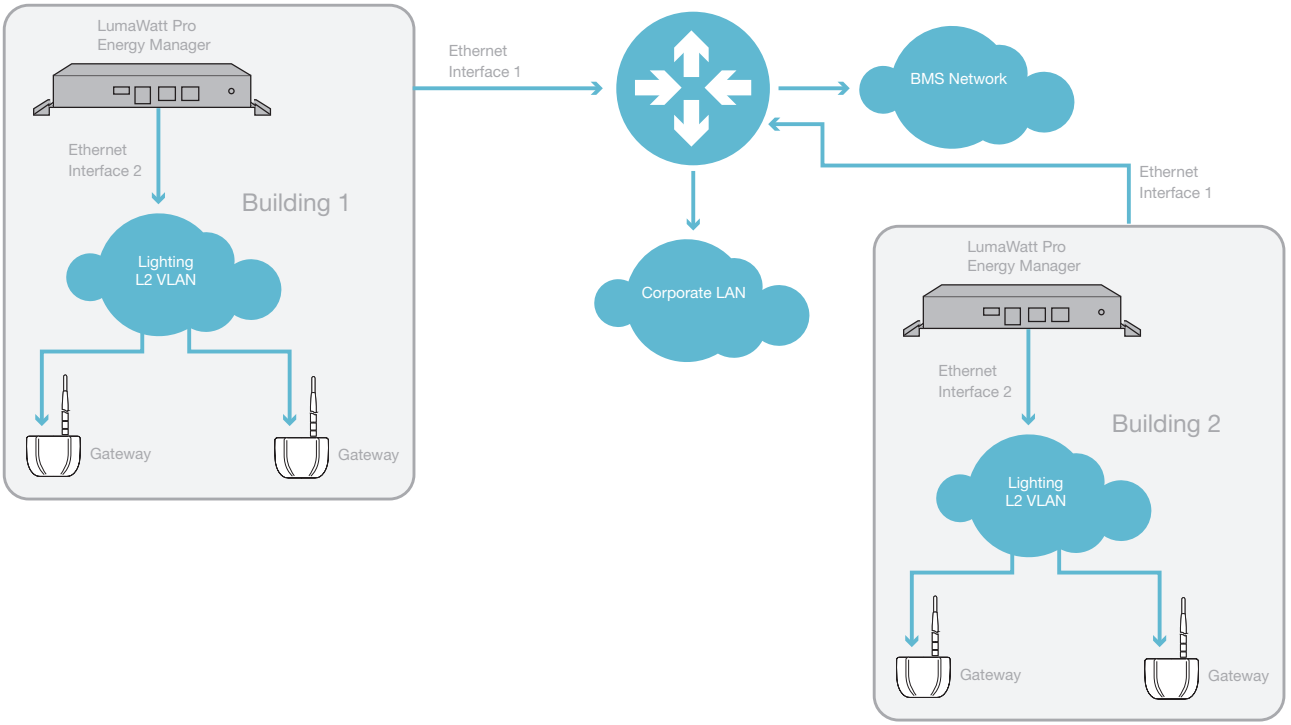
Option 1:
- Energy Manager Acts as DHCP server and services addresses only to ENL Gateways
- Gateways automatically discovered added to EM

Option 2:
- EM DHCP Server turned off
- Corporate DHCP Server serves addresses
- Gateways and EM addresses reserved via DHCP reservation
- Gateways manually added to EM

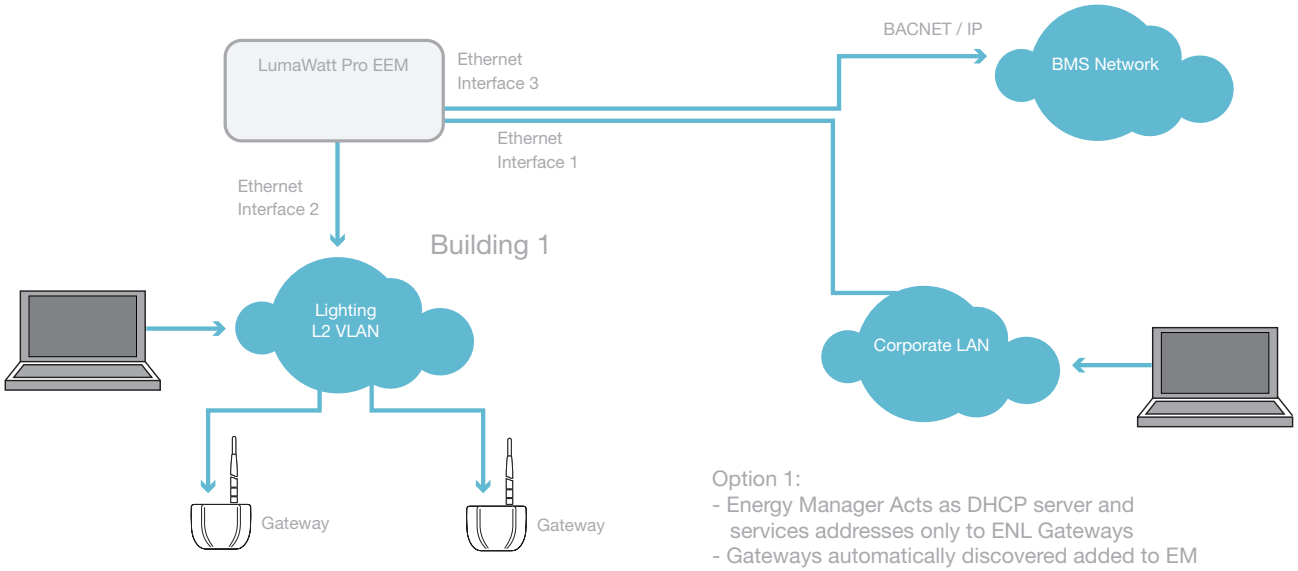
Option 4: Corporate LAN Deployment with BMS Connection - Mode 1



Option 5: Corporate LAN Deployment with BMS Connection - Mode 2



Option 6: Enterprise Energy Manager Development with BMS Connection



Option 1:
- Energy Manager Acts as DHCP server and services addresses only to ENL Gateways
- Gateways automatically discovered added to EM

Option 2:
- EM DHCP Server turned off
- Corporate DHCP Server serves addresses
- Gateways and EM addresses reserved via DHCP reservation
- Gateways manually added to EM

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Eaton
Lighting systems
1121 Highway 74 South
Peachtree City, GA 30269
www.eaton.com/lightingsystems

Printed in USA
Publication No. AP503023EN
January 2018

Powering Business Worldwide