General Information

Cooper Lighting Solutions views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the WaveLinx connected lighting (WCL) system employs current industry best practices to reduce, identify, contain and manage security risks. WaveLinx 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 Cooper Lighting Solutions Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of WaveLinx and offers Cooper Lighting Solutions customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain Cooper Lighting Solutions product solutions in a secure environment. More information on the Cooper Lighting Solutions PCCoE can be found at www.cooperlighting.com/cybersecurity

The WaveLinx connected lighting (WCL) 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.

Security Features Include

1.   Physical security:
- An architecture that isolates the wired Ethernet network from the wireless network, which strictly limits the possibility of the WaveLinx wireless being used as an access point to the corporate network and gain confidential information.
- Physical access also involves the customer location. This includes not allowing unauthorized personnel in areas where they do not belong, or access to devices they should not be connecting to.

2.   Customer security:
- Customer security process is a partnership between Cooper Lighting Solutions and the customer and involves multiple levels of password and network access protection.
- Beyond physical access the customer provides an additional layer of security with strong authentication to access their corporate wired or wireless network and limiting the devices that can access those networks.
- Cooper Lighting Solutions provides additional protection with unique username and password requirements for each WaveLinx Area Controller that are securely stored per NIST-recommended best practices.

3.   Device communication security:
- For secure device-to-device communications, encryption is an important factor to reduce the potential of someone reading data sent on the network. For that reason, all WaveLinx communications use AES 128-bit encryption, recommended by NIST as part of FIPS publication 197.

4.   Network communication security:
- WaveLinx uses secure HTTPS (TLS1.2) protocols for securing connections to the WaveLinx Area Controller over the wired network.
- WaveLinx uses secure WPA2 Enterprise technology for secure connections to the WaveLinx Area Controller over the Wi-Fi network when acting as an access point. If the WaveLinx Area Controller is connected to a wired network for communications this connection method is disabled.
- WaveLinx mobile applications uses HTTPS (TLS1.2) as part of its communications to the WaveLinx Area Controller regardless of connection method, which means only our mobile application can send data to the WaveLinx connected lighting (WCL) system.

5.   Network segmentation security:
- Each WaveLinx Area Controller employs its own unique keys, which limits any potential breach to only a small area of the system.
- The WaveLinx Area Controller (WAC) provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network.
- The IT/OT network segmentation provides a barrier to possible IT network attack surface exposure. Even if an attack within the lighting (OT) network and its devices is successful, the WAC isolates the enterprise IT network from potential attack.

6. **OTA update security:**
    - WaveLinx provides a method to allow for digitally signed firmware update files to be sent to the devices over the air (OTA). It is imperative as part of network security to ensure OTA updates are digitally signed firmware images from their manufacturer so the devices recognize they are valid updates from that manufacturer and not sent with a malicious intent.

7. **COE assurance:**
    - Cooper Lighting Solutions Cybersecurity Center of Excellence involvement and guidance was key as part of the WaveLinx development to ensure our product incorporates industry and governmental network security best practices.
    - 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.
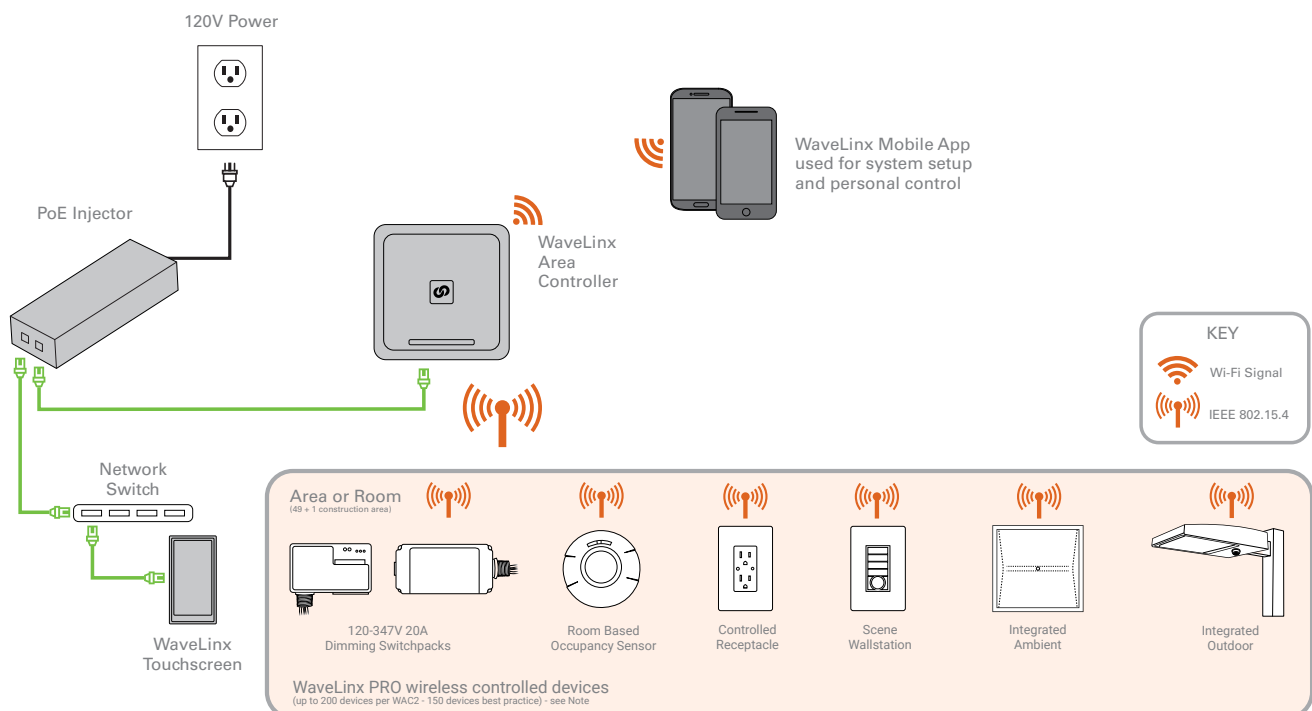
WaveLinx PRO deployments

Connected to the corporate IT network via Ethernet:

- The WaveLinx CORE connects to the corporate network via PoE switch and must have Ethernet access. This is required for certain features such as BACnet® integration or CORE Locate.
- This can also accommodate setting up separate networks for your lighting control or building systems than your business information network such as a VLAN.
- Wi-Fi is used for communications from the smart phone or laptop to the WaveLinx Area Controllers for programming, configuration and personal control through the use of internal web pages or the WaveLinx mobile application.
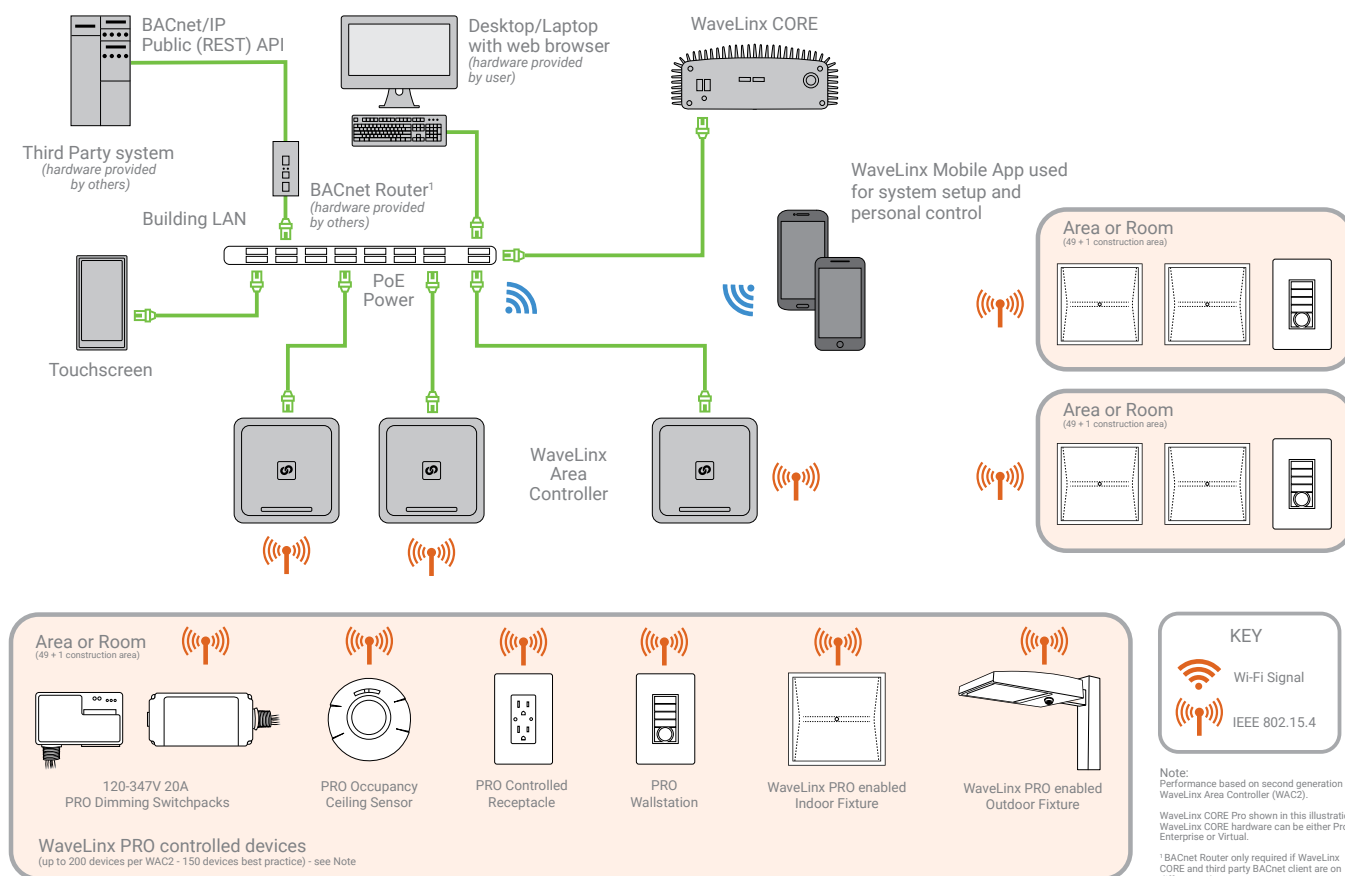
Dedicated WaveLinx Network:
- The WaveLinx Area Controller does not connect to the physical corporate IT network at all. This means the WaveLinx Area Controller is setup as a WiFi access point and the WaveLinx mobile application connects directly to the WaveLinx Area Controller using WPA2 wireless encryption and secure network username and password (this still requires attention to Security features 1 and 2 above.
- The WaveLinx Area Controller still uses AES 128-bit encryption for all device to device network communications.
- WiFi is used for communications from the phone smart device or laptop to the WaveLinx Area Controllers for programming, configuration and personal control through the use of internal web pages or the WaveLinx mobile application.

120V Power

WaveLinx Mobile App used for system setup and personal control

PoE Injector

WaveLinx Area Controller

KEY

Wi-Fi Signal

IEEE 802.15.4

Network Switch

Area or Room
(49 + 1 construction area)

120-347V 20A Dimming Switchpacks

Room Based Occupancy Sensor

Controlled Receptacle

Scene Wallstation

Integrated Ambient

Integrated Outdoor

WaveLinx Touchscreen

WaveLinx PRO wireless controlled devices
(up to 200 devices per WAC2 - 150 devices best practice) - see Note

COOPER
Lighting Solutions

Connected to the corporate IT network via Ethernet:

- The WaveLinx Area Controller connects to the corporate network via PoE switch or power injector and must have Ethernet access. This is required for certain features such as BACnet® integration or future smart building integration features.
- This can also accommodate setting up separate networks for your lighting control or building systems than your business information network such as a VLAN.
- WiFi is used for communications from the phone smart device or laptop to the WaveLinx Area Controllers for programming, configuration and personal control through the use of internal web pages or the WaveLinx mobile application.

BACnet/IP
Public (REST) API

Desktop/Laptop
with web browser
*(hardware provided
by user)*

WaveLinx CORE

Third Party system
*(hardware provided
by others)*

Building LAN

BACnet Router[1]
*(hardware provided
by others)*

WaveLinx Mobile App used
for system setup and
personal control

Area or Room
(49 + 1 construction area)

PoE
Power

Touchscreen

WaveLinx
Area
Controller

Area or Room
(49 + 1 construction area)

Area or Room
(49 + 1 construction area)

120-347V 20A
PRO Dimming Switchpacks

PRO Occupancy
Ceiling Sensor

PRO Controlled
Receptacle

PRO
Wallstation

WaveLinx PRO enabled
Indoor Fixture

WaveLinx PRO enabled
Outdoor Fixture

WaveLinx PRO controlled devices
(up to 200 devices per WAC2 - 150 devices best practice) - see Note

KEY

Wi-Fi Signal

IEEE 802.15.4

Note:
Performance based on second generation
WaveLinx Area Controller (WAC2).

WaveLinx CORE Pro shown in this illustration.
WaveLinx CORE hardware can be either Pro,
Enterprise or Virtual.

[1] BACnet Router only required if WaveLinx
CORE and third party BACnet client are on
different subnets.

Cooper Lighting Solutions advises following your corporate best practices and selecting the installation method to meet your building and application requirements. Refer to the following Cooper Lighting Solutions white paper for additional guidelines about secure network configuration and management.

COOPER
Lighting Solutions