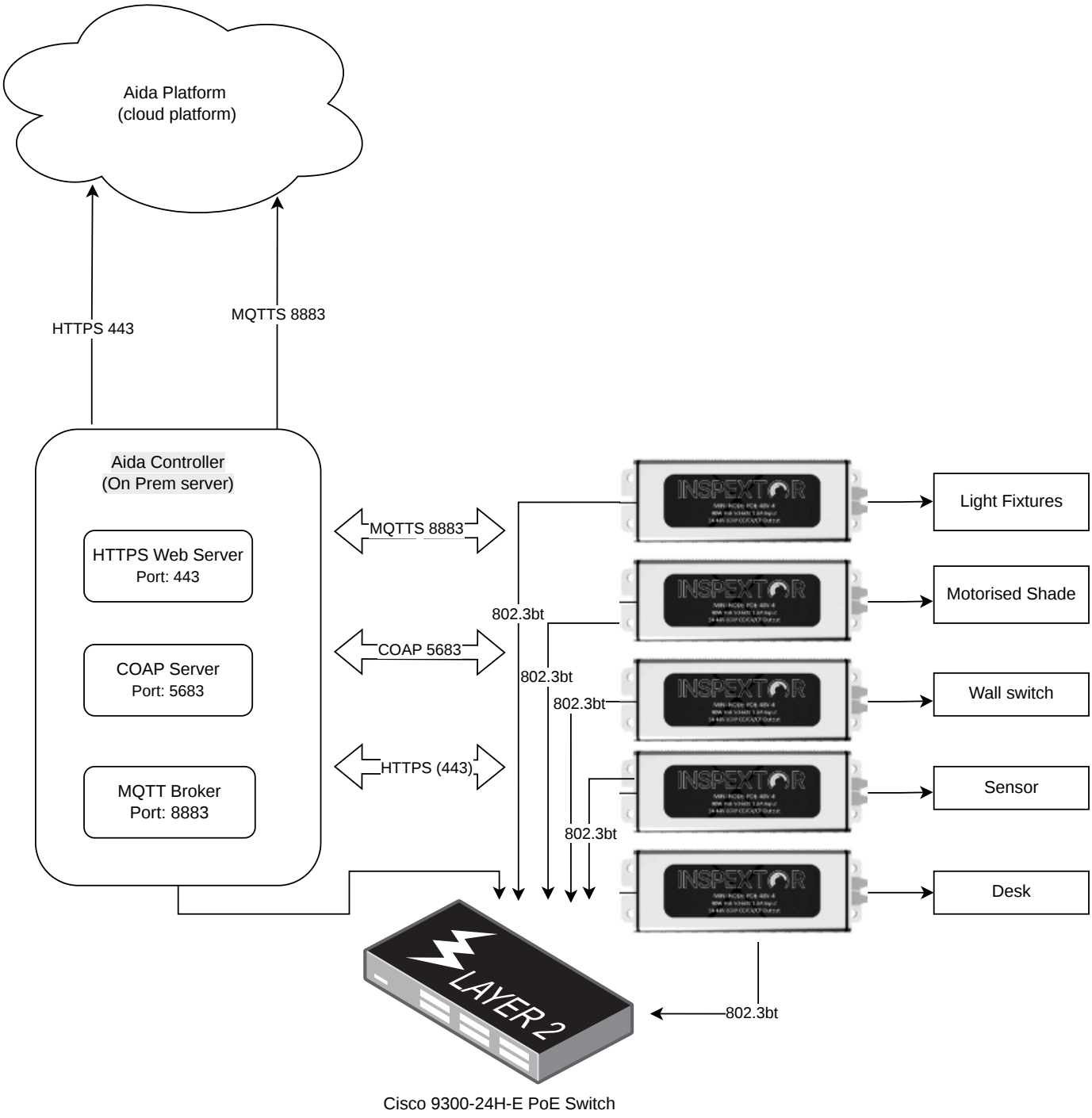

Cisco 9300-24H-E PoE Switch

MHT Core Node Communication Flow

Overview

The Aida Controller is the on-premises lighting control server responsible for configuring, monitoring, and managing all MHT Core Nodes. The controller is connected to the Cisco Catalyst PoE switch, and all Core Nodes communicate with the controller over the local network.

The MHT Core Node provides the same functionality as the Node90, including control and management of connected field devices such as:

- Light Fixtures
- Motorized Shades
- Wall Switches
- Occupancy/Environmental Sensors
- Desk Controllers

The Aida Controller manages:

- Device discovery
- Device configuration
- Scheduling
- Monitoring
- Diagnostics
- Firmware updates
- Lighting and shade control

Unlike the Node90, the MHT Core Node supports two communication modes:

1. CoAP Mode

- Provides the same communication behavior as Node90.
- Uses CoAP communication over UDP port 5683.
- Uses local broadcast messaging for real-time device control.

- Control events are processed locally by Core Nodes without requiring communication with the Aida Controller.

2. Secure MQTT Mode

- Provides secure communication between the Aida Controller and Core Nodes.
- Uses MQTT over TLS (MQTTS) on TCP port 8883.
- All control events are securely transmitted between Core Nodes and the Aida Controller.
- The Aida Controller centrally processes control requests and sends commands to the required devices.

Communication Flow

1. User Access to Aida Controller

Users access the Aida Controller through a web browser using HTTPS.

Source	Destination	Protocol / Port	Purpose
User PC	Aida Controller	HTTPS (TCP 443)	Secure access to Aida Controller web interface

Users can access the controller by navigating to:

https://<Aida_Controller_IP>

---

2. Aida Controller ↔ Core Node Communication

The MHT Core Node supports two communication methods depending on the selected operating mode.

Mode 1: CoAP Communication Mode

Core Node Communication Using CoAP

In CoAP mode, the MHT Core Node communicates using the same communication method as the Node90.

The Aida Controller communicates with Core Nodes using:

Protocol	Port	Purpose
CoAP	UDP 5683	Device discovery, configuration, monitoring, scheduling, status updates, and control commands

CoAP is the primary communication channel between the Aida Controller and Core Nodes for system management and configuration.

CoAP Mode – Local Broadcast-Based Control

In CoAP mode, real-time device control is performed using local broadcast communication.

When a user activates a connected device, such as:

- Wall switch
- Occupancy sensor

the associated Core Node generates a CoAP broadcast message on the local network.

The broadcast message contains the required control information, including the assigned group (cluster) identifier.

All Core Nodes on the network receive the broadcast message and evaluate the group information.

Operation:

- If the received group identifier matches the Core Node's configured group, the Core Node executes the requested action.
- If the group identifier does not match, the Core Node ignores the message.

Because control messages are distributed locally between Core Nodes, the Aida Controller is not required for every user interaction.

This provides:

- Low-latency control
- Faster response times
- Distributed system operation

- Continued local control capability even if the Aida Controller is temporarily unavailable

---

Mode 2: Secure MQTT Communication Mode

Secure Communication Between Aida Controller and Core Nodes

When Secure MQTT Mode is enabled, the MHT Core Node communicates with the Aida Controller using MQTT over TLS.

Communication uses:

Protocol	Port	Purpose
MQTT over TLS (MQTTS)	TCP 8883	Secure real-time communication between Aida Controller and Core Nodes

In this mode, Core Nodes no longer rely on broadcast messaging.

All control events are securely transmitted through the Aida Controller.

MQTT Mode Control Flow

When a user activates a wall switch or when a sensor is triggered:

1. The Core Node generates a control event.
2. The event is securely transmitted to the Aida Controller using MQTT over TLS.
3. The Aida Controller processes the request.
4. The Aida Controller sends the appropriate command to the required Core Node(s) in that group.
5. The Core Node executes the requested action.

All communication occurs using secure unicast MQTT messages.

Advantages of MQTT Mode:

- Secure device-to-server communication
- Centralized control processing
- No dependency on Layer 2 broadcast traffic

- Improved visibility and monitoring through the controller

---

3. Configuration and Firmware Updates

Regardless of operating mode, configuration and firmware updates are performed using secure HTTPS communication.

Source	Destination	Protocol / Port	Purpose
Aida Controller	Core Node	HTTPS TCP 443	Configuration, firmware updates, device management

HTTPS communication provides secure transfer of:

- Firmware packages
- Configuration parameters
- Device settings
- System updates

---

4. Aida Controller → Aida Platform (Cloud)

The Aida Controller establishes secure outbound connections to the Aida Platform cloud service.

No inbound Internet connections or port forwarding are required.

Protocol	Port	Purpose
HTTPS	TCP 443	Secure communication with Aida Platform
MQTT over TLS	TCP 8883	Secure real-time cloud communication

These outbound connections enable:

- Webex integration
- Remote system management (when enabled)
- Cloud monitoring

- Software updates
- Secure cloud communication

IP Address Assignment (DHCP)

All MHT Core Nodes require a valid IP address to communicate with the Aida Controller.

Core Nodes obtain IP addresses automatically from the customer's DHCP server.

After receiving an IP address, Core Nodes can communicate with the Aida Controller using the configured communication mode.

Requirements

- DHCP server must be available on the Core Node network.
- Each Core Node must receive a unique IP address.
- Aida Controller and Core Nodes must communicate through the same network or properly routed VLANs.
- Required firewall rules must allow required communication ports.

Network Switch Requirements (IEEE 802.3bt PoE)

Each MHT Core Node must be connected to an IEEE 802.3bt (PoE++) capable switch port.

The Core Node uses power received from the network switch to operate itself and connected field devices.

Supported devices include:

- Light Fixtures
- Motorized Shades
- Wall Switches
- Sensors
- Desk Controllers

Requirements

- Switch ports must support IEEE 802.3bt (PoE++).

- PoE must be enabled on Core Node switch ports.
- Network switch must have sufficient PoE power budget.
- Cisco Catalyst 9300-24H is an example of a compatible switch.

Required Firewall and Network Ports

Direction	Protocol	Port	Purpose
User PC → Aida Controller	HTTPS	TCP 443	Access Aida Controller web interface
Aida Controller ↔ Core Node	CoAP	UDP 5683	Device communication, configuration, monitoring, control
Core Node ↔ Core Node	CoAP Broadcast	UDP 5683	Local distributed control communication (CoAP Mode only)
Aida Controller ↔ Core Node	MQTTS	TCP 8883	Secure real-time communication (MQTT Mode only)
Aida Controller → Core Node	HTTPS	TCP 443	Firmware updates and configuration
Aida Controller → Aida Platform	HTTPS	TCP 443	Secure cloud communication
Aida Controller → Aida Platform	MQTTS	TCP 8883	Secure cloud messaging

---

Summary

The MHT Core Node supports two operating modes:

CoAP Mode

In CoAP mode, Core Nodes operate similarly to Node90 devices.

- Communication uses CoAP over UDP port 5683.
- Real-time control relies on local CoAP broadcast messages.

- Wall switch and sensor events are distributed directly between Core Nodes.
- Only Core Nodes belonging to the matching group/cluster respond.
- Control operation does not require every event to pass through the Aida Controller.

Secure MQTT Mode

In Secure MQTT Mode:

- Core Nodes communicate securely with the Aida Controller using MQTT over TLS on TCP port 8883.
- All control events are transmitted through secure unicast MQTT messages.
- The Aida Controller centrally processes commands and controls the appropriate devices.
- Broadcast communication is not used.

For configuration, device management, and firmware updates, the MHT Core Node uses secure HTTPS communication over TCP port 443.

The Core Node provides flexibility by supporting both distributed local control using CoAP and secure centralized control using MQTT, allowing deployment designs to adapt to different network security and operational requirements.