Overview

Overview of Cisco Sensor Connect for IoT Services

Cisco Sensor Connect for IoT Services solution enables the delivery of advanced BLE capabilities over Cisco Catalyst Wireless infrastructure. The key component of this solution is the IoT Orchestrator, which is a Cisco IOx application that can be deployed on any existing Cisco Catalyst 9800 Wireless Controller platforms. With the Cisco Sensor Connect for IoT Services solution, you can:

- Securely onboard and control BLE devices

- Consume data telemetry using the Message Queuing Telemetry Transport (MQTT)

Cisco's IoT Orchestrator is loaded on Cisco Catalyst 9800 Wireless Controllers and leveraged as an IoT gateway. This utilizes your existing network deployments and interfaces, reducing the need to deploy an entirely new infrastructure. The IoT Orchestrator manages IoT devices to simplify the service deployment and ease of operation. The IoT Orchestrator provides a central area to control BLE devices and send BLE device data to appropriate recipients.

Cisco Sensor Connect Solution

The following diagram depicts the elements of the Cisco Sensor Connect solution.

Figure 1: Cisco Sensor Connect Solution (On-Premises Solution)
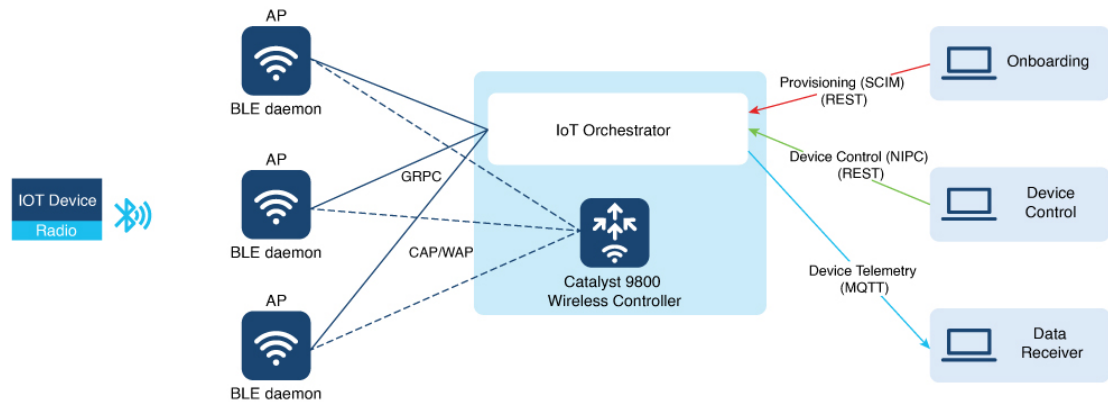
The IoT orchestrator is the new IOx application deployed on the Cisco Catalyst 9800 Wireless Controller as a Cisco IOx container that interacts with the AP using gRPC channels.

The AP uses its IoT radio to interact with the BLE device.

The IoT orchestrator provides APIs for the following:

- **Onboarding applications**: The onboarding applications leverage IETF SCIM for device models (https://datatracker.ietf.org/doc/draft-ietf-scim-device-model/). The SCIM allows an application to send a SCIM object to a SCIM server (gateway) to create, update, and delete devices in networks.

- **Device control applications**: The device control applications allow an application to connect to a non-IP device to exchange data with the device and register topics for streaming telemetry. The IETF draft used for this protocol is called the Non-IP Control (NIPC).

- **Data receiver applications**: The telemetry application receives the telemetry data from the IoT Orchestrator application.

- **Message Queuing Telemetry Transport (MQTT)**: Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol commonly used for communication between devices in IoT applications. Subscriptions and notifications play crucial roles in enabling devices to receive and react to messages. In MQTT, the clients subscribe to topics for receiving messages published to those topics. A topic is a string that the MQTT broker uses to filter messages for each connected client. The notification for subscribed topic happens from the IoT Orchestrator application to the data receiver application.

Note

- The existing NIPC APIs were created when the standard was still evolving, leading to some aspects being implemented differently. Starting with IoT Orchestrator release 2.0, these APIs will be updated to align with the latest draft version of NIPC. Please note that backward compatibility with APIs from version 1.x will not be supported.

- Applications must be authenticated and authorized using either a certificate-based method or an API key-based method, but not both. If both methods are selected, the certificate-based approach is preferred. For API key-based authentication, applications such as onboarding, control, and data receiver must be registered with the IoT Orchestrator to obtain an API key. These applications must include the API key in their requests when interacting with the IoT Orchestrator. For certificate-based authentication, the certificate must be presented in API requests to the IoT Orchestrator.