IoT FND in a FAN Solution

As the network management system, IoT FND lets you manage other components in a FAN, and perform various monitoring and administrative operations. Key FAN components include IoT FND itself, routers, endpoints, gateways, and security hardware and software. This chapter provides an overview of the roles and interactions of these key FAN components.

IoT FND Components

This section explains the role and function of the following IoT FND core components in the FAN solution:

- IoT FND Application Server
- IoT FND Database Server
- Tunnel Provisioning Server
- Load Balancer
- Software Security Module

IoT FND Application Server

The IoT FND application server resides in the data center and performs the functions that are needed to monitor and manage the FAN and devices. It hosts the IoT FND application and interacts with many of the components in the headend, including the IoT FND database server, DHCP server, headend routers (HER), and tunnel provisioning server (TPS). This server hosts the IoT FND user interface from which you perform IoT FND operations and management procedures and view information about the network, devices, and related items, and it stores the IoT FND log files.

The IoT FND application server runs under the Red Hat Enterprise Linux (RHEL) operating system and can be installed on a bare metal server or a virtual machine (VM).

IoT FND Database Server

The IoT FND database server resides in the headend and is the storage repository for the data that IoT FND generates and collects. This data includes metrics, device properties such as firmware images, configuration templates, and event notifications.

The IoT FND database server runs under the Red Hat Enterprise Linux (RHEL) operating system and can run the Oracle or Postgres database. When running Oracle, the IoT FND database server can be installed on a bare metal server or a VM. When running Postgres, this server can be installed only on a VM.

The IoT FND application server is the only component that interacts directly with the IoT FND database server.

Tunnel Provisioning Server

The tunnel provisioning server (TPS) resides in the DMZ and is a proxy server for IoT FND. The TPS provides a bridge for the communication between IoT FND and FARs. It relays tunnel requests from FARs to IoT FND and provides FARs with the configuration for the tunnel to the headend.

When they first start up, routers communicate with IoT FND through the TPS. After IoT FND provisions tunnels, routers communicate with IoT FND directly.

Load Balancer

An optional load balancer provides IoT FND server high availability. You can connect multiple IoT FND servers to a load balancer.

Load balancing is configured using a third-party device and is supported only in an IoT FND bare metal server deployment.

Software Security Module

The software security module (SSM) is an optional component of IoT FND. It is used to sign CSMP messages that IoT FND sends to meters and to Cisco IR500 endpoints. The SSM is bundled with the IoT FND image.

The SSM has a limited scaling capability and does not support high availability. We recommend that a hardware security module be used instead of the SSM in production environments.

Devices Managed by IoT FND

IoT FND lets you manage and monitor the following types of devices in a FAN:

- Field Area Routers
- Headend Routers
- Endpoints
- Gateways

Field Area Routers

Field area routers (FARs) reside in the FAN. They communicate with headend routers through tunnels that are provisioned by the TPS.

IoT FND provides options for managing the lifecycle activities of FARs, and for monitoring and troubleshooting.

You can use IoT FND to manage the following FARs:

- Cisco Catalyst IR1800 Rugged Series Router
- Cisco Catalyst IR8100 Heavy-Duty Series Router
- Cisco Catalyst IR1100 Rugged Series Router
- Cisco 1000 Series Connected Grid Router
- Cisco 800 Series Industrial Integrated Services Router
- Cisco 800 Series Router

Headend Routers

Headend routers (HERs) reside in the DMZ and provide routing connectivity between FARs and other headend components in the DMZ and data center. These headend components include IoT FND, the AAA server, the DHCP server, and utility application servers, such as SCADA and MDMS servers.

IoT FND does not provide options for managing lifecycle activities of headend routers, but it does provide options for monitoring their status and configuration. It also provides options for provisioning tunnels between HERs and FARs and for viewing the status of tunnels.

Headend routers include the following devices:

- Cisco 8000 Series Router
- Cisco ASR 1000 Series Aggregation Services Routers (ASR 1001 or 1002)
- Cisco 4000 Series Integrated Services Router (ISR)
- Cisco Cloud Services Router 1000V Series (CSR)

Endpoints

Endpoints are Cisco and third-party devices, including meters from Itron and Landis+Gyr, range extenders, cameras, battery endpoints, and cellular endpoints.

IoT FND provides options for managing lifecycle activities of endpoints, and for monitoring and troubleshooting.

You can use IoT FND to manage the following endpoints:

- Cisco 500 Series Wireless Personal Area Network (WPAN) Industrial Routers (IR500)
    - Cisco IR510 (DA Gateway)
    - Cisco IR530 Series Resilient Mesh Range Extenders
- Mesh endpoints (from Itron and Landis+Gyr)

Gateways

Gateways provide connections between the FAN and other networks or the internet.

IoT FND provides options for managing lifecycle activities of gateways, and for monitoring and troubleshooting.

You can use IoT FND to manage the following gateways:

- Cisco IC3000 Industrial Compute Gateway
- Long Range Wide Area Network (LoRaWAN) Interface Module for Cisco 800 Series Industrial Integrated Services Routers (IR800)
- Landis+Gyr N2450 Network Gateway

Security Components in a FAN Solution

This section explains the key security components and their roles and interaction with IoT FND in the FAN solution.

- Public Key Infrastructure, on page 4
- Registration Authority
- Hardware Security Module, on page 4
- Authentication, Authorization, and Accounting

Public Key Infrastructure

A public key infrastructure (PKI) includes hardware and software for managing and controlling digital certificates and public-key encryption. In the FAN solution, digital certificates are issued to IoT FND and FARs so that they can authenticate and securely communicate with each other and with other FAN components.

The PKI includes a certificate authority (CA) server that issues RSA certificates for routers, ECC certificates for endpoints, and web certificate for IoT FND. Routers use Simple Certificate Enrollment Protocol (SCEP) to request and receive certificates. Endpoints use Enrollment over Secure Transport (EST) to request and receive certificates.

Registration Authority

A registration authority (RA) is a proxy that FARs use when requesting a digital certificate. Because a CA server cannot be in a public network, FARs use the RA to communicate with the CA to obtain digital certificates for secure communication. The RA proxies requests between public and private networks.

Hardware Security Module

A hardware security module (HSM) is a third-party appliance that is used to sign CSMP messages that IoT FND sends to meters and Cisco IR500 endpoints.

An HSM scales to support large FANs and supports high availability. We recommend that an HSM be used instead of the SSM in production environments.

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA) is a security framework that authenticates (verifies) FARs and endpoints before they can join the FAN, authorizes (grants access) for these devices to join the

FAN, and provides accounting (tracking) of the activities of these devices. The RADIUS protocol is used for authorization.

DHCP Server

The dynamic host configuration protocol (DHCP) server allocates IPv4 and IPv6 IP address to FARs. During tunnel provisioning, IoT FND sends requests to the DHCP server for the IP address on behalf of FARs, compiles the addresses that it receives as part of the tunnel provisioning configuration, and pushes the addresses to FARs through the TPS.