Cisco Edge Fog Fabric (EFF)

April 2017

Q What is Cisco Edge Fog Fabric (EFF)?

A Cisco® Edge Fog Fabric (EFF) is an open, modular, and microservice architecture IoT platform. It enables immediate and intelligent processing and distribution of data. It is designed to process data where it is actively created. It provides a differentiated approach that filters, aggregates, and compresses data at the edge, in the fog, or in the data center or the cloud as appropriate for the operations. Independent software modules, implemented as microservices, connect to each other using a common architecture, providing the flexibility to add, modify, and upgrade as required over time. This openness allows for EFF to easily incorporate custom microservices or microservices from third parties to add functionality and enhance the system.

Q What business problems does Cisco EFF solve?

A Cisco EFF enables a new class of IoT applications for industrial customers in verticals such as manufacturing, oil and gas, utility, mining, transportation, smart grid, and more and helps solves business problems in areas as follows:

- Advanced monitoring and diagnostics
- Overall equipment efficiency (OEE)
- Real-time quality detection
- Proactive maintenance
- Operational intelligence
- Asset tracking and management
- Condition-based maintenance
- Personnel safety

Q Why should I use EFF?

A Customers should use Cisco EFF for the following reasons:

- EFF has the ability to immediately process and analyze distributed data at the edge and fog nodes.

- EFF runs on top of existing Cisco networking equipment and servers and third-party IoT gateways/servers, enabling business intelligence at the edge without affecting bandwidth, making the IoT network smarter.
- EFF continuously analyzes and makes decisions about IoT data at the edge in environments where connection to the cloud is unreliable or intermittent.
- EFF is an open architecture platform, preventing vendor lock-in. SDKs in various languages are available to create microservices or applications by any third party, allowing for unlimited capability and growth by adding software components that optimize the results of the application, system, or outcome.
- Secure remote access to IoT data for sensor SME, engineers, and operators.

Q What are the major components of Cisco EFF software? What does each component do?

A Cisco EFF includes several components that combine to create a modular, highly scalable, and secure system for deploying, managing, and running enterprise IoT solutions. Key components includes system administrator, dataflow editor, system monitor, and IoT historian database:

- **System administrator:** A graphical user interface for quickly and effectively viewing and managing the lifecycle of EFF components such as message brokers, microservices, and users.
- **Dataflow editor:** An easy-to-use drag-and-drop development tool for defining streaming data transformations and analytic logic.
- **System monitor:** A standalone tool for operators to obtain real-time functional status of a deployed EFF solution.
- **Message broker:** A software component that reliably routes messages between clients by providing publish-subscribe and request-reply message exchange with guaranteed QoS delivery.
- **Links:** A software component that enables communication between edge devices and brokers and can be used for data acquisition and/or control. It communicates with the IoT device using its native language and bridges from native protocol to EFF protocol.
- **IoT historian database:** A massively parallel (MPP), shared-nothing data management system optimized to run complex analytical queries over extremely large amounts of data on a cluster of commodity servers.

Q How does EFF work (features and benefits)?

A EFF puts analytics at the point of data collection, streamlining the way businesses monitor processes. We start with the underlying IP network and superimpose EFF components on the network so we can move the data from the edge to the cloud. Using EFF configuration tools, we make connections to the various devices and applications, which results in a working IoT system. Disparate and distributed data is connected, instantly comparing operational parameters against business rules governing performance. Sensed changes are measured against models suitable for business conditions at the point of collection; corrective actions can precisely align with trending changes.

EFF provides the following capabilities:

- **Open aarchitecture:** EFF provides modules from Cisco and third parties as needed. The platform accommodates a wide variety of distributed/IoT use cases, from simple to very complex. You can normalize and modify data as it is flowing to convert or customize for specific operations.

- **Scalable:** Present data consistently with the ability to incorporate microservices from any third party as your business grows. Processing is completed where most appropriate, and data filtering, aggregation, and compression are performed at the edge, in the fog, or at the data center.
- **Robust:** With a well-tested system, validated design, and proven methodology, EFF is ideal for the requirements of IoT systems that must be monitored, managed, and secure with high availability. Operations performance is maximized through real-time insights on which businesses can take action while eliminating the need to transfer all their data.
- **Control and action:** EFF accomplishes data collection and actuation in a unique, flexible, and repeatable manner. Disparate data is connected automatically, where it's needed, in business context, reducing complexity and cost. Control and automation can be implemented with a predefined policy architecture.
- **Multipurpose:** Value and use of data change over time. Built-in intelligence expands network capabilities without affecting bandwidth. Streaming data is valuable for monitoring and control where responsiveness is crucial. Later, analytics can create optimization, production improvements, or cost savings.

Q What devices and applications are supported?

A Connections to devices and applications are supported through specific protocol links. EFF supports a long list of common IoT devices and services. However, if a proprietary interface is needed, after the specifications and test equipment are supplied, a new data link can be developed. The full list of protocol links (both open source and custom) can be found at https://iot-dsa.github.io/links/web/status/. Protocol links are added and updated on a regular basis.

Q What are the Cisco EFF system requirements?

A The characteristics of the data (volume, velocity, and variety) and the processing desired drive the system requirements. For example, at the edge, where small amounts of compute resources are available, functions such as data transformations, filtering, and aggregations are typically performed. Table 1 provides the minimum system requirements at each layer of the EFF deployment architecture.

Table 1. System Requirements

Edge (low compute)	Disk space	N/A
	Hardware	Single core
	Memory	256 MB
	Operating system	Red Hat 7.2, CentOS 7.2, Ubuntu 14.04 LTS, Windows 10, IOX
Edge/fog/data center (high compute)	Disk space	100 GB
	Hardware	Six core, 2.4 GHz
	Memory	2 GB/core
	Operating system	Red Hat 7.2, CentOS 7.2, Ubuntu 14.04 LTS, Windows 10

Q What Cisco hardware is supported for the edge and fog nodes?

A Although EFF does not require any specific hardware, EFF software supports running on top of a number of Cisco servers and networking devices, creating a distributed computing fabric. Additionally, EFF supports running on third-party IoT gateways and servers. Table 2 outlines the Cisco specific hardware recommended based on the network location.

Table 2. Recommended Cisco Hardware

Network Location	Cisco Hardware
Edge (low compute)	Industrial edge routers ▪ IR 809/829 Industrial Ethernet switches ▪ IE 4000 Integrated services router ▪ ISR 4000 (with embedded Cisco UCS®)
Edge/fog/data center (high compute)	Cisco UCS C-Series Rack Servers ▪ Cisco UCS C220 ▪ Cisco UCS C240

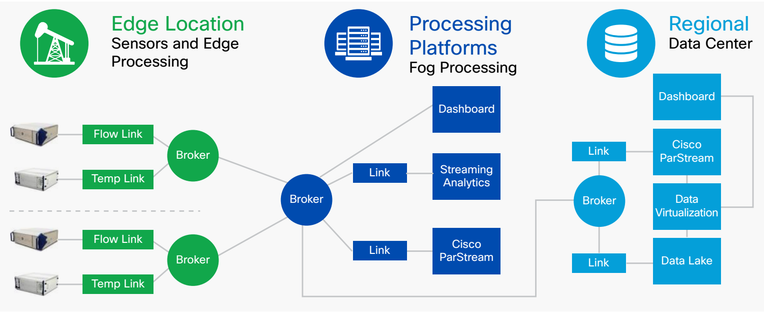
Q Is EFF installed on the premises or in the cloud?

A EFF is a distributed architecture where the majority of EFF components are installed at the edge, on the premises in the fog and the data center, but EFF enables data publication to external/cloud-based data stores and enterprise applications.

Q How is Cisco EFF deployed?

A Every IoT project is unique. This is because of different verticals with different business objectives as well as different networking topologies. Generally, IoT deployment architectures fall into three topologies with two, three, or four tiers of computing. To accommodate the wide range of system scope, topologies, and geography, EFF is an open, modular platform. Each of the functions within the EFF system can be installed at a given tier based on the processing needs at that location. Figure 1 depicts how each EFF component can be installed across the different tiers.

Figure 1. Sample Edge and Fog Fabric Deployment Architecture



Q What protocol is used between nodes in Cisco EFF?

A NodeAPI is the communication method for all EFF nodes and facilitates all messaging between entities in a standardized manner. NodeAPI makes sure of node compatibility and bidirectional control and monitoring ability between connected components. NodeAPI is a stateful and lightweight streaming remote procedure call (RPC) protocol.

Q How is Cisco EFF communication secured?

A The first rule of IoT security is the assumption that any device on a public IP with an open inbound port will be attacked. Thus, all initial connection handshakes among DSA nodes are outbound. All connections within EFF are established utilizing a reverse-tunnel metaphor. A link must connect to a message broker, thus advertising itself to it, and the message broker based on security policy establishes a connection back to the link through the same web socket channel or by pushing event queues if the link is connected through a long polling HTTP channel. The message broker is responsible for security enforcement, including authentication and authorization.

For More Information

Read more about the Cisco EFF or contact your local account representative.