Remote and Mobile Assets
Design and Implementation Guide
First Published: January 2019
# Contents

Part I: Overview .................................................. 3
   Introduction to Cisco Remote and Mobile Assets. .................. 3
   Target Customers and Markets .................................. 4
   Target Audience for the Cisco Remote and Mobile Assets Solution .... 6
Cisco Validated Design Overview .................................. 7
   Technology Components ..................................... 7
   Solution Building Blocks ..................................... 8
Part II: IT Design ................................................. 11
   Technology Guidance ........................................ 11
   Selecting the Router ......................................... 12
   Designing Your Solution ...................................... 13
Security Overview ............................................... 14
   Introduction to IoT Security .................................. 14
   Securing the GMM Management Plane ......................... 15
   Securing the Data Plane .................................... 16
   Introduction to FlexVPN ..................................... 16
   Benefits of using FlexVPN ................................... 17
   IoT Gateway and Device Security .............................. 18
   Other Security Best Practices ................................ 20
Industrial Routers ............................................... 21
   The Cisco Industrial Router Portfolio .......................... 21
   Select Hardware Features ................................... 24
   Network Features ............................................. 27
Cloud Provisioning and Management .............................. 31
   Introduction to Cisco Gateway Management Module .......... 32
   Provisioning .................................................. 33
   Authentication during the Gateway Registration and Claim Process .. 34
   Custom Configuration Templates for IOS Features ............ 35
   Management .................................................. 37
Network Integration ............................................. 41
   Headend Architecture and Design ............................ 41
   Edge Gateway Routing ....................................... 46
Wi-Fi ............................................................ 48
   Wi-Fi Connectivity .......................................... 48
Remote and Mobile Assets

This document is divided into four major parts, which are described below:

<table>
<thead>
<tr>
<th>Part I: Overview, page 3</th>
<th>Introduction to Cisco Remote and Mobile Assets, page 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Excerpts from the Solution Brief that describes the Cisco Remote and Mobile Assets solution and the target audience.</td>
</tr>
<tr>
<td></td>
<td>Cisco Validated Design Overview, page 7</td>
</tr>
<tr>
<td></td>
<td>Excerpts from the Solution Brief that provide a summary of the key components of this Cisco Validated Design.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part II: IT Design, page 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Guidance, page 11</td>
</tr>
<tr>
<td>Guidance for selecting the most appropriate Industrial Router and the platform architecture based on use cases and requirements.</td>
</tr>
<tr>
<td>Security Overview, page 14</td>
</tr>
<tr>
<td>End-to-end security considerations including securing the management plane, the data plane, and effective device security.</td>
</tr>
<tr>
<td>Industrial Routers, page 21</td>
</tr>
<tr>
<td>Information on the Cisco Industrial Router portfolio, key capabilities, and best practices for setting up the router and its accessories.</td>
</tr>
<tr>
<td>Cloud Provisioning and Management, page 31</td>
</tr>
<tr>
<td>Details of the Cisco Kinetic Gateway Management Module (GMM) with descriptions of key functional elements and best practices for using this platform.</td>
</tr>
<tr>
<td>Network Integration, page 41</td>
</tr>
<tr>
<td>Best practices and architectures for integrating the gateways with the enterprise network.</td>
</tr>
<tr>
<td>Wi-Fi, page 48</td>
</tr>
<tr>
<td>Best practices and architectures for enabling the Wi-Fi functionality on the IR829 and configuring the Workgroup Bridge (WGB).</td>
</tr>
<tr>
<td>Backhaul, page 55</td>
</tr>
<tr>
<td>Guidance for integrating the desired backhaul (LTE, Ethernet, or Wi-Fi), including redundancy options.</td>
</tr>
<tr>
<td>Prepare for Deployment, page 59</td>
</tr>
<tr>
<td>Key steps required to set up the GMM template, set up user accounts and prepare an existing gateway to be claimed by GMM using the Gateway Provisioning Tool (GPT).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part III: Field Operate, page 62</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Deployment, page 62</td>
</tr>
<tr>
<td>Easy to use workflows for onboarding a new gateway, replacing the gateway, and offboarding the gateway.</td>
</tr>
<tr>
<td>Field Monitoring and Troubleshooting, page 71</td>
</tr>
<tr>
<td>Best practices for monitoring and troubleshooting the gateway.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part IV: Sample Configurations, page 78</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and Software Matrix, page 78</td>
</tr>
<tr>
<td>Hardware and software versions that were validated in this CVD.</td>
</tr>
<tr>
<td>Data Center Configurations, page 79</td>
</tr>
<tr>
<td>Sample configurations for the three critical components of the data center. These include redundant, virtual HERs, a virtual Wireless LAN Controller, and the RADIUS server.</td>
</tr>
<tr>
<td>Extending the Enterprise Network, page 93</td>
</tr>
<tr>
<td>Sample configurations for extending the enterprise network to the gateways for devices and hotspot clients.</td>
</tr>
<tr>
<td>Custom Configuration Templates, page 101</td>
</tr>
<tr>
<td>Sample custom configuration to allow for additional Cisco IOS configurations such as Firewall, QoS, and Ignition Sensing. Uses the GMM Custom Configuration Templates.</td>
</tr>
<tr>
<td>Section</td>
</tr>
<tr>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Headend Router Configuration, page 104</td>
</tr>
<tr>
<td>Appendix, page 107</td>
</tr>
<tr>
<td>Ordering Information, page 107</td>
</tr>
<tr>
<td>Common Gateway Issues, page 109</td>
</tr>
<tr>
<td>Firewall Ports for GMM to Gateway</td>
</tr>
<tr>
<td>Communication, page 111</td>
</tr>
<tr>
<td>A Sample GMM Report, page 113</td>
</tr>
<tr>
<td>IOx and Fog Applications, page 114</td>
</tr>
</tbody>
</table>
Part I: Overview

This part includes the following chapters:

<table>
<thead>
<tr>
<th>Introduction to Cisco Remote and Mobile Assets, page 3</th>
<th>Excerpts from the solution brief that describes the Cisco Remote and Mobile Assets solution and the target audience.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Validated Design Overview, page 7</td>
<td>Excerpts from the Solution Brief that provide a summary of the key components of this Cisco Validated Design.</td>
</tr>
</tbody>
</table>

Introduction to Cisco Remote and Mobile Assets

The explosive growth in IoT and extending connectivity beyond office walls demands a new approach to networking. Enterprises need to connect geographically dispersed assets, accelerate IoT deployments, and act with insight—all while maintaining a comprehensive security fabric. This Cisco Remote and Mobile Assets solution pairs Cisco’s leading industrial routers (IR series) with Cisco Kinetic®. It provides a cloud-based platform for managing every component of asset connectivity—from the network and data to sensors and applications. The goal is to provide IT teams the tools they need while allowing field teams to focus on asset operations.

Figure 1   Overview of Cisco Remote and Mobile Assets
Target Customers and Markets

Target customers for the Cisco Remote and Mobile Assets solution have similar application requirements for connecting their assets, as shown in Table 1:

**Table 1 Application Requirements**

<table>
<thead>
<tr>
<th>Typical Applications</th>
<th>Platform Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Telemetry</td>
<td>SCADA-certified, ruggedized routers to meet stringent specifications</td>
</tr>
<tr>
<td>Asset Control</td>
<td>Edge compute options for automation and legacy protocols</td>
</tr>
<tr>
<td>Predictive Maintenance</td>
<td>Architecture for remote machine access and data acquisition</td>
</tr>
<tr>
<td><strong>Mobile Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Telematics</td>
<td>Best practices to deploy and manage at scale with a limited IT staff</td>
</tr>
<tr>
<td>Automatic Vehicle Location (AVL)</td>
<td>Integrated GPS and geofencing</td>
</tr>
<tr>
<td>Computer-Aided Dispatch (CAD)</td>
<td>Enterprise application integration using edge compute</td>
</tr>
</tbody>
</table>

Despite these similarities, the target segments also have distinct requirements based on their industry. Typical users fall into six categories with a number of vertical industries covered by each, as shown in Table 2:

**Table 2 Target Customers and Markets**

<table>
<thead>
<tr>
<th>Segment Category</th>
<th>Description</th>
<th>Sample Requirements</th>
</tr>
</thead>
</table>
| Connected Machines     | Enterprises with industrial equipment at distributed customer and indoor locations. Includes:  
                          | ■ Conveyor belts, escalators, etc.  
                          | ■ Indoor equipment                                                               | ■ Real-time telemetry of machines at customer locations  
                          |                                                                    | ■ Preventative maintenance/control without a truck roll  
                          |                                                                    | ■ Flexible routing options based on available connectivity |
| Outdoor Equipment      | Enterprises and public sector entities with industrial equipment in the field or at outdoor locations.  
                          | Includes:  
                          | ■ Oil and Gas Companies  
                          | ■ Roadways and Traffic management  
                          | ■ Utilities                                                          | ■ Ingress Protection (IP)-rated equipment to meet stringent temperature, dust, and operating specifications  
                          |                                                                    | ■ Edge compute options for legacy protocols  
                          |                                                                    | ■ SCADA-ready |
| Remote Sites           | Connectivity for remote and distributed sites. Includes:  
                          | ■ Retail and distribution centers  
                          | ■ Kiosks                                                                       | ■ Remote setup and operations by field workers  
                          |                                                                    | ■ Reliable data access and options for additional network services  
                          |                                                                    | ■ Simplified cloud management  |
Table 2  Target Customers and Markets (continued)

<table>
<thead>
<tr>
<th>Segment Category</th>
<th>Description</th>
<th>Sample Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Assets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Fleets</td>
<td>Enterprises that use large fleets to deliver customer services as an extension of their business. Includes:</td>
<td>- Extend enterprise network to vehicles  &lt;br&gt;- Enterprise application integration using edge compute  &lt;br&gt;- Enterprise VPN termination and unified Wi-Fi policies</td>
</tr>
<tr>
<td></td>
<td>- Utilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Telco and cable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Specialized freight</td>
<td></td>
</tr>
<tr>
<td>Buses and Taxis</td>
<td>Enterprises that use vehicles as their primary means of service delivery. Includes:</td>
<td>- Growing range of in-vehicle services (such as ticketing, Wi-Fi, video entertainment, and video cameras)  &lt;br&gt;- Vehicle telemetry, performance tracking, and driver safety  &lt;br&gt;- Deploy and manage at scale with limited IT staff</td>
</tr>
<tr>
<td></td>
<td>- Bus companies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Taxi companies</td>
<td></td>
</tr>
<tr>
<td>Public Safety Vehicles</td>
<td>Cities and municipalities that use fleets of specialized vehicles for citizen and municipal services. Includes:</td>
<td>- Lives depend on an always-on connectivity  &lt;br&gt;- Frequent increase in vehicle devices (such as computers, dash cams, and sensors)  &lt;br&gt;- Multiple connectivity options (such as Single-LTE/Dual-LTE and Wi-Fi)</td>
</tr>
<tr>
<td></td>
<td>- Police vehicles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Ambulances</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fire trucks</td>
<td></td>
</tr>
</tbody>
</table>
Target Audience for the Cisco Remote and Mobile Assets Solution

This solution is available to current and prospective customers and partners. The main functional areas expected to consume this document are described in Table 3:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
<th>Sample Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Buyers</td>
<td>Select the optimal asset connectivity platform</td>
<td>1. Security and budget considerations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. A secure and scalable platform that meets current and future requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. An easy way to validate RFP requirements and build confidence in the solution</td>
</tr>
<tr>
<td>IT Managers and Architects</td>
<td>Select the optimal connectivity option to extend an existing enterprise network to geographically dispersed assets</td>
<td>1. For mobile assets, Wi-Fi integration with APs at stations/depots and operations in a variety of models such as Unified, Autonomous, and WGB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. FlexVPN for highly secure headend connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Consideration for different network availability scenarios and management of cellular backhaul for all availability modes, especially active and hot-standby</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Documentation of architectural options and recommendations to simplify design and implementation</td>
</tr>
<tr>
<td>Field Managers and Technicians</td>
<td>Responsible for all asset technologies and performance of the connected assets</td>
<td>1. Support for all asset connectivity requirements, including existing and future devices and applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Simplified asset deployment and router provisioning through zero-touch using a variety of tools such as cloud-based platforms and mobile phone apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Easy configuration and support for required network and security options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Documentation of workflows and best practices</td>
</tr>
<tr>
<td>Technology Operations and Support</td>
<td>Operation, support, and upgrade of asset technologies</td>
<td>1. Unified policy management and technology operation with a limited staff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Easy configuration of required network and security options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Simplified troubleshooting across multiple platform components and providers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Remotely push software updates including device, network, and security policies</td>
</tr>
</tbody>
</table>
Cisco Validated Design Overview

Since the inception of IP networking, Cisco Validated Designs (CVDs) have been used to validate, architect, and configure next-generation technologies—helping companies accelerate digital transformation, innovate faster, and stay competitive. This solution is no exception. The Cisco Remote and Mobile Assets solution CVD, which is documented in this Cisco Remote and Mobile Assets Design and Implementation Guide (DIG), provides a design foundation that incorporates a broad set of technologies, features, and applications. Every aspect has been thoroughly tested and documented, helping ensure deployment that’s faster, more reliable, cost effective, and predictable. You can expect:

- Standardized architecture templates and adherence to best practices.
- Designs and configurations to help integrate the IoT gateway with the enterprise headend to ensure secure, scalable, and highly reliable VPN connectivity.
- Best practices and guidance for choosing between Unified or Autonomous Wi-Fi modes and setting up your Workgroup Bridge (WGB).
- Advanced templates and automation scripts so you can configure specialized Cisco IOS features.

With constant change, there’s always a new frontier to explore and master, opening up vast potential for businesses if they have the right tools.

Technology Components

The Cisco Remote and Mobile Assets solution provides a powerful way to extend the network to geographically-dispersed assets using the simplicity of zero-touch gateway deployment using a LTE, Ethernet, or Wi-Fi connection while maintaining a robust security posture. This allows customers to treat fleet vehicles and field assets as a full extension of their corporate network with the same access to enterprise Wi-Fi and network services, automatic user authentication, access to enterprise applications, video and collaboration services, and a host of other features. All of this without requiring multiple LTE connections or repeated user authentication and without compromising enterprise security.

This document uses the terms “Industrial Routers” and “IoT Gateways” interchangeably to mean edge IoT network devices.

Architecture features are described in Table 4:

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Architecture Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Features</td>
<td>Benefits</td>
</tr>
<tr>
<td>Industrial Routers</td>
<td>Comprehensive network capabilities in a ruggedized form factor</td>
</tr>
<tr>
<td>Cloud-Based Management</td>
<td>Unified security, policy, and operations using existing staff</td>
</tr>
<tr>
<td>Multiple Connectivity Options</td>
<td>Optimize use of available backhaul and budgets</td>
</tr>
<tr>
<td>Enterprise Security and Controls</td>
<td>Secure edge and superior VPN performance with Cisco IOS® Software</td>
</tr>
<tr>
<td>Simplified Network Integration</td>
<td>Enterprise-class VPN and wireless with zero-touch gateway deployment</td>
</tr>
<tr>
<td>Edge Compute and Microservices</td>
<td>Integrated legacy protocols and data management at the network edge</td>
</tr>
</tbody>
</table>
Remote and Mobile Assets

Part I: Overview

Solution Building Blocks

The design consists of five building blocks with a comprehensive security wrapper. In addition to providing edge device authentication and security for the data and control planes, but it also far exceeds industry standards, ensuring that more aspects of the platform are secure.

Key Security Features

- Encrypted IPSec tunnel to provision and manage the edge gateways
- Certificate-based authentication during the gateway claiming process
- Secure connectivity from the edge gateways to the enterprise headend using FlexVPN
- IEEE 802.1X authentication for Wi-Fi connected endpoints with WPA2, PSK, or RADIUS-based authentication

Figure 2   Cisco Remote and Mobile Assets Building Blocks
Part I: Overview

Industrial Routers

From the harsh environmental conditions of a vehicle trunk to remote and dusty locations, the Cisco Industrial Routers are built for durability. The solution offers zero touch deployment (ZTD), ease of authenticating edge devices, GPS and gyroscope functionality, and suitability of antenna and power options. The design also considers in-vehicle requirements, such as ignition control and operation at high speeds. Finally, this document provides best-practice IOS configurations, enabling customers to program firewall, security, and QoS policies on the router.

Cloud Provisioning and Management

The secure, cloud-based Cisco Kinetic Gateway Management Module (GMM) application streamlines the provisioning process and provides browser-based visibility and control of routers and connected IP devices. The solution validates and documents the entire process, starting from when the routers are shipped out to their manufacturing configuration. This document includes best practices for claiming the router and configuring the routing policies and VPN options. Guidelines include integration with Cisco Control Center for SIM management, updating firmware, and troubleshooting in the field.

Network Integration

One of the biggest benefits of this solution is the availability of standardized templates for secure, seamless connectivity to the enterprise network. This includes designs and configurations for network VPN termination and sample scripts to automate setting up the FlexVPN. In addition, high availability and security policy options are included to maximize flexibility while demystifying even the most complex architectures. This allows simplified endpoint deployments without needing to configure endpoint VPNs.

Wi-Fi*

Cisco has deep experience in providing secure Wi-Fi networks and extending enterprise Wi-Fi policies to hotspots inside and outside vehicles. Cisco’s WGB technology connects vehicles to the station/branch’s Wi-Fi seamlessly and flawlessly. In addition, this document provides standardized Wi-Fi design and configuration templates, enabling the simplified selection of authentication modes that best meet the network requirements.

*IR829 only
Backhaul Options

The platform allows for selection of cellular, Ethernet, and/or Wi-Fi backhaul based on the use case, budget, and connection quality. The CVD provides guidance for configuring single or dual LTE connections in an active/active mode for mission-critical IoT applications. In situations of signal strength degradation, configurations for automatic failover to a standby connection are documented. It also includes best practices to ensure high security levels for both public or private APNs.
Part II: IT Design

This part is divided into the following chapters:

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Guidance, page 11</td>
<td>Guidance for selecting the most appropriate Industrial Router and the platform architecture based on use cases and requirements.</td>
</tr>
<tr>
<td>Security Overview, page 14</td>
<td>End-to-end security considerations, including securing the management plane, the data plane, and effective device security.</td>
</tr>
<tr>
<td>Industrial Routers, page 21</td>
<td>Information on the Cisco Industrial Router portfolio: key capabilities and best practices for setting up the router and its accessories.</td>
</tr>
<tr>
<td>Cloud Provisioning and Management, page 31</td>
<td>Details of Cisco Kinetic GMM with descriptions of key functional elements and best practices for using this platform.</td>
</tr>
<tr>
<td>Network Integration, page 41</td>
<td>Best practices and architectures for integrating the gateways with the enterprise network.</td>
</tr>
<tr>
<td>Wi-Fi, page 48</td>
<td>Best practices and architectures for enabling the Wi-Fi functionality on the IR829 and configuring the WGB.</td>
</tr>
<tr>
<td>Backhaul, page 55</td>
<td>Guidance for integrating the desired backhaul (LTE, Ethernet, or Wi-Fi), including redundancy options.</td>
</tr>
<tr>
<td>Prepare for Deployment, page 59</td>
<td>Key steps required to set up the GMM template, user accounts, and prepare an existing gateway to be claimed by GMM using the Cisco Gateway Provisioning Tool (GPT).</td>
</tr>
</tbody>
</table>

Technology Guidance

Figure 3  Cisco Remote and Mobile Assets–Solution Architecture
Figure 3 highlights the two primary components of the Cisco Remote and Mobile Assets solution—our portfolio of Cisco Industrial Routers (IRs) and Cisco Kinetic GMM:

- The Cisco IR portfolio consists of different models of hardened industrial grade gateways that can be installed with fixed and mobile assets. For mobile assets, the gateways are capable of providing non-stop vehicle connectivity and an in-built GPS to track the current and historical location of the mobile asset.

- Cisco Kinetic GMM is a cloud-hosted provisioning and management platform that enables ZTD and management of the edge routers. GMM establishes a secure IPSec management tunnel to each of the on-boarded routers for provisioning and managing the routers from a centralized cloud. If customers wish to extend their enterprise network to the edge IoT gateways, GMM provisions the FlexVPN tunnel from each of the edge gateways to the enterprise headend VPN router.

Getting started with the Cisco Remote and Mobile Assets solution requires two steps:

1. Selecting the Router, page 12
2. Designing Your Solution, page 13

Selecting the Router

Cisco offers a wide range of industrial routers to meet a range of requirements and budgets. To support selection of the best option, Table 5 lists some of the prominent features supported by each of the routers:

<table>
<thead>
<tr>
<th>Router</th>
<th>IR807</th>
<th>IR809</th>
<th>IR829</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Optimized for Low Power:</td>
<td>Compact Feature Rich:</td>
<td>Single/Dual LTE with Wi-Fi, Optional PoE and mSATA:</td>
</tr>
<tr>
<td></td>
<td>- Din Rail Mounting</td>
<td>- Edge compute</td>
<td>- Storage and Edge Compute</td>
</tr>
<tr>
<td></td>
<td>- Compact and rugged</td>
<td>- Panel Mounting</td>
<td>- Panel Mounting Ignition</td>
</tr>
<tr>
<td></td>
<td>- Low power consumption</td>
<td>- SCADA integration</td>
<td>- Power Management</td>
</tr>
<tr>
<td></td>
<td>- SCADA integration</td>
<td>- Utility Certifications</td>
<td>- Industrial and Automotive Certification</td>
</tr>
<tr>
<td></td>
<td>- Utility certifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Markets</td>
<td>Utilities</td>
<td>Utilities</td>
<td>Service Fleets</td>
</tr>
<tr>
<td></td>
<td>- Roadside and traffic</td>
<td>- Oil and Gas</td>
<td>Buses and Taxis</td>
</tr>
<tr>
<td></td>
<td>- Remote sites</td>
<td>- Remote sites</td>
<td>Public Safety Vehicles</td>
</tr>
<tr>
<td>Ports and Backhaul</td>
<td>2 Fast Ethernet</td>
<td>2 RJ45 routed ports (10/100/1000 Mbps)</td>
<td>4 RJ45 with switch ports (10/100/1000 Mbps)</td>
</tr>
<tr>
<td></td>
<td>- Single LTE (Dual SIM)</td>
<td>- Single LTE (Dual SIM)</td>
<td>- Single and Dual LTE (Dual SIM)</td>
</tr>
<tr>
<td></td>
<td>- 2 Fast Ethernet</td>
<td>- 2 RJ45 routed ports (10/100/1000 Mbps)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Single LTE (Dual SIM)</td>
<td></td>
<td>- Single and Dual LTE (Dual SIM)</td>
</tr>
<tr>
<td></td>
<td>- 2 Serial Ports (RS232 DTE and DCE/RS485)</td>
<td></td>
<td>- 2 Serial Ports (RS232 DTE and RS232 DCE/RS485)</td>
</tr>
<tr>
<td>Wi-Fi and WGB</td>
<td>None</td>
<td>None</td>
<td>802.11</td>
</tr>
<tr>
<td>Embedded Sensors</td>
<td>GPS</td>
<td>GPS</td>
<td>GPS, Gyroscope, Accelerometer</td>
</tr>
</tbody>
</table>
Remote and Mobile Assets

Part II: IT Design

Table 5  Industrial Router Options (continued)

<table>
<thead>
<tr>
<th>Router</th>
<th>IR807</th>
<th>IR809</th>
<th>IR829</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Compute</td>
<td>None</td>
<td>1 CPU for edge compute,</td>
<td>1 CPU for edge compute,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>767MB Memory</td>
<td>767MB Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50GB or 100GB mSATA storage on IR829M models</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>6.6w</td>
<td>19w</td>
<td>40w</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>70w with PoE option</td>
</tr>
<tr>
<td>Other Features</td>
<td>IP30, Fanless</td>
<td>IP30, Fanless</td>
<td>IP40 (IP54 enclosure available), Fanless</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shock and vibration proof</td>
</tr>
<tr>
<td>Dimensions and Availability</td>
<td>1.84 X 5.07 X 4.37 in North America and Europe</td>
<td>1.15 X 5.05 X 6.27 (Globally)</td>
<td>1.73 X 11 X 7.7 (Globally)</td>
</tr>
</tbody>
</table>

Designing Your Solution

Because of the flexibility of the Industrial Routers and the Kinetic GMM software, the Cisco Remote and Mobile Assets CVD describes a number of available options. Table 6 and Table 7 provide sample guidance for Basic Connectivity versus Advanced Connectivity to provide a flavor for the range of possibilities.

- The Basic Connectivity option provides basic Internet connectivity for edge device(s) behind the IR, with a focus on easy deployment and minimal requirements from the enterprise network.

- The Advanced Connectivity option provides more complex architectures for experienced customers desiring to use their edge gateways as a full extension of the enterprise.

All gateway configuration options shown throughout Part II of this document are implemented through Kinetic GMM templates. Table 6 and Table 7 are examples that demonstrate the range of design options available through GMM. Actual customer requirements should drive the technology decisions since those use cases may look different from the options shown below.

Although Cisco IOS provides many more options and features, these are outside the scope of this document. Mixing GMM and manual configuration is not recommended.

Table 6  Remote Assets Use Case

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Basic Connectivity</th>
<th>Advanced Connectivity, including Edge Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR807</td>
<td>Single Cellular</td>
<td>Single Cellular</td>
</tr>
<tr>
<td></td>
<td>Single SIM</td>
<td>Dual SIM</td>
</tr>
<tr>
<td></td>
<td>Wired FastEthernet</td>
<td>Wired GigabitEthernet</td>
</tr>
<tr>
<td>WAN backhaul</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edge device connectivity</td>
<td>Wired FastEthernet</td>
<td>Wired GigabitEthernet</td>
</tr>
<tr>
<td></td>
<td>Serial</td>
<td>Serial</td>
</tr>
<tr>
<td>Outbound connectivity from gateway</td>
<td>Public APN for Cellular, access to any resource exposed to the Internet</td>
<td>Private APN or Public APN + FlexVPN, access to enterprise (and Internet)</td>
</tr>
<tr>
<td>Inbound connectivity to gateway and edge devices</td>
<td>Kinetic GMM Remote Access</td>
<td>FlexVPN Site-to-Site Tunnel</td>
</tr>
</tbody>
</table>
Security Overview

Introduction to IoT Security

IoT Security emphasizes safeguarding the connected devices and the networks. Using a comprehensive security architecture will optimize protection from potential vulnerabilities. A security-centric IoT design helps ensure that every element of the platform is secure starting from the authentication of edge devices. This helps ensure secure device access and provides multiple secure connectivity options, which help ensure protection of enterprise data. End-to-end solution-level security goes much deeper than product standards compliance. Each layer of the IoT architecture must be secured by ensuring security of both the management plane and the data plane.

Management Plane Security

- Use of an encrypted IPSec Tunnel to provision and manage the edge gateways.
- Certificate-based authentication during the gateway claiming process.
- GMM Web-UI Two-Factor Authentication.
Remote and Mobile Assets

Part II: IT Design

Data Plane Security

- Secure connectivity from the edge gateways up to the enterprise headend using FlexVPN to establish encrypted tunnels using IPSEC and IKEv2.
- Support for Cisco AnyConnect VPN and Port Forwarding to enable secure remote access to devices behind the gateway via VPN from outside the firewall.
- WPA2-protected Wi-Fi with Pre Shared Keys (PSK) or RADIUS-based authentication.

Gateway and Device Security

- Use of 802.1x to authenticate wireless clients.
- Gateway functionality to enforce image signing and secure boot.
- Please refer to IoT Gateway and Device Security, page 18 for additional recommendations regarding Cisco IOS firewall features.

Securing the GMM Management Plane

The cloud-hosted Cisco Kinetic Gateway Management Module (GMM) offers the following security elements:

Encrypted IPSec Tunnel

The provisioning and management of the edge gateways all occur over encrypted IPSec tunnels to ensure secure communication between GMM and the gateways.

Certificate-based Authentication

The registration and claim process between GMM and the gateways is secured via a certificated-based authentication process. This helps prevent spoofing of the gateway and against man-in-the-middle attacks where an external server claims to be acting on behalf of a legitimate GMM server.

GMM Web UI Two-Factor Authentication

Usernames and passwords are no longer a safe security method for your online accounts. Data breaches occur daily, and hackers are always inventing new ways to take over your accounts. GMM supports 2-Factor Authentication on its Web-UI to provide an extra layer of security. Users first enter their username and a password, and are then required to provide their One-Time Password (OTP) that is sent to a different device.

Cisco GMM Cloud Security—Please refer to the Cisco Kinetic Security White Paper that documents the GMM Cloud Security Architecture, best practices, and considerations at the following URL:

Securing the Data Plane

Introduction to IPSec VPNs

Virtual Private Networks (VPNs) are designed to securely and inexpensively extend the reach of corporate networks. Several options have been built on top of IPSec, a framework that deals with the tasks of ensuring Confidentiality, Integrity, Authentication (CIA) of origin and secure key distribution for VPNs.

Some of the notable strengths of IPSec are its independence from the transport layer (UDP, TCP or raw IP) and the easy replacement of one or more of its components (such as the hash functions and cryptographic algorithms) so that it can withstand brute force attacks while keeping up with evolution of the hardware.

The Cisco IOS software offers multiple VPN options including Classic IPSec, IPSec/GRE, Virtual Tunnel Interface (VTI), EasyVPN, and Dynamic Multipoint VPN (DMVPN). Each of these technologies were developed to solve specific problems:

- Crypto Maps are the initial/legacy solution devised before IPSec was an RFC. Although the services available are very basic, they do help with interoperability.
- VTI brings a logical interface to IPSec deployments without needing to use Generic Routing Encapsulation (GRE).
- EasyVPN allows branch routers (or other types of VPN appliances) to behave as hardware clients that are centrally configured by a VPN concentrator.
- DMVPN provides the capability to dynamically establishing tunnels between spokes on a hub-and-spoke scenario.

<table>
<thead>
<tr>
<th>VPN</th>
<th>Inter-Op</th>
<th>Dynamic Routing</th>
<th>IPSec Routing</th>
<th>Remote Access</th>
<th>Simple Failover</th>
<th>Source Failover</th>
<th>Per-peer config</th>
<th>Per-peer QoS</th>
<th>Full AAA Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMVPN</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>group</td>
</tr>
<tr>
<td>Crypto Map</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Poor</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FlexVPN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The Cisco Remote and Mobile Assets solution uses IPSec-based FlexVPNs rather than SSL-based VPNs. Since it is application agnostic, IPSec can support a number of legacy protocols and traditional client/server applications with minimal effort. This is not the case with SSL VPNs, which have been built around Web-based applications. As a result, SSL VPN-based options like OpenVPN could severely limit the security and network options for remote and mobile assets by requiring always-on connectivity to the headquarters.

Introduction to FlexVPN

FlexVPN is a framework for configuring IPSec VPNs on Cisco IOS devices. It was created to simplify the deployment of VPN solutions of all types (such as Hub-and-Spoke, Spoke-to-Spoke, Site-to-Site, and Remote Access implemented through EasyVPN, DMVPN, and Crypto Maps).

- **FlexVPN requires use of version 2 of the Internet Key Exchange protocol (IKEv2), which is a more secure option than the original implementation (IKEv1).**
- **IKEv2, by design, is not backward compatible with IKEv1 since it provides increased security. IKEv2 requires reconfiguration of all IPSecVPNs.**
Benefits of using FlexVPN

- **Built on IKEv2**—IKEv2 is more secure than IKEv1 because it supports the latest Suite B cryptographic algorithms. IKEv2 has built-in support for Dead Peer Detection (DPD) and NAT-Traversal. It is also resistant to DoS attacks.

- **Ease of Configuration**—Easy to configure using IKEv2 smart defaults; no need to define policies, transform sets, etc., since IKEv2 has built in defaults.

- **Cost-Effective**—The FlexVPN Hub-and-Spoke design does not require NHRP (unlike DMVPN). This reduces WAN bandwidth utilization and costs due to reduced Control Plane traffic.

- **Support for Hardware Encryption**
  - **IKEv2 Stability**—It automatically resumes working as normal after a temporary interruption of your connection, such as a power outage or entering a real-world tunnel.
  - **IKEv2 Route Advertisement**—Another cost benefit is IKEv2’s ability to advertise routes during tunnel negotiation, which helps reduce chatty control messaging that can eat up data plans.

- **Centralized Policy Control**—VPN dynamic policies such as split-tunnel policy, encryption network policy, Virtual Route Forwarding (VRF) selection, and Domain Name System (DNS) server (for remote access) can be fully integrated with the authentication, authorization, and accounting (AAA)/RADIUS server and applied on a per-peer basis.

- **Support for High Availability and Scalability**—In this solution architecture, we propose using IKEv2 Load Balancing, which relies on HSRP between the hubs to allow for scaling to higher than 10,000 sessions. All HSRP members are part of a cluster with one of the hubs active while others are in standby mode. The active hub sends IKE redirect messages to hubs with lower utilization.

- **Support for Multi-Cast Traffic**—GRE encapsulation allows multicast applications, including dynamic routing protocols, to traverse the tunnel without needing NHRP on the headend router (HER).

- **IPv4 and IPv6 Support**—Backward compatible as well as future proofed for IoT IP addressing requirements.

- **Flexible AAA Options**—Authentication and Authorization may be performed by means of a local database or using RADIUS (more convenient for Service Provider environments, which typically require multi-tenancy).

- **Dynamic Tunnel Configuration**—This has been simplified so that theoretically only a single interface template would be required on the Hub site to allow all types of incoming VPN connections.

FlexVPN supports hardware encryption, which is offered by most Cisco products to optimize VPN performance. This provides exponentially better throughput vs software encryption.

FlexVPN requires the use of the version 2 of the Internet Key Exchange protocol (IKEv2), a more secure option than the original implementation (IKEv1).

Private vs Public Access Point Names

Public Access Point Names (APNs) are the default Internet connectivity for cellular gateways. Some customers purchase Private APNs from their cellular carriers. A Private APN may either be a dedicated APN for a customer or just a "virtual one," meaning that all traffic coming over the radio network is examined to identify the device cellular ID, enabling this traffic to be routed to the Private APN (similar to an ACL for the data). In most cases, the data traverses the public Internet to get to the network. This will always introduce the possibility for security violations.

Cisco recommends the use of FlexVPNs for Private APNs since this provides end-to-end encryption to ensure that no man-in-the-middle can view enterprise network resources.
IoT Gateway and Device Security

The Cisco Remote and Mobile Assets solution allows greater flexibility for end user devices connected to the Cisco Industrial Router. Since the gateways support secure connectivity with technologies such as FlexVPN and WPA2 with IEEE 802.1x authentication, security policies can be enforced on the gateway instead of relying on the edge devices (such as laptops, phones, tablets, and video cameras). Allowing users to connect and authenticate the same way as in the office increases acceptance and efficiency.

Best Practice:

- While the solution is generally edge-device agnostic, Cisco suggests that wireless devices connect via IEEE 802.11n (or better) and wired devices connect over FastEthernet or Gigabit Ethernet.
- Using WPA2 with PSK or 802.1x authentication for wireless devices ensures that an end device is what it claims to be. This greatly enhances security by allowing 802.1x to accept or reject users who want full access to a network.
- Leveraging network-based VPNs increases the range of edge device options and simplifies security management. Software-based VPN clients on each edge device can be cumbersome to manage and require computing overhead to encrypt and decrypt data, resulting in a diminished user experience.

IEEE 802.1X Authentication for Wireless Clients

Any typical TCP/IP network that uses DHCP is defenseless against individuals who can find an unsecured network drop. The DHCP server could grant an IP address to unauthorized end devices, which would enable an attacker to launch a variety of attacks such as breaking into specific servers, eavesdropping on network packets, or unleashing a worm or a Denial of Service (DoS) attack. IEEE 802.1x provides a solution for such problems. By authenticating user access at the network edge, network administrators can be assured that no unauthorized access will take place, and all user authentication can take place on a centralized authentication server like a RADIUS server deployed at the enterprise headquarters.

Cisco ISE can be used as an alternative to Open RADIUS. For further information, please refer to:

Remote and Mobile Assets

Part II: IT Design

Hardware Encryption

The Cisco IRs offer hardware-accelerated encryption to support a full range of security services such as hardware cryptography to significantly increases IPSec VPN performance. This allows using Cisco’s Next Generation Encryption (NGE), which evolves traditional encryption technology to meet today's increasing security needs while improving scalability and efficiency. Figure 4 shows the list of technologies that are included in NGE.

Figure 4 Hardware Encryption Features on the Industrial Router Platforms

ACT2: Hardware Root of Trust

The ACT2 chip is a security device containing product identity information and assertion functionality to support product identity for anti-counterfeit, secure storage and other security functions. Key capabilities include:

- Anti-Theft and Anti-Tamper chip designed only for Cisco products.
- Secure Unique Device Identifier (SUDI) and a certificate chain (X.509) that can be provisioned only at manufacturing. Linking the installed certificates and the ACT-2 chip provides the data needed for assertion and reconciliation by tracing the chip from creation to completion of the Identity Insertion Process.
- Secure storage for certificates and objects used for encryption/decryption and other identities.
- Certifiable entropy for random number generation of one-time token/private key ensuring that no two gateways end up with the same set of private keys and SSH keys.

Image Signing and Secure Boot

Image signing ensures that, at every instance, the software stack, including the boot loader and OS stack, is authentic and has not been tampered with or manipulated. It provides software integrity against any back door image modifications.

- The golden bootloader image is always in a permanent read-only boot flash that is encapsulated in epoxy and has the tamper evident label signed.
- Field-programmable gate array (FPGA) boot loader images are signed so that they can be validated by Cisco Secure Boot using burnt-in certificates in ACT2.
- Protects system boot sequence against changing boot sequence, booting from alternate device, bypassing integrity check, and adding persistent code.
- Each step of the software booting is authenticated by the previous stack to ensure end-to-end integrity.

For more information about Cisco Next Generation Encryption, please refer to the following URL:

Other Security Best Practices

- A major issue cited with IoT security is the use of hard-coded or default passwords, which can lead to security breaches. Even if passwords are changed, they are often not strong enough to prevent infiltration. Ensure that passwords within your IoT infrastructure are changed frequently and that the change is enforced on a recurring schedule. Enforce the use of strong passwords.

- Many IoT devices are “set and forgotten.” For example, they are deployed and left until their end of life with no security updates or patches. Ensure that all the necessary security patches and updates are applied to all elements within your network IoT fabric.

- Encrypt any sensitive data both in transit and at rest between IoT edge devices and backend systems using standard cryptographic algorithms. This will help maintain data integrity and prevent data sniffing by hackers.

- All encryption must be accompanied by an encryption key lifecycle manage process, since poor key management will reduce overall security.
Industrial Routers

This section describes the Cisco IR portfolio and their hardware and networking features. When evaluating specific hardware or software features in this section, refer to the icons below that indicate which of the three Industrial Router platforms support the described feature.

IR807  IR809  IR829

The Cisco Industrial Router Portfolio

Cisco IR807 Ruggedized Gateway

The Cisco IR807 is a compact multimode 3G and 4G LTE wireless router. It provides an ideal solution for power-constrained needs for remote asset management across industry segments such as distribution automation and other energy applications.

Figure 6  Cisco IR807 Ruggedized Gateway

Dimensions: 1.84” x 5.07” x 4.37” (H x W x D) (46.74 x 128.78 x 110.99 mm)

Temperature: -40°C to +60°C

Cisco IR807 Datasheet:

Cisco IR807 Hardware Installation Guide:
Cisco IR809 Ruggedized Gateway

The IR809 is Cisco’s smallest multimode 3G and 4G LTE wireless router, making it an excellent solution for remote and mobile asset use cases that require a full featured router with edge compute that needs to fit into a very constrained space.

**Figure 7** Cisco IR809 Ruggedized Gateway

**Dimensions:**
- 5" x 6.25" x 1.25" (DxWxH)

**Temperature:**
- -40°C to +60°C

**Cisco IR809 Datasheet:**

**Cisco IR809 Hardware Installation Guide:**
**Cisco IR829 Ruggedized Gateway**

The IR829 is Cisco’s flagship IoT gateway, purpose built for deployment on-board a vehicle. The optional Dual-LTE feature provides multi-path LTE and/or WAN backhaul for mission-critical IoT initiatives requiring highly secure data delivery, edge application execution, and redundant connectivity. With two LTE modems, the IR829 can concurrently connect to two cellular networks for high reliability, enhanced data throughputs, load balancing, and differentiated services.

*Figure 8: Cisco IR829 Ruggedized Gateway*

- **Key features of the IR829 include:**
  - Seamless switching between wireless networks without manual intervention to ensure transparency to users. Devices (laptops, smart devices, sensors, and cameras) and applications maintain continuous connectivity as the WAN links change.
  - Allows an entire mobile network or subnet to stay connected since the dual-radio 2.4GHz and 5 Ghz WLAN can serve as both clients and access points.
  - Track vehicle fleets through the built-in GPS systems.
  - Dual Subscriber Identity Module (SIM) support for reliability and multi-homing capabilities over LTE and HSPA-based networks. The two SIMs operate in active/backup mode on the single LTE models of the IR829. On the Dual-LTE IR829, the two SIMs can operate in active/active mode with each of the SIMs assigned to different cellular carriers.

**Cisco IR829 Datasheet:**

**Cisco IR829 Hardware Installation Guide:**

**Dimensions:**
- 7.7”x11”x1.73” (DxWxH)

**Temperature:**
- -40°C to +60°C

---

**Dual SIM active/backup mode is supported only on single LTE models of the IR829.**
Select Hardware Features

Choice of Antennas

All Cisco hardware offer a wide range of antenna options to support the use case requirements. Best practices for antenna installation include:

- **Offers** MIMO on LTE. Without MIMO, WCDMA, UMTS, HSPA, and DC-HSPA+ are only possible for diversity. In the case of 3G UMTS, a solo antenna limits switching to the diversity port.

- Install the router with two antennas (Main and Aux) to guarantee the best performance level. A single antenna may affect downlink performance by more than 3dB, and by as much as 20dB because of multipath fading (destructive interference between direct and reflected radio waves).

- Poorly installed MIMO antennas that have a strong correlation coefficient between the antennas may cause the two streams to interfere with each other since the system will have trouble separating the streams (lack of diversity). We recommend the use of multi-element antennas (5-in-1, 3-in-1, 2-in-1) since they have good diversity.

- On the IR829, ensure physical spacing between antennas for RF isolation between different radios. The router requires a guaranteed >15dB (ideally 20-25dB) isolation between Wi-Fi and LTE antennas to ensure optimum performance.

For antenna selection and installation for the different gateways (Cellular Antenna, WLAN Antenna - 5 Ghz, WLAN Antenna - 2.4GHz), please refer to the *Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide* at the following URL:


To help with antenna selection, refer to the *Antenna Selection Table* at the following link:


**SIM-based Auto-Carrier Selection (AutoSIM)**

- The routers automatically detect the active SIM and configure its modem for the appropriate cellular carrier when an active SIM is inserted and it is powered up. This provides a number of benefits including:
  - Simplified configuration and reduced setup time
  - Single SKU for all carriers
  - Simplified procurement, reduced inventory complexity, and simplified deployments
Figure 9  Industrial Router Auto SIM

Gyroscope / Accelerometer

The IR829 includes a built-in gyroscope and accelerometer that can detect linear acceleration and angular movement. This functionality could potentially be used to detect equipment tampering or assist in automotive applications where movement is involved. Devices connected through the serial port can access the accelerometer and gyroscope data through the IOS CLI or IOx. These routers will, by default, take an accelerometer and gyroscope reading every second, but this can be changed to once every 6 seconds, or once every 60 seconds.

SSD Storage

The IR829-M models offer the option for an mSATA Solid State Disk that is available in 50 and 100 GB capacities. This replaces the 4 GB of disk storage available in other IR829 models and is only visible and usable in IOX (not the IOS part of the router). Once the module is installed, no additional configuration is needed to use the extra disk space. Since this module is not hot-swappable, the router will need to be powered off before installing the module.

For additional information on the mSATA SSD module, refer to mSATA SSD as Additional Storage at the following URL:

The Ignition Power Management feature helps keep the IR829 gateway up and running, without draining the vehicle battery, while the vehicle is stopped. Because of this, users do not have to wait for routers to boot-up each time the vehicle is stopped:

- **Zero boot up time (no cold start)** because the platform stays powered up for a pre-determined period of time when the vehicle engine is turned off. The pre-determined period is programmable between 60 to 7200 seconds (2H00) using the IOS ignition off-timer command.

- **Energy management** by allowing user to program automatic power-down of the router when the vehicle battery drops below a certain voltage threshold.

- **Vehicle power fluctuations** can be mitigated since the IR829 withstands the cold crank down to 6V for a period of time specified in the ISO-7637-2.

- **IOS-based discharge management** to prevent battery discharge by turning the router off if the vehicle has the ignition off for a period of time (programmable) and protects the router by turning the router off if the battery voltage rises above a certain level (fixed amount of time).

- **Automatic event logging** including ignition state (on or off), ignition-off timer expiry, features enabled or disabled through the CLI, and under-voltage and over-voltage events.

*Figure 10  Ignition Power Management Features*
Virtual Routing and Forwarding

If your enterprise network falls in the IP address range 10.0.0.0/8, Virtual Routing and Forwarding (VRF) will be required to create a separate routing instance on the gateway since these IP addresses overlap with the IP addresses for the Kinetic infrastructure. We recommend one of the following options to avoid routing conflicts:

**Routed Mode with VRF**

We recommend VRF without NAT (routed mode) if you want two-way connectivity between subtended devices and the enterprise network.
**Remote and Mobile Assets**

**Part II: IT Design**

Figure 12  **Routed Mode with VRF**

Gateway uses Global Routing Table to reach 10.0.0.0/8 on GMM

- **Global Routing**
- **VRF Routing**

Gateway uses VRF routing table to reach 10.0.0.0/8 on Enterprise

Figure 13  **NAT Mode with VRF**

Enable VRF in conjunction with NAT (Site-To-Site VPN) if you only require one-way communication from the subtended devices and the enterprise network. This will create a separate routing instance for the device.
GMM offers several options for IP addressing of the LAN network behind the managed IR8xx gateway. These options can generally be divided into "routed" and "NAT" modes:

**Routed Mode**

In routed mode, the subnetwork assigned to the VLAN 1 is advertised over the FlexVPN tunnel to the enterprise HER using IKEv2 during the tunnel negotiation. This will allow the devices on the LAN behind the gateway to be directly reachable without the need for NAT or port forwarding.

**NAT Mode**

In NAT mode, the LAN subnetwork can be the same for many gateways, since the inside (VLAN 1) network addresses (VLAN 1) will be translated to the outside address (Cellular or Tunnel 2). This option makes the most sense when outbound connectivity from LAN devices to the Internet or enterprise is the primary use case and access to LAN devices is not required or is very limited.

**Best Practices for using Routed Mode include:**

- Ensure that the subnet assigned to a gateway’s LAN is unique and does not overlap other routes in the enterprise network. If you need to use address space for the LAN that overlaps with the networks assigned by GMM, the VRF feature can put the LAN (VLAN 1) and Cellular interfaces in a different routing table from the loopback and tunnel interfaces used by GMM.

- Set LAN devices to point to the gateway as the DNS server or alternatively enable the VRF functionality in GMM. This helps avoid a situation where DNS requests sent from the LAN to Google DNS (8.8.8.8) will be forwarded over the Cellular interface directly, instead of through the FlexVPN tunnel. If packets are sent out the Cellular interface, but are sourced from an IP other than that assigned to the Cellular interface; it can cause the Cellular interface to flap up and down since the carrier may tear down the connection as a security mechanism to prevent unexpected traffic.

**NAT Mode**

In NAT mode, the LAN subnetwork can be the same for many gateways, since the inside (VLAN 1) network addresses (VLAN 1) will be translated to the outside address (Cellular or Tunnel 2). This option makes the most sense when outbound connectivity from LAN devices to the Internet or enterprise is the primary use case and access to LAN devices is not required or is very limited.

**Remote Access to Devices Behind the Gateway**

Access to devices behind the gateway can be performed in several ways, depending on the deployment model. The management tunnel that is created and used by GMM for all its monitoring and management functions can also be used to access the gateway by first logging into the Kinetic GMM management VPN with a Cisco AnyConnect client. Once connected to the VPN, the router and subtended devices are accessible directly. Access to LAN devices in this scenario requires the LAN subnetwork to use GMM-assigned addresses that are advertised (and reachable) through the Kinetic GMM HER (not the Enterprise Site-to-site VPN).
If a custom subnet is used instead of the Kinetic GMM-assigned subnet, then a site-to-site VPN to the enterprise HER must be created to access the LAN devices. In this scenario, both NAT and routed modes can be used. NAT mode must be used in conjunction with the port forwarding feature to access specific ports on specific LAN devices. When using routed mode, the LAN subnet will be advertised over the enterprise site-to-site VPN tunnel and will be reachable directly from within the enterprise.

When using cellular connectivity with a Private APN that provides direct access to the enterprise network, Cisco recommends using a site-to-site FlexVPN over the Cellular connection. This provides more robust security that uses end-to-end encryption and also enables the GMM template to provision the Port Forwarding (with NAT) or Routed Mode. This feature is only available when used with site-to-site VPN.
Remote and Mobile Assets

Part II: IT Design

Cloud Provisioning and Management

This section covers the provisioning and management of the gateways including:

**Provisioning:**
- Claiming and grouping the gateways
- Gateway states and configuration using templates
- Use of the Cisco Kinetic GMM Mobile App

**Management:**
- Enabling GPS
- Managing access to GMM including remote management using VPNs
- Upgrading the gateway firmware and using GMM APIs
- Custom configuration templates for IOS Features
- Gateway monitoring
- Integration with the Control Center

GMM uses many different networks in the 10.0.0.0/8 range that are integral to managing gateways. Because of this, if any potential destination networks exist in the 10.0.0.0/8 range, it is best practice to enable VRF and Routed Mode for the custom subnet. This ensures that the GMM traffic and the customer traffic do not mix.
Introduction to Cisco Gateway Management Module

The Cisco Kinetic Gateway Management Module (GMM) provides a secure cloud-hosted gateway provisioning and management platform to help manage gateways securely and cost-effectively at scale. The cloud-hosted GMM streamlines provisioning and provides you with ongoing visibility and control of your Cisco IRs from your browser.

Figure 17  GMM Capabilities

GMM helps you drastically reduce gateway on-boarding time with a simple three-step process:

1. Power up the gateway with the WAN cable plugged-in or use a cellular connection to call home to the cloud-hosted GMM.

2. Enter the gateway’s serial number into the Cisco Kinetic GMM dashboard to securely "claim" it.

3. Select from your library of templates to automatically configure the gateway.

The entire process involves ZTD. No network engineer is required to be on-site. Any non-IT field resource can power up the gateway and ensure that it has a connection; the rest is handled by GMM. Bulk operations can be applied to handle volume provisioning for even greater efficiency. Once on-boarded, the gateway can also be managed using GMM.

Benefits of GMM include:

- Supports IR807, IR809, and IR829
- Allows customer to bring new gateways online in minutes instead of days with low-touch provisioning
- Allows gateways to be viewed and controlled remotely from a secure cloud-based dashboard
- Reduces upfront deployment and ongoing operational and maintenance cost
- Allows for real-time status view, so issues can be identified and resolved in timely manner
- Available in 2 Geos (US and EU)

For a high-level overview of GMM please refer to:

- [https://developer.cisco.com/docs/kinetic/#!gmm-overview/gmm-overview](https://developer.cisco.com/docs/kinetic/#!gmm-overview/gmm-overview)

For an overview of the GMM Architecture and its components please refer to:

Provisioning

Claiming your Gateways

Figure 18 depicts the claiming process of the gateway with GMM.

Please pick one of the two following deployment options based on your deployment:

- **Greenfield Deployment**—Greenfield deployments cover new IRs ordered from Cisco. When the gateways are ordered with their respective license and subscription, they are prepared and provisioned at the factory for ZTD.

  **Note:** Cisco recommends Greenfield deployments. The step-by-step process to claim the gateways can be found at
  - https://developer.cisco.com/docs/kinetic/#!claim-gateways

- **Brownfield Deployment**—Brownfield deployment cover the re-purposing of previously purchased gateways by allowing customers to order only the additional GMM license and subscription. To do this, the gateway should be factory reset using the Gateway Provisioning Tool (GPT) before it can be claimed by GMM. A support request will also need to be sent to GMM using the Cisco Kinetic portal to enable the gateway to be GMM managed.

For more information on provisioning a gateway using GPT, please refer to:


Please refer to the ordering guide for information on ordering gateways, licenses, and software subscriptions at the following URL:

Authentication during the Gateway Registration and Claim Process

The following three certificates are involved in the initial registration and claim process:

- The gateway’s own certificate that comes pre-installed on the gateway when it is shipped by Cisco manufacturing. This certificate is signed by Cisco.
- GMM Management Tunnel Certificate which is signed by Comodo certificate authority.
- Self-signed GMM certificate.

The Management Tunnel setup and Gateway Management certificates are both installed by Cisco Manufacturing if the gateways were ordered as part of the Kinetic bundle, or they can be installed during the GPT process for existing gateways.

Initial Registration and Claim Process

1. During the initial registration process, the gateway first calls home to the cloud-hosted Cisco Kinetic GMM server. During this process, a basic TLS handshake occurs where the gateway requests the GMM server certificate to validate the server. This helps prevent any man-in-the-middle type of attacks where a rogue server acts as the GMM server.

2. Next, the GMM server requests the Cisco-signed gateway certificate. GMM uses this to validate the gateway to ensure that it is a valid Cisco gateway and not a rogue device.

3. Once the Cisco-signed certificate has been validated by GMM, the server extracts the serial number and the gateway model number embedded as part of the certificate. This also helps validate that it is a valid gateway with the correct serial number and gateway model and helps establish that the gateway is indeed legitimate and can be trusted.

4. Once this is done, a secure IPSec management tunnel is established between GMM and the gateway.

5. Next, the gateway and the GMM server perform a basic TLS handshake. Here again the gateway requests and validates the Gateway Management server certificate and the server requests the gateway’s certificate to help establish that both the gateway and the server are legitimate by verifying their identity.

6. The Gateway Management certificate being a self-signed certificate is not seen as a major issue since this exchange happens within the context of the secure IPSec Management tunnel.

Grouping your Gateways

A useful feature of GMM is its ability to grouping of gateways based on their purpose such as asset type, location, or any other user-defined category. This allows gateways to be grouped and filtered based on their tags. This can then be used to apply certain specific configurations to a certain set of gateways, perform upgrades to sets of gateways, view status by group, etc.
Gateway States and Configuration

A gateway undergoes several state changes as it moves from Out-of-box to Operational.

**Figure 19  GMM Edge Gateway Lifecycle**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kinetic Startup</td>
<td>Kinetic gateway that is received from manufacturing, or Kinetic gateway that has been factory reset or a standard IR809/IR829 gateway that has been converted to a Kinetic gateway using GPT tool.</td>
</tr>
<tr>
<td>1st Claim</td>
<td>First time the gateway is claimed from &quot;Kinetic Startup&quot; state. Gateway hard code the WAN (uplink) from configuration template to the boot up configuration as the &quot;Kinetic Base&quot; state. Note: WAN configuration on configuration template is only used in initialization.</td>
</tr>
<tr>
<td>Kinetic Base</td>
<td>Base state with cloud default configuration. Calls home to cloud – waits to be claimed.</td>
</tr>
<tr>
<td>Claim</td>
<td>Initiate Kinetic configuration process. Claim is executed using &quot;add gateway&quot; function on the Kinetic gateway page.</td>
</tr>
<tr>
<td>Operational</td>
<td>Gateway is operating as configured.</td>
</tr>
<tr>
<td>Unclaim</td>
<td>Delete the gateway from the Kinetic. Unclaim is executed by the &quot;delete gateway&quot; function on Cisco Kinetic gateway page. Gateway returns to &quot;Kinetic Base&quot; configuration and waits to be claimed.</td>
</tr>
<tr>
<td>Fallback</td>
<td>An operational gateway will fall back to &quot;Kinetic Base&quot; state when it misses 4 consecutive heartbeats from Kinetic. Gateway will automatically move to the &quot;Operational&quot; state again once connectivity is restored.</td>
</tr>
<tr>
<td>Factory Reset</td>
<td>To hard factory reset the gateway to factory default.</td>
</tr>
</tbody>
</table>

For further details about this process of transition for the gateway, please refer to the following URL:

Template-based Configuration

Templates are used to define a gateway's network settings, allowing the same template to be applied to multiple gateways. These templates are applied when the gateway is claimed or deployed. Templates can also be used to change a gateway's configuration by applying a new template to an existing gateway. The default templates can also be defined or modified through the use Custom Configuration Templates.

Custom Configuration Templates for IOS Features

Although Kinetic GMM provides easy-to-use templates that cover many of the most commonly used features and use cases, some customers may require additional functionality. The Custom Configuration Templates feature unlocks the full IOS feature set and makes it available for customized configurations. This powerful feature allows IOS commands to be pushed down to the gateway, thereby enabling advanced configurations that are not available through the standard GMM templates.

Although the configurations possible with Custom templates is nearly endless, some common examples have been included in Part IV: Sample Configurations, page 78. These include:

- Firewall (access-lists) configurations for restricting access to specific applications or networks
- Quality of Service
- Ignition Management
Since the Custom Configuration Templates allow for any IOS command, they can very easily modify the working configuration required for GMM, or compromise the security of the device. This feature, which should be exercised with care, is only available through the Kinetic Help feature in the GMM portal to ensure review by the GMM support team.

**Best Practices for use of Custom Configuration Templates:**

- Does not change any configuration related to CGNA
- Does not use/modify/delete the "admin" or "operator" user
- Does not use/modify/delete profile names "Flex_IKEv2" or "CVPN_I2PF"
- Does not use/modify/delete tunnel interface numbers 1 or 2
- Does not use/modify/delete tracking object numbers 2 or 4
- Does not use/modify/delete dialer number 1, dialer-list 1 or Virtual-Template1
- Does not use/modify/delete VLAN 555
- Does not use/modify/delete route-maps "RM_Tu2" or "RM_WAN_ACL"
- Does not use/modify/delete ACL names "NAT_ACL", "GWIPS"

Once the Custom Configuration Template is approved and made available in GMM, it appears as a standard template (like any other feature). This allows customers to select the template and input the required variables.

**Figure 20  Selecting the Template**

![Advanced Template](image)

**Important Note:**

Once an Advanced Template has been applied to a device, the configuration cannot be removed or modified. If changes need to be made, the device will have to be removed and reclaimed by GMM. Since Cisco cannot own or validate the impact of the Custom Template on the customer network, the customer bears full responsibility for these configurations.

More information on Advanced Templates can be found at:

- [https://confluence-eng-sjc5.cisco.com/conf/display/GSG/Flexible+Gateway+Template](https://confluence-eng-sjc5.cisco.com/conf/display/GSG/Flexible+Gateway+Template)
Remote Management using VPN

Customers can use the Cisco AnyConnect client to remotely manage and interact with devices behind the gateway. For example, an elevator technician could create a VPN between his PC and an elevator in another city. This would allow remote diagnostics to troubleshoot issues, determine a solution, or dispatch a repair technician with the right parts for that issue.

For more details on Remote Management using VPNs, please refer to:


We recommend using a VPN with an IP device that uses DHCP and is directly connected to the gateway. Devices with a static IP address require a custom gateway configuration.

Upgrading the Gateway Firmware

A useful feature offered by GMM is cloud-hosted remote firmware upgrades for the gateways. Firmware builds are hosted in the cloud and upgrades are made available online, triggered using GMM. You can schedule upgrades or trigger them immediately. An upgrade is available if displayed under **Firmware Upgrades**.

The upgrade process takes up to 2-1/2 hours. The firmware image is first downloaded to the gateway and then installed. The gateway will be down during the installation and unavailable for data delivery. Factory resetting a gateway restores the gateway to its original firmware version. The remote firmware upgrade procedure is then used to upgrade the gateway to the latest version.

For more details on gateway firmware upgrade, please refer to the following URL:


Using GMM APIs

Customers can integrate GMM functionality with their own Management and Provisioning system using RESTful APIs rather than using the GMM UI. An example of this is available in **Appendix, page 107**, which contains a Python Script for HER configuration that queries the Kinetic GMM API to obtain a list of serial numbers of gateways. The script subsequently generated an IOS configuration for the VPN that includes proper keyring statements for each gateway.

**GMM API Usage and Documentation:**


**GMM Generating API Keys:**


Firewall Ports for GMM to Gateway Communication

If the routers are located behind a firewall, Cisco Kinetic requires specific TCP/UDP network ports to be opened and IP protocols to be permitted. This allows Cisco Kinetic to communicate with the gateways. Please refer to **Appendix, page 107** for the required settings.
GPS and Geofencing

GMM can enable the GPS functionality within a gateway to provide GPS information and geofencing. This is especially useful for asset tracking and recording movement. Available information includes the current location of the asset, historical location information, and history of a gateway over time. The gateway location history is displayed by default for the past 24 hours in 1-hour increments. The information for a specific gateway can also be displayed for a specific day over a 30-day period.

The geofence can be easily defined in GMM to track when a gateway enters or leaves a geographic location such as when a truck is within a mile of the shipping dock or when it leaves that same area. The geofence can be added by specifying a predefined radius around a geographical location or being custom drawn on the map (see Figure 21).

For more information on setting up a geofence and performing GPS troubleshooting, please refer to the following URL:


Figure 21  Geofencing
Monitoring

GMM provides various methods to monitor and troubleshoot the management of gateways. Customers have role-based access to the portal for monitoring the status of the gateways such as its overall health, claim status, view event logs, run diagnostics, and verify network connectivity. Customers can also generate reports, set up audit logs, and create alerts based on the events on the gateways.

For more information on how to monitor gateway status, generate reports, and create alerts, please refer to:


Integration with Cisco Control Center

Cisco Control Center (formerly Jasper Control Center) is a cloud-hosted platform that allows customers to manage the cellular connection of their device. Using Cisco Control Center, customers can access a portal for monitoring the status of devices using Control Center-managed SIM cards. Available information includes the rate plan, SIM status, and data usage. SIM state modifications can be made to individual SIMs or to a group.

Kinetic GMM uses the Control Center API to access the Control Center information and make changes to the SIM state of an associated gateway. When API access information for Control Center is entered into Kinetic GMM, it automatically identifies all gateways using Control Center-managed SIMs. Kinetic GMM displays summary information about the cellular rate plan, SIM state, current billing cycle, and data usage, and identifies if a data overage limit (set in Control Center) has been reached. Finally, a link is provided to open the full Control Center web portal.

Figure 23 displays the device list information available through the Cisco Control Center integration.
The Control Center can also provide details (Figure 24) of a single SIM card such as the IP address assigned to a connected device, connection status, and historical data usage.

**Figure 24  Cisco Jasper Control Center–Device Details**

The Control Center integration also provides users with the option to deactivate the SIM card when the gateway is deleted from Kinetic GMM.

While Kinetic GMM natively provides cellular usage data, this data originates from the gateway rather than the cellular carrier. Cisco Control Center provides the carrier usage data. For additional information about Control Center, please refer to the following URL:

- [https://www.jasper.com/products](https://www.jasper.com/products)
Network Integration

This chapter includes information on the headend architecture and design as well as Edge Gateway routing options for integrating the asset network with the enterprise network.

Headend Architecture and Design

This section highlights the headend best practices relevant to the Cisco Remote and Mobile Assets solution. The core network components include:

- **Data Center Infrastructure**—This includes compute resources and networking resources like switches and routers, WLC, enterprise firewalls, Intrusion Prevention Service (IPS), Intrusion Detection Service (IDS), and Web Application Firewall (WAF).

- **VPN HER Cluster**—Cisco offers a number of HERs based on the number of IoT Gateways and throughput requirements. This includes the Cisco CSR1000v, ISR4000, and ASR 1000 series routers.

- **RADIUS Server**—Enterprise RADIUS server for IEEE 802.1X authentication.

For the CVD, a pair of Cisco CSR1000v virtual appliances were used. More information is available at:


Testing was performed using a FreeRADIUS authentication server. For more details, please refer to the following link:

- [https://freeradius.org/](https://freeradius.org/)

For a more detailed enterprise head quarter network design, please refer to:


Please refer to the Cisco Data Center Security recommendations located at:

VPN Headend Routers

To extend enterprise connectivity from your enterprise HQ to your edge gateways, FlexVPN tunnels will be required from each edge gateway to the enterprise HQ. This will require a cluster of highly available, redundant, and scalable routers to terminate the FlexVPN connections and traffic coming in from each of the edge gateways.

Cisco offers a number of HER options, the two most common being ASR 1000 physical routers for scale deployments and a redundant cluster of the Cisco CSR1000v virtual appliances for smaller deployments:

- **Low-End Option**—If targeting a pilot or a few hundred gateways, we recommend using a cluster of Cisco CSR1000v virtual appliances at the headend in order to terminate the FlexVPN connections coming in from the edge gateways.

- **Mid-Range Option**—If needing to scale from a few hundred to a couple of thousand edge gateways, we recommend using a cluster of the physical Cisco ISR 4000 series or the Cisco ASR 1000 series of routers that provides higher scale and throughput capabilities.

- **High-End Option**—If needing to scale to thousands of edge gateways, we recommend using a cluster of the physical Cisco ASR 1000 series of routers which provides extreme scalability and throughput capabilities.

**Best Practices:**

- When using virtual appliances, it is best to distribute each virtual appliance on a different virtualization host so as to protect against host failure.

- In order to provide redundancy, load balance incoming FlexVPN connections and provide higher scale, we recommend using the IKEv2 Load balancing feature along with HSRP, as described below.

Gateway VPN Resiliency

Multiple methods are available to support VPN resiliency from the edge gateways to the enterprise HQ:

**Cellular Redundancy Options**

- **Single-LTE Dual-SIM**—This deployment model provides some resiliency by allowing a back-up Service Provider through the use of a second SIM.

- **Single-LTE Single-SIM**—This deployment model does not provide any form of VPN resiliency since it uses a single LTE connection with a single Service Provider.

**VPN Headend Resiliency**

- As detailed in IKEv2 Load Balancing, page 43, this design proposes the use of a cluster of headend routers running HSRP + IKEv2 load balancing to provide VPN resiliency at the enterprise headquarters.

- For an additional level of redundancy, dual Site-to-Site FlexVPN can be deployed using a Dual-LTE gateway. However, what is generally deployed is a single FlexVPN tunnel with IKEv2 clustering to provide failover at the HER.

- Embedded Event Manager (EEM) scripts could be used on the gateway to trigger SIM failover to provide redundancy for WAN cellular links. This is especially useful with Dual-LTEs or Dual-SIMs.
FlexVPN Headend Design

We recommend using a pair of HERs running the HSRP in order to provide routing redundancy and mitigates the dependency on any single router.

Best Practices:
- Deploy each of the Cisco CSR1000v virtual appliances on separate virtualization hosts to protect against the underlying failure of the computer host.
- For physical ASR 1000s routers, please use applicable HA technologies like IOS-XE process redundancy, dual route processors (RPs) for hardware control-plane redundancy, and dual ESPs.

For detailed information on how to go about configuring IKEv2 Load Balancing, please refer to:

Figure 26 FlexVPN Headend Design

IKEv2 Load Balancing

The IKEv2 Load Balancer feature enables clusters of FlexVPN gateways and distributes incoming IKEv2 connection requests among FlexVPN gateways. It redirects the incoming FlexVPN client requests to a least loaded FlexVPN gateway based on the system and crypto load factors. Prerequisites for IKEv2 Load Balancing include:

- For the server-side configuration, the HSRP and FlexVPN server (IKEv2 profile) must be configured.
- For the client-side configuration, the FlexVPN client must be configured.

Benefits of the IKEv2 Load Balancer include:
- The IKEv2 Load Balancer support feature is cost effective and easy to configure.
- A FlexVPN client does not need to know the IP addresses of all the gateways in the cluster. The client need only know the virtual IP address of the cluster.
- The entire crypto session is redirected to a node in the cluster.
IKEv2 also has a redirect mechanism that enables a VPN gateway to redirect a FlexVPN client request to another VPN gateway based on load condition and maintenance requirements. This redirect mechanism is performed in the following scenarios:

- On security association (SA) initialization (IKE_SA_INIT)
- On SA authentication (IKE_AUTH)

The IKEv2 Load Balancer feature provides a Cluster Load Balancing (CLB) solution by redirecting requests from remote access clients to the Least Loaded Gateway (LLG) in the HSRP group or cluster. The CLB solution works with the IKEv2 redirect mechanism defined in RFC 5685 by redirecting requests to the LLG in the HSRP cluster.

**Figure 27 IKEv2 Clustering with HSRP Failover to Standby**

Cluster Load Balancing occurs in three steps:

1. An active HSRP gateway is elected as a "master" in the HSRP group and takes ownership of the Virtual IP address (VIP) for the group. The master maintains a list of gateways in the cluster, keeps track of the load on each gateway, and redirects the FlexVPN client requests to the LLG.

2. The remaining gateways, termed as "slaves," send load updates to the master at periodic intervals.

3. When an IKEv2 client connects to the HSRP VIP, the request first reaches the master, which in turn, redirects the request to the LLG in the cluster.

The components of the CLB solution are as follows:

- HSRP
- CLB master
- CLB slave
- CLB communication
- IKEv2 redirects mechanism
Remote and Mobile Assets

Part II: IT Design

HSRP
The Hot-Standby Router Protocol (HSRP) is a Cisco standard for providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail. Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and SVIs.

HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group’s MAC and IP addresses. A new standby router is also selected at that time if one is available. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

The design that was tested used dual CSR1000v in combination with HSRP, which provides redundancy, resiliency, and high availability for FlexVPN tunnels coming in from the edge gateways. A failure of the master HSRP router causes one of the standby slave routers, which is part of the HSRP group, to take over as the master and take ownership of the VIP address. Any FlexVPN sessions that were terminating on the failed master are renegotiated and established to the remaining routers that are part of the HSRP/IKEv2 load balancing group based on the load on each of the gateways. The newly assumed master node will monitor the load on each of the gateways that are part of the group and accordingly load balance the IKEv2 requests.

CLB Master
A CLB master runs on the HSRP master or "Active Router" (AR). The master receives updates from CLB slaves and sorts them based on their load condition to calculate the least loaded gateway (LLG). The master sends the IP address of the LLG to IKEv2 (on the FlexVPN server). The IP address is sent to the initiator (FlexVPN client), which initiates an IKEv2 session with the LLG. The master redirects incoming IKEv2 client connections towards the LLG.

CLB Slave
A CLB slave runs on all devices in an HSRP group except on the AR. The slaves are responsible for sending periodic load updates to the server. A CLB slave is a fully functional IKEv2 gateway which supplies information to the CLB master. Apart from updates, CLB slaves send messages for aliveness assurance to the CLB master.

CLB Load Management Mechanism
The CLB Load Management Mechanism, which is a TCP-based protocol running between the CLB master and the CLB slaves, informs the CLB master about the load on the CLB slaves. Based on this information, the CLB master selects the LLG to handle the session on each new incoming IKEv2 connection.
**Edge Gateway Routing**

We provide two options for designing the edge gateway routing:

- **Option-1: Split Tunnel at Edge Gateway, page 46**
- **Option-2: Default Route Advertised by Enterprise Headend, page 47**

**Option-1: Split Tunnel at Edge Gateway**

In this option, a split tunnel is used for traffic originating from devices behind the gateway. Traffic destined for the public Internet is directly sent over the cellular interface out to the Internet. The only traffic that traverses the FlexVPN tunnel is for the subnets that are advertised by the Enterprise HER to the edge gateways. The advantage of this design is that it reduces the throughput needed at the enterprise headend since it does not need to deal with traffic intended for the Internet. The downside is that all traffic intended for the Internet will be allowed. This design is most suited to enterprises that want to forward any Internet bound traffic directly to the Internet without applying any policies.

**Figure 28  Split Tunnel Routing at Edge Gateway**
Option-2: Default Route Advertised by Enterprise Headend

When using this routing option, a default route is advertised by the Enterprise HER and all traffic from the edge devices are first routed to the Enterprise HERs. This scenario is used by enterprises that have strict network policies requiring total control over all traffic and requirements to inspect and filter all traffic. In this case, enterprise firewall rules can be applied and enforced within the enterprise data center before the traffic is forwarded to its destination. Unintended traffic can even be blocked and discarded. The same is true for traffic destined for the public Internet.

This architecture allows the enterprise to route the traffic via a WAF before routing the traffic to the public Internet and apply and enforce rules for what traffic can be forwarded to the Internet. The disadvantage of this design is that since all traffic is first routed to the enterprise headend, it needs to be able to support much higher throughput rates as compared to the split-tunnel design. The advantage is that the enterprise gains control over all traffic originating from the edge, both enterprise bound and Internet bound, and can apply policies (firewall rules, WAF rules) to restrict and filter traffic.

Both options allow control of which enterprise subnets are visible to the edge devices by advertising the appropriate subnets to the edge gateway.
Wi-Fi

This chapter, which provides Wi-Fi architectures and best practices, includes recommendations for the router Wi-Fi mode and the station architecture and design, including the use of WGBs.

Wi-Fi Connectivity

Wireless technology based on IEEE 802.11 is a key requirement for many customers looking to extend their enterprise network, especially for mobile use cases. The IR829 router makes 802.11n connectivity available for downstream client access ("hotspots"). The ability to wireless connect laptops, phones, tablets, cameras, and a wide range of other devices to the remote or mobile gateway enables clients to achieve an experience consistent with being within range of the enterprise wireless infrastructure.

Wi-Fi is currently available only on the IR829 router. The IR807 and IR809 routers do not support Wi-Fi.

2.4 GHz and 5 GHz

When operating as a hotspot, the AP803 onboard the IR829 can use both its 2.4 GHz and 5 GHz radios for client connections, providing maximum performance and compatibility. When operating as both a hotspot and a WGB, the hotspot will use the 2.4 GHz radio, while the WGB will use the 5 GHz radio.

Figure 30  IR829 Wireless with Autonomous Mode and Hotspot Only
A Service Set Identifier (SSID), which is generally used as a "name" to identify a wireless network, is used by client devices to specify which network to join. Depending on the use case, it may be beneficial to use a unique SSID for each IR829 acting as a hotspot or use a common one across all APs deployed across an enterprise.

- If the intent is for individuals to only have access to a single IR829’s network, using a unique SSID and PSK for authentication may be ideal. This is available through Autonomous Mode since the wireless APs are not integrated with the corporate wireless infrastructure and the Cisco Wireless LAN controller.

- If the goal is to provide a unified extension of the fixed enterprise wireless network, using the same SSID and authentication method that is used in that fixed wireless network is recommended. Using Unified Mode, the gateways use a Cisco Wireless LAN controller for AP configuration and management. This is ideal for businesses with existing Cisco Unified wireless infrastructure and allows the existing fixed wireless infrastructure to be extended to remote and mobile gateways. This provides centralized configuration management and monitoring of the APs onboard the IR829. This also helps provide a seamless experience for employees connecting to the fixed wireless network by creating a wireless network “bubble” around the IR829 without needing to use a different SSID or authentication method.

Unified APs use the Control and Provisioning of Wireless Access Points (CAPWAP) protocol to communicate with the Cisco Wireless LAN Controller (WLC). CAPWAP uses a Layer 3 tunnel over UDP between the Unified AP and the WLC. Ensure that the firewall setting allows CAPWAP control packets to be sent between the ephemeral UDP port on the AP and UDP port 5246 on the WLC.

Since most WLCs reside inside the enterprise on a secure network that is not directly accessible via the Internet, two general options for a GMM-managed IR829 to communicate with the WLC exist:

1. In the first option, the IR829 maintains a FlexVPN tunnel connected to the enterprise VPN headend that provides connectivity to the enterprise network, including the WLC. This FlexVPN tunnel will typically be established over the cellular interface(s) of the IR829 using a public APN with access to the Internet, but could also be connected over the Ethernet to an external modem or network.
2. The second option for establishing enterprise connectivity between the Unified AP and the WLC is to use a Private APN. In this scenario, the private APN should be set up to allow enterprise-owned cellular devices to connect directly into the enterprise network without needing a VPN tunnel.

In a Unified Wireless LAN architecture, two options are typically available for determining how the client data will be routed or switched through the network.

1. In centrally-switched mode, all client data is routed through the CAPWAP tunnel and through the WLC.

2. In locally-switched mode, the client data does not need to traverse the CAPWAP tunnel and WLC, but instead can be switched or routed on the local network (IR829 in this case) itself.

We recommend the use of the locally-switched mode so that any communication between devices connected to the IR829 will not have to traverse the WAN connection, thus reducing the latency and cellular data usage.
Note: The Cisco Remote and Mobile Assets solution supports either Autonomous or Unified Mode for configuring the AP803 onboard the IR829 to act as a wireless hotspot.

Recommendation:
Use the same SSID and authentication for mobile hotspots that are used in fixed enterprise wireless networks, if applicable. Enable locally-switched mode when using Unified Wireless on the IR829. If the IR829's onboard AP will be deployed in autonomous mode and configured to use the WGB feature, the WGB should be set to connect to the enterprise fixed wireless network SSID. For additional information about Cisco Unified Wireless, refer to the Enterprise Mobility 8.5 Design Guide at the following URL:


Authentication

Authentication of wireless clients is accomplished by one of two available methods:

- The simplest form of authentication is via a pre-shared key (PSK), which is essentially a common password that is shared by all clients that need to connect to the wireless hotspot network. This PSK is best suited to use cases where ease of connectivity is prioritized over security such as in a public transportation vehicle where the goal is to provide hotspot connectivity for passengers. The PSK is communicated to users out-of-band (for example, by a posted sign or word-of-mouth).

- The alternative authentication method supported in the solution is via 802.1x, which is an IEEE standard mechanism for network-based authentication. 802.1x defines how Extensible Authentication Protocol (EAP) packets can be encapsulated for use over LANs (this is called EAPOL, for EAP over LAN), including wired Ethernet and wireless 802.11 networks. Three parties are involved in every 802.1x authentication transaction:
  - Supplicant—This is the end client device, such as a laptop, phone, or tablet that needs to access the wireless network. Typically, the supplicant functionality will be built into the operating system, or could be implemented in another application such as Cisco AnyConnect.
  - Authenticator—This is the network device, such as a wireless access point, or a switch that acts as an enforcement point in the network, blocking client access until authentication is complete.
  - Authentication Server—This is an application that actually authenticates the supplicant and typically communicates using protocols like RADIUS and EAP.
The authentication process is outlined below in the ladder diagram in Figure 34.

**Figure 34  802.1x Authentication Ladder Diagram**

The Cisco Remote and Mobile Assets solution supports 802.1x authentication with a username and password for wireless hotspot clients connected to the IR829. Authentication for wired clients using 802.1x is not supported. In order for clients to authenticate using 802.1x, the WAN connection from the IR829 to the RADIUS server must be available. If the WAN connection is interrupted, new wireless client authentications will fail and clients will not be able to connect. Clients using PSK authentication will still be able to authenticate locally on the AP if the WAN connection is interrupted.

**Wi-Fi Network Architecture and Design**

Customers require a scalable Wi-Fi infrastructure to deliver secure and high bandwidth wireless connectivity to vehicles parked at the station. Figure 35 shows the main Wi-Fi components used by the Cisco Remote and Mobile Assets solution:

- **Cisco Wireless LAN Controller**—A high-density controller for configuring and managing the APs. This is available in both a virtual and a physical form factor.
- **Cisco IW3702 Ruggedized Access Points**—IP67-rated outdoor AP that provides IEEE 802.11ac Wave 1 Wi-Fi coverage for the clients parked outside the station.
- **Station Network**—This includes the branch router with backhaul connectivity to the enterprise headquarters using some technology like MPLS VPN, and iWAN/SD-WAN. It also includes PoE-enabled switches to power the wireless APs and provide them with network connectivity.

Since most enterprises are expected to already have some form of wireless deployment already in place, the Cisco Remote and Mobile Assets solution has been designed to integrate seamlessly with existing wireless deployments.

- **WGB** requires support for the 5 Ghz band.
- **Unified mode deployments** require a Cisco wireless infrastructure with a Cisco Wireless LAN controller.
Cisco Wireless LAN Controller

The WLC is used to manage large quantities of lightweight access points (LAPs) from a single location and can take the form of a physical device, a virtual machine, or even software on a Catalyst 9300. The WLC can be managed via GUI or CLI. Important things to note about WLCs are as follows:

- WLCs can be located centrally or at the remote site depending on the Wi-Fi network requirements and best practices.
- All configuration for the LAPs is pushed down from the WLC. This can include:
  - Authentication method (dot1x or PSK). For more information, see Authentication, page 51.
  - Certificates
  - RF Management
  - Software version
  - SSIDs
  - Switching Mode
- All management and provisioning traffic is communicated via the CAPWAP protocol.
In this solution, the FlexConnect switching mode was validated to ensure that all data traffic is locally switched on the LAP itself, instead of tunneled to the WLC.

Existing Unified Wireless networks will require a separate WLAN for the WGB. For security reasons, this WLAN should not be broadcast and should only be accessible by gateways connecting via WGB.

Lightweight Access Point

The IW3702 and IW 3502 Access Points were validated for this solution and may be deployed with a variety of omni-directional or directional antennas, depending upon the branch/station layout and coverage requirements. Each station layout will present unique criteria and challenges for wireless deployment, so a site survey is required to determine the optimal positioning and density for access point deployment. Important things to consider for the LAP are:

- Access to a Yard Switch that supports Power over Ethernet (PoE)
- How it associates with the WLC
- Its outdoor radio coverage

Associating the LAP

LAPs must establish a CAPWAP tunnel with the WLC in order to get its software image and configuration. Therefore, it is necessary for the access point to find a list of available controllers with which it can associate. This can be done in one of three different ways:

- Broadcast on the local subnet
- DHCP Option 43 returned from the DHCP server
- DNS lookup for "CISCO-CAPWAP-CONTROLLER.localdomain"

In cases that the LAP does not reside in the same network as the WLC, "ip-helper" will need to be configured on the switch to which the LAP is connected. This way any broadcast messages for DHCP discovery will be directed to a central DHCP server, instead of needing to deploy a DHCP server at the edge of each Branch Network.

Branch Site - Backhaul to DC

We recommend using a technology such as an MPLS VPN connection from the enterprise HQ to each of the branch/station sites. MPLS VPN provides advantages around secure connectivity, requesting certain QoS Attributes, scalability, and traffic routing capabilities. The backhaul connectivity from station to headquarters should be resilient and low latency, and have adequate bandwidth to support the needs of the station.

Workgroup Bridge

The WGB feature provides a high bandwidth uplink for the in-vehicle router to use when it is in range of the fixed wireless infrastructure. A primary use case of this functionality is that of an IR829 installed in a vehicle that collects a high volume of data (such as high definition video stored on a camera). In order to conserve LTE bandwidth, customers may opt to offload the data to an external server at the end of the shift when the vehicle returns to the station. Routing metrics can be set to give preference to the WGB uplink over the cellular uplink when the vehicle gets in range of the fixed wireless infrastructure and successfully connects. This allows for the secure and rapid transfer of bulk data and video files without incurring LTE bandwidth charges.

With WGB, the IR829’s on-board AP acts as a client to the fixed wireless network. When the IR829 is configured for WGB, it will need to be configured in autonomous mode and will dedicate the 5 GHz radio on the onboard AP803 for the WGB connection and reserve the 2.4 GHz radio for hotspot functionality.

Some factors to consider when using WGB through Kinetic GMM:

- WGB functionality is only supported on the IR829 gateway
- WGB functionality is only supported when the IR829’s on-board AP803 is operating in autonomous mode
Remote and Mobile Assets

Part II: IT Design

- WGB functionality currently supports only PSK authentication to the fixed wireless network
- When WGB mode is enabled, 802.1X authentication is not supported for hotspot clients

Restricted Subnet

In order to ensure that connectivity to a specific host or network is only available via the WGB, we recommend the use of a restricted subnet. This will prevent high-bandwidth services and applications from consuming the cellular data. When the WGB connection is down, any traffic destined to the restricted subnet will be dropped regardless of what other uplinks are active.

Typical WGB Applications

Stations and branches are likely to host a number of applications that require high-bandwidth access to and from the mobile gateways, some example of applications that would benefit from a WGB connection include:

- **Video Offload Server**—Most public service fleets like police cars and city buses capture a lot of video surveillance footage. This video will need to be uploaded to the video server when the vehicles dock at the branch/station site. Doing this using the WGB functionality discussed above will limit the use of expensive and limited cellular bandwidth.

- **Location History Server**—Many enterprises want to store the location history for each of their mobile assets for security and regulatory reasons. This can be achieved by having a location history storage server at each of the branch sites. Again, location history can be offloaded using the WGB functionality to preserve the expensive and limited cellular bandwidth.

Backhaul

This chapter discusses the available backhaul options, including Ethernet, Wi-Fi WGB and Cellular LTE. Further detail is provided on the LTE options including public vs private APNs, dual SIMs and radios, and how best to achieve QoS.

Available Backhaul Options

The Cisco Industrial Router portfolio offers a variety of Wide Area Network (WAN) backhaul options to suite customer use cases and requirements.

<table>
<thead>
<tr>
<th>Table 8 Backhaul Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Model</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IR807</td>
</tr>
<tr>
<td>IR809</td>
</tr>
<tr>
<td>IR829GW-LTE</td>
</tr>
<tr>
<td>IR829B-LTE</td>
</tr>
<tr>
<td>IR829-2LTE</td>
</tr>
<tr>
<td>IR829M-2LTE</td>
</tr>
<tr>
<td>IR829B-2LTE</td>
</tr>
</tbody>
</table>

GMM-managed gateways can have multiple WAN interfaces configured; the routing behavior of the traffic will change for each interfaces based on the GMM template.
Remote and Mobile Assets

Part II: IT Design

Ethernet
All of the industrial routers include an Ethernet port that can be used as a high speed, reliable uplink to connect the gateway to the Internet or the enterprise network. This interface will typically connect to an external modem (cable, DSL, or satellite) or an existing wired LAN network. Routers installed in locations with an existing wired LAN (e.g., a factory floor or retail store) will require that the security policy and implementation at that location allow for the gateway to communicate with the Kinetic GMM cloud services (see Appendix, page 107 for required port and protocol settings). If the security policy in place does not allow this kind of access, we recommend instead using the cellular connection on the gateway to ensure Kinetic GMM access. An example of this use case is a machine builder with a ruggedized gateway in their equipment, used for monitoring access and machine maintenance. This gateway would require Internet connectivity to enable GMM management.

Wi-Fi Workgroup Bridge
As described in Wi-Fi, page 48, the WGB on the IR829 provides a high bandwidth uplink using the 5 GHz IEEE 802.11 radio in the on-board access point. This would typically be used by fleet vehicles needing to upload bulk video/data or download bulk GIS or similar data when parked at the station. Performing these large transfers over cellular would be slower and significantly more expensive.

Since we assume that the WGB will connect directly into a trusted enterprise wireless network, the standard GMM Template does not support Site-to-site FlexVPN over a WGB link. GMM Custom Configuration Templates can be used by customers requiring FlexVPN over WGB. This is common if the connection is through a public Wi-Fi network (such as a municipal network shared by many groups).

Cellular
Cellular connectivity allows the ruggedized gateways to wirelessly access the Internet or enterprise network while the gateway is installed in a moving vehicle, or remote location where wired connections are not feasible. The rest of this chapter details the various cellular options available to customers.

Available Cellular Options

Public and Private APNs
The Cisco Industrial Routers support both public and private APNs over their cellular connection. This is used to determine which network the modem will attempt to join. An APN can fall into one of several categories, defined below:

- **Public APN**—Public APNs connect directly to the wireless service provider’s network. Any traffic traversing the provider network is not encrypted. This is the default option available to a GMM-managed gateway out of the box.

- **Private APN with Public APN Support**—These APNs will typically connect to certain enterprise networks directly, while allowing other destinations on the Internet to be reached directly through the service provider network (without having to go through the enterprise). As with Public APNs, GMM-managed gateways can connect to these networks out of the box. In this case, the initial connection to the Kinetic GMM cloud services will be made with the default public APN and the APN is updated during the claiming and provisioning process to use the private APN configured in the template for enterprise access.

Cisco recommends ensuring an air gap between the gateway and the enterprise wired network if the wired network cannot be configured to connect to the Kinetic GMM cloud service.

When selecting a data plan for cellular connectivity, customers need to account for the 80MB of monthly data required for Cisco GMM management traffic. Cisco recommends that customers analyze their data usage during the pilot phase to determine a suitable data plan.
**Private APN**—Private APNs provide a tunnel between the gateway and the enterprise network. All traffic traverses the enterprise network, including traffic destined for the public Internet (such as the Kinetic GMM cloud). Please refer to Security Overview, page 14 and Industrial Routers, page 21 for further information on the use of Private APNs.

Cisco highly recommends not mixing Public and Private APNs on the same router since this may cause configuration and routing incompatibility.

---

**Quality of Service Options**

QoS uses various queuing, prioritization, and policy mechanisms to ensure that congested interfaces prioritize the most important traffic. QoS techniques increase in importance with less reliable and lower bandwidth links (such as cellular) or when specific types of traffic or applications need to be protected during congestion (such as voice traffic).

Since LTE can dedicate bandwidth to important traffic by prioritizing specific bearer channels, IOS can be used to align the QoS configuration on the gateway with the service provider SLAs. Prioritized applications typically include voice and streaming video, as well as various control plane protocols that are sensitive to latency, jitter, and loss. On other interfaces, such as Ethernet and WGB, standard Cisco QoS practices should be applied using the Modular QOS Command Line Interface (MQC) that uses class-maps and policy-maps to classify traffic types and apply desired behavior to that traffic.

GMM Custom Configuration Templates should be used to configure the customer-specific QoS policies. A sample QoS configuration has been included in Part IV: Sample Configurations, page 78. For a detailed look at cellular QoS on Cisco routers, refer to:


For details about QoS design and implementation, refer to the Enterprise QoS SRND:


For more information on Wi-Fi QoS, review the Enterprise Mobility Design Guide:

Remote and Mobile Assets

Part II: IT Design

LTE Radio and SIM Options

**Single LTE, Single SIM**

The simplest cellular option available on the Cisco Industrial Routers is a single cellular modem with a single SIM card. This allows the gateway to connect to a single provider, with no mechanism for redundancy or load balancing.

**Single LTE, Dual SIM**

The IR807, IR809, and some IR829 routers offer two SIM cards with a single cellular modem. The two SIM cards can belong to different cellular providers and are used in an active/standby manner to provide redundancy. When the primary SIM loses connectivity, it switches to the secondary SIM. However, if the primary SIM regains connectivity, the router only switches back to the primary SIM when the secondary SIM loses connectivity to the network.

The switchover between active and standby SIM cards typically take around 3 to 4 minutes (connection failure detection to connectivity restored on the standby SIM). Customers requiring faster switchover are encouraged to consider the IR829 with dual-radios. For further information, refer to the Configure Dual SIM Feature and SIM Failover at the following URL:


**Dual LTE, Dual SIM**

Some IR829 models (identified by 2LTE in the part number) contain two cellular modems, and one SIM card per modem. This allows the IR829 to maintain two simultaneous cellular connections. The two cellular connections can be used in a redundant fashion with a quicker failover time than the single radio, dual-SIM option. When an IR829 with dual LTE modems is provisioned in active/standby mode using Kinetic GMM Templates, the failover mechanism monitors the state of the management VPN tunnel (Tunnel1). If the tunnel changes state to “down,” an EEM script is triggered, which clears both cellular connections and attempts to bring the Tunnel back up over the standby cellular interface.

Dual cellular interfaces can also be configured to operate in active/active mode. In this mode, the router will load balance traffic across the two interfaces. The default load balancing algorithm is per-destination rather than per-packet. Per-destination load balancing pins traffic between a specific source and destination IP pair to a specific outbound interface. As new source-destination connection pairs are established, they are alternatively assigned to the available load balanced interfaces. Kinetic GMM also provides an option to assign a specific destination subnet to the second cellular interface when enabling active/active LTE. In this case, all other traffic will use the first cellular interface.

- **Dual radio IR829s offer 90-second switchover time from active to standby modes (connection failure detection to connectivity restored on the standby SIM). Refer to the Configure Dual SIM Feature and SIM Failover document on Cisco.com for further information.**

- **An active/active LTE configuration cannot be supported if Site-to-site FlexVPN is also configured in Kinetic GMM.**
Cellular to WGB Switchover and Switchback

In addition to switchover between two cellular interfaces, the IR829 also supports switchover from cellular to WGB backhaul. This is implemented via a simple routing statement and happens seamlessly. Since the health of the WGB is checked every 60 seconds, the switchover from WGB to cellular could take up to 60 seconds.

Prepare for Deployment

A key benefit of the Cisco Remote and Mobile Assets solution is the simplicity of onboarding gateways. This allows non–IT users in the field to deploy the gateway with little to no IT support. This also significantly speeds up bulk gateway deployments across geographically-dispersed locations.

This chapter describes the process for preparing for ZTD from an IT user's perspective. It includes the key steps required to set up the GMM template and user accounts, and, if required, to prepare an existing gateway to be claimed by GMM using the Gateway Provisioning Tool (GPT).

Figure 36 Prepare for Deployment

Step 1: Create GMM Template

Previous chapters of this IT Design section describes the technologies, architectures, and best practices for architecting and designing the Cisco Remote and Mobile Assets solution. This will enable IT staff to create a GMM Template with the required features and functionality.

Cisco recommends that customers use Kinetic GMM templates rather than Cisco IOS to configure the gateways unless directed to IOS by GMM support. This will prevent gateway configurations that could conflict with GMM and break connectivity to Kinetic GMM. This also allows the gateway to be password protected during the claiming process to prevent admin–level access to the router. GMM also creates an Operator account on the gateway to provide troubleshooting access.

For a step-by-step guide to configuring Templates in Kinetic GMM, please refer to the official product documentation:

- [https://developer.cisco.com/docs/kinetic/#!gmm-overview](https://developer.cisco.com/docs/kinetic/#!gmm-overview)

Step 2: Enable GMM Access for Field Operators

The GMM admin must create Operator accounts for field users who will be responsible for deploying and maintaining the gateways.

Refer to this link for a step-by-step guide to creating user accounts:

- [https://developer.cisco.com/docs/kinetic/#!add-users](https://developer.cisco.com/docs/kinetic/#!add-users)
Step 3: Activate SIM Cards
Previous chapters in this IT Design part provide an overview of the available SIM card options, including setting up the APN required for the initial gateway claiming process.

Ensuring that field users have working SIMs with the correct APN is critical for ZTD.

Step 4: GPT Process for Existing Gateways
As described in Cloud Provisioning and Management, page 31, new Cisco IRs that are purchased with the GMM option selected are set up for GMM at the factory prior to being shipped. Customers wanting to GMM-enable existing routers (and other routers that were not purchased with GMM enabled) will need to use the GPT to prepare these routers for GMM.

Preparing for GPT
Prior to configuring the gateway using GPT, users will need to download the GPT tool and connect the gateway to their computer using the USB console cable. If set up correctly, the GPT tool will automatically find the router via the connected console and will flash up the serial number of the gateway.

1. Download the Cisco GMM Provisioning Tool (GPT) here:
   https://software.cisco.com/download/home/286321160/type/286321251/release/1.91

2. Connect the Cisco gateway to a computer using the USB console cable:
   - For Windows:
   - For MacOS:
   - For Linux:

3. Connect the PC Ethernet port to the gateway
   - IR807: FastEthernet0 (FE0)
   - IR809: GigabitEthernet0 (GE0)
   - IR829: GigabitEthernet1 (GE1)

4. Run GPT.

This step is only necessary for routers that were not purchased with GMM enabled as well as replacement routers shipped as part of the Cisco Return to Manufacturer (RMA) process.

Please write down the serial number of the gateways being set up using GPT. For additional help with GPT, please refer to:

Running the GMM Gateway Provisioning Tool (GPT) Process

The following information is required in order to set a gateway up using the GMM GPT:

1. Gateway serial number
2. Custom APN information (if required)
3. Expected deployment geo (us.ciscokinetic.io for US or eu.ciscokinetic.io for Europe)
4. Port in use for the Ethernet cable
5. Gateway’s IP address (if static IP is required)
6. Host IP of the PC that is connected to the gateway
7. Whether the AutoSIM feature needs to be activated (please refer to Industrial Routers, page 21 for further information)
8. Option for use of Cartridges for IOx or Custom IOS Configurations (the default is “No” unless instructed to do so by GMM Technical Support)

Please follow the screen prompts in the tool to follow the GPT process.

The GPT process can take up to 30 minutes.

Adding GPT Gateways to Your GMM Organization

Once a gateway has been provisioned using GPT, users must contact GMM Technical Support to add the gateways to the GMM organization. An email confirmation will be sent once gateways are available in GMM.

Contact GMM Technical Support by logging into GMM, click Help, and then click Contact Customer Support. Users can select Add Gateway from the drop-down menu and enter the serial number recorded during the GPT process.

Return to Manufacturing (RMA) Process

For more information on the RMA process for Cisco Industrial Routers, refer to the following URL:


Please refer to common gateway issues in Common Gateway Issues, page 109 for additional tips on ensuring a smooth gateway deployment process.
Part III: Field Operate

This part includes the following chapters:

| Chapter 1: Gateway Deployment, page 62 | Easy-to-use workflows for onboarding a new gateway, replacing the gateway, and offboarding the gateway. |
| Chapter 2: Field Monitoring and Troubleshooting, page 71 | Best practices for monitoring and troubleshooting the gateway. |

Gateway Deployment

Onboarding a New Gateway

A key benefit of the Cisco Remote and Mobile Assets solution is the simplicity of onboarding gateways, which allows non-IT users in the field to deploy the gateway with little to no IT-support. This also significantly speeds up the bulk gateway deployments across geographically-dispersed locations. This section describes the process from a field operator perspective, without getting into too much technical detail. By following the steps below, field users can deploy a new Cisco Industrial Router into production in a few minutes.

**Figure 37 Onboarding a New Gateway**

**Step 1: Install Gateway and Accessories**

Part II: IT Design, page 11 provides an overview of the Cisco Industrial Router portfolio and available accessories including power supply and antennas.

Refer to the following links for installation best practices for gateways and accessories:

- IR807:

- IR809:

- IR829:
  - [https://developer.cisco.com/docs/kinetic/#!add-users](https://developer.cisco.com/docs/kinetic/#!add-users)
Step 2: Verify SIM Card(s)
Part II: IT Design, page 11 provides an overview of the available SIM card options including setting up the APN required for the initial gateway claiming process.

Inserting a working SIM with the correct APN is critical for ZTD.

Step 3: Claim Gateway
Claiming the gateway will complete the process to provision them based on the configured template and make them available for monitoring. Gateways can be claimed by using the Cisco Kinetic mobile app for Android and Apple iOS or through the web interface on any computer with an Internet connection.

The APN information is important for gateways using their cellular connection:
- Gateways using public APN should be able to automatically connect to the Internet and perform the claiming process.
- Gateways using private APN will be required to follow the private APN process outlined below.

Using the GMM Mobile App to Claim the Gateway
Follow these steps to claim a gateway with the GMM Mobile Application:
1. Download the GMM mobile app to your smartphone or tablet.
2. Scan the gateway bar code
3. Select the gateway model on the app
4. Select the appropriate configuration template that has been pre-loaded

Download the GMM mobile app from the app store by searching for Cisco Kinetic:

For additional information on the Cisco Mobile App, refer to the following URL:
The screenshots below depict the claiming and verification process using the mobile app.

**Step 1: Scan Barcode**

Use the Mobile app to "scan" the barcode on the router. This will start the claiming process. For more information on where to find your serial # barcode follow this link:


**Step 2: Select Type of Gateway**

Once successfully scanned, the drop-down menu will provide a choice of gateway models (IR807, IR809, or IR829). Once selected, click **Next**.
Step 3: Select from List of Available Templates

Your IT Staff has created templates to be used. You will see these listed under saved templates. Select the appropriate template and click **Next**.

- **Scan or Select Model**
- **Set Custom Fields (Optional)**
- **Select Template**
  - Default Template - IR809
- **Select Fog Applications (Optional)**
- **Add Subscribed Devices (Optional)**
- **Review**

Step 4: Review and Finish

Detailed information about the gateway and template will be visible once a template is selected. Users are encouraged to verify this information before clicking **Finish**. The gateway will reboot several times during the claiming process before it appears as a gateway in the Web UI.
Using the GMM Web App to Claim the Gateway
The same four steps are used to claim a gateway with the GMM Web Application:

1. Log into the GMM account using the username and password provided by the administrator and navigate to the **Claim Gateway Screen**.

2. Enter the gateway serial number

3. Select the gateway model

4. Select the appropriate pre-loaded configuration template.

5. Log into the following URL using your GMM credentials:
   - US: https://us.ciscokinetic.io
   - EU: https://eu.ciscokinetic.io

For additional information on the Cisco Web App, refer to:
- [https://developer.cisco.com/docs/kinetic/#!claim-gateways](https://developer.cisco.com/docs/kinetic/#!claim-gateways)

The screenshots below depict the claiming and verification process using the web app.

**Step 1: Navigate to Claim Gateway Screen**
Once successfully logged into the GMM web portal, click **Gateway** on the left and then select **Gateways**:

![Dashboard](image1)

Next, select **Claim Gateway**:

![Gateways](image2)
Remote and Mobile Assets

Part III: Field Operate

**Step 2: Enter the Gateway Information**
For more information on where to find your serial # barcode, follow this link:


The claim gateway screen will provide a choice of gateway models (IR807, IR809 or IR829). The address information is optional. Once selected, click **Next**.

**Claiming Gateways**

1. **Set up**
   - Serial/Numbers (separate entries with spaces, commas or semicolons): 
     - FTQ14442...LM
   - Model: IR829
   - Address 1 (Optional): 
   - State/Province/Region (Optional): 
   - Address 2 (Optional): 
   - Zip/Postal Code (Optional): 
   - City (Optional): 
   - Country: 

   Click **Next**.

2. **Configuration**
   - Template: 
     - Default Template: IR829
     - Default Template - IR829
     - Custom Template

   Click **Next**.

**Step 3: Select from List of Available Templates**
Your IT Staff has created templates to be used. You will see these listed under **Saved Templates**. Select the appropriate template. The fog and device information is optional. Click **Next**.
Step 4: Review and Finish

Detailed information about the gateway and template will be visible once a template is selected. Users are encouraged to verify this information before clicking **Finish**. The gateway will reboot several times during the claiming process before it appears as a gateway in the Web UI.
Provisioning a Gateway with a Private APN

Provisioning a gateway with a SIM that has a Private APN will require one additional step. The initial claiming process MUST be completed with the gateway connected to an Ethernet port that has Internet access since the cellular modem will not work until after the gateway has been claimed. During the gateway claiming process, GMM will automatically push down a Private APN configuration. Once the gateway has been claimed and shows up, it will run on its cellular connection.

Use the following ports on the gateway for your Ethernet connection:

- 807—FastEthernet0 (FE0)
- 809—GigabitEthernet0 (GE0)
- 829—GigabitEthernet1 (GE1)

Ensure use of the special Private APN template during configuration.

Offboarding/Removing a Gateway

Offboarding or deactivating gateways require a few simple steps that can be completed by non-IT users in the field without IT-support. This significantly speeds up the deactivation of gateways in geographically dispersed locations. By following the steps below, field users can uninstall a Cisco 8x9 gateways in a few minutes.

Figure 38  Offboarding/Removing a Gateway

Step 1: Deactivate the Gateway in GMM
Select the gateway to be removed or replaced and click Delete. If the SIM card associated with the gateway is managed through Control Center, you will be asked if you want to deactivate the SIM upon deletion from GMM. The SIM can be reactivated later through Control Center.

Refer to the following links for deactivation best practices for gateways and accessories:

**IR807:**

**IR809:**

**IR829:**
- https://developer.cisco.com/docs/kinetic/#!add-users
**Step 2: Uninstall the Gateway and SIM**

Remove the gateway and ship it back to the IT department. Either deactivate the SIM or return it to the SIM pool for reuse.
Field Monitoring and Troubleshooting

The Cisco Remote and Mobile Assets solution offers a number of tools for non-IT users in the field to use during monitoring and troubleshooting. This greatly reduces the IT-support requirements.

Monitoring the Gateway

Kinetic GMM provides several monitoring tools for monitoring key aspects of field operations including:

- Gateway status
- GPS location and Geo-fencing
- Reports
- Alerts

Gateway Status

Figure 40 provides an overall view of the key information available through the GMM console, including location and status of the gateways. This screen is available when users click Dashboard on the GMM console.

Figure 40 Gateway Status
GPS Location and Geofencing

Users can track the GPS location of any gateway that has GPS enabled by logging into the GMM Dashboard. Using the +/− in the map, the gateway in question can be identified and detailed GPS information displayed. Users can also specify a geofence for the gateway. The gateway will generate an alarm if it enters or leaves this area. More information on the GPS and geofence capabilities is available in Part II: IT Design, page 11.

For more information on GPS tracking and Geo-Fencing, please refer to the following URL:

Reports

GMM provides a simple reporting tool to track cellular and gateway inventory. To access these reports, users log into the GMM portal and click **Tools > Reports**.

**Figure 42  Reports**

Users can then select the type of report required (**Inventory** or **Cellular Usage**) and specify required information, recurrence and the report name.

**Figure 43  Report Selection**
A CSV file of the report can be downloaded by clicking the red CSV button:

**Figure 44  Download CSV File of Report**

For more information on reports, click refer to the following URL:

- [https://developer.cisco.com/docs/kinetic/#!view-reports](https://developer.cisco.com/docs/kinetic/#!view-reports)

A sample report is available in Appendix, page 107.

**GMM Alerts**

GMM can provide alerts for a variety of events, including:

- SIM removal
- Geofencing
- Gateway rebooted
- Gateway Health up/down
- VPN Down
- WGB Down
- Change in Gateway template
Setting up an alert is simple. Users click **Tools > Alerts** on their GMM Dashboard.

**Figure 45  Setting up an Alert**

When **Add Alerts** is clicked, GMM prompts for a name for the alert and the gateways that should be monitored. Users can provide an email address for the alerts and types of alerts to receive.

**Figure 46  GMM Prompt for Alert**

For more information on creating alerts, click here:

- [https://developer.cisco.com/docs/kinetic/#create-alerts](https://developer.cisco.com/docs/kinetic/#create-alerts)
Troubleshooting the Gateway

Gateway Logs

Gateway logs can be accessed through the following screen:

**Figure 47 Accessing Gateway Logs**

![Gateway Logs Access](image)

Gateway Diagnostics

GMM offers a rich set of field-accessible gateway diagnostics tools.

1. Select **Gateway > Gateways**.
2. Select a gateway.
3. Click **Diagnostics**.
4. Click a button to run the predefined diagnostics:
   a. Connectivity with Kinetic—Click **Gateway** or **App Infra** to verify that the gateway and apps can communicate with Cisco Kinetic.
   b. Test network:
      - Click **Ping** or **Trace Route** to verify connectivity from the gateway to a different IP address. See below for more information.
      - Click **Test Throughput** and enter an iPerf Server address to retrieve cellular throughput information. Use this to find out where the connectivity is bad, such as signal strength or uplink bandwidth issues. You can host your own iPerf server (recommended) or use a public iPerf server.
5. Show Commands—Click **Run** to run a set of pre-defined show commands in the gateway that display information about the device.
6. Debug Commands—Retrieve the syslogs, clear the syslogs, and enable/disable additional debugging on the gateways.
7. Refresh—Click **Refresh App Management** to reboot the gateway, reboot the access point (AP) for IR 829 gateways, and refresh the App Management state (this forces Kinetic to resync with the IOx apps running the gateway).
Click Export to download a text file with the diagnostic results. Please refer to Common Gateway Issues, page 109 for additional tips on ensuring a smooth gateway deployment.
# Part IV: Sample Configurations

This part includes the following chapters:

<table>
<thead>
<tr>
<th>Hardware and Software Matrix, page 78</th>
<th>Hardware and software versions that were validated in this CVD.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Configurations, page 79</td>
<td>Sample configurations for the three critical components of the data center. These include the VPN Headend, a virtual Wireless LAN Controller, and the RADIUS server.</td>
</tr>
<tr>
<td>Extending the Enterprise Network, page 93</td>
<td>Sample configurations for extending the enterprise network to gateways for devices and hotspot clients.</td>
</tr>
<tr>
<td>Custom Configuration Templates, page 101</td>
<td>Sample custom configuration to allow for additional Cisco IOS configurations such as Firewall, QoS, and ignition sensing. Uses the GMM Custom Configuration Templates.</td>
</tr>
<tr>
<td>Headend Router Configuration, page 104</td>
<td>Sample Python script that uses the GMM Restful APIs to generate the FlexVPN HER configuration which can be pasted into the headend routers.</td>
</tr>
</tbody>
</table>

## Hardware and Software Matrix

*Table 9* lists the hardware and software used in the Cisco Remote and Mobile Assets solution.

**Table 9  Hardware and Software Matrix**

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN HER</td>
<td>Cisco Cloud Services Router (CSR) 1000V</td>
<td>Version 16.06.04</td>
</tr>
<tr>
<td>Mobile Gateway</td>
<td>Industrial Router 829</td>
<td>IOS Version 15.8(3)M0a</td>
</tr>
<tr>
<td></td>
<td>Modem Firmware: SWI9X30C_02.20.03.00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Embedded AP: 15.3(3)JF4</td>
<td></td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>Industrial Router 807</td>
<td>IOS Version: 15.8(3)M0a</td>
</tr>
<tr>
<td></td>
<td>Industrial Router 809</td>
<td>IR807 modem: SWI9X07Y_02.18.05.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IR809 modem: SWI9X15C_05.05.58.00</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>VMWare ESXi</td>
<td>Version 6.5.0</td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td>Cisco Virtual Wireless Controller</td>
<td>Version 8.3.143.0</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>CentOS VM + FreeRADIUS</td>
<td>Version 7.5.1804 (Core) FreeRADIUS Version 3.0.13</td>
</tr>
<tr>
<td>Lightweight Access Point</td>
<td>Cisco Aironet 3702</td>
<td>Primary Software Version 8.3.143.0 IOS Version 15.3(3)JD16</td>
</tr>
</tbody>
</table>
Data Center Configurations

This section focuses on three critical data center components and provides sample configurations on VMWare:

1. Redundant Virtual HERs
2. Virtual Wireless LAN Controller
3. RADIUS Server

For more information, refer to the following:

Deploying VMWare on Cisco UCS:

Verified Data Center Architecture:

Headend on CSR1000V or ASR 1000

Deploying CSR1000V on VMWare ESXi

Important:
- This solution uses redundant CSR1000Vs, so deploying two is required.
- Install each on separate physical servers to maximize redundancy.

A comprehensive guide for deploying CSR1000V on ESXi can be found at:

VPN Headend on CSR1000v

To support the site-to-site VPN feature, the HER must be configured to terminate the VPN at the corporate end. In this solution, a pair of CSR1000Vs use an HSRP virtual IP address as the endpoint for the FlexVPN tunnels. This way, if one CSR were to lose network reachability for whatever reason, the site-to-site tunnel would not be affected.
The following is a sample configuration for an HER:

**HSRP Specific Configuration for CSR-1**

```plaintext
interface GigabitEthernet6
    description DMZ WAN
    ip address <CSR-1 IP Address> 255.255.255.240
    ip nat outside
    standby 64 ip <Virtual IP Address>
    standby 64 priority 110
    standby 64 name dmz-group
    negotiation auto
    cdp enable
    no mop enabled
    no mop sysid
end
```

**HSRP Specific Configuration for CSR-2**

- The IP addresses should be reachable over the gateway's WAN interface so that a site-to-site tunnel can be established.
- The IP address specified in "standby 64" must be the same on both CSRs because it will serve as the VIP for HSRP. This is the address that will be specified for the site-to-site VPN.
- The interfaces that are used for this configuration must correspond to the interface associated with the public VLAN on the VMWare vSwitch.

```plaintext
interface GigabitEthernet6
    ip address <CSR-2 IP Address> 255.255.255.240
    ip nat outside
    standby 64 ip <Virtual IP Address>
    standby 64 name dmz-group
    negotiation auto
    cdp enable
    no mop enabled
    no mop sysid
end
```

**FlexVPN with GMM-Compliant Configuration**

The authorization policy defines the routing policies and DHCP pool that the peer tunnel device will use:

- "pool" specifies the address pool that the remote tunnel interface is going to pull an IP address from. An example is found later in this configuration.
- "route set access-list" specifies the corporate networks that will be advertised over the tunnel to the peer.
- "no route accept" tells the CSR to not accept any routes coming from the peer.

```plaintext
crypto ikev2 authorization policy default
    pool FlexSpokes
    route set interface
    route set access-list CLOUD
    no route accept
```
The keyring is used for authorizing attempted tunnel connections with PSK:

- For every gateway, a peer must be added with the correct Gateway Serial Number.
- The identity email MUST be formatted as `<GW-SN>@iotspdev.io`. Any other email and the connection will be rejected:

```
crypto ikev2 keyring Flex_key
peer <GW-SN>
    identity email <GW-SN>@iotspdev.io
    pre-shared-key <pre-shared-key>
```

The IKEv2 profile specifies the authentication type, keyring, and domain to match on for tunnel requests:

- Replace the local key-id with the actual identity (e.g., public VIP).
- Authentication "local" and "remote" specify the type of authentication that will be used. GMM requires PSK to be used for the tunnel.
- "keyring local" specifies which keyring to be used for authentication.
  - It doesn’t have to be “Flex_key,” but it must match where the peers are defined virtual-template 1 specifies the template that tunnels will be created from. Virtual-Template configuration can be found later in this section.

```
crypto ikev2 profile Flex_IKEv2
    match fvrf any
    match identity remote email domain iotspdev.io
    identity local key-id <CSR-Public-IP>
    authentication local pre-share
    authentication remote pre-share
    keyring local Flex_key
    dpd 250 10 on-demand
    aaa authorization group psk list default
        virtual-template 1
```

The following is the IKEv2 cluster configuration. It allows for the load balancing of the IKEv2 tunnel across both CSRs, and the configuration must be the same on both.

```
crypto ikev2 reconnect key 1 active <password>
crypto ikev2 cluster
    standby-group dmz-group
    slave max-session 10000
    no shutdown
```

The loopback interface functions as the gateway for traffic across the tunnel. The loopback number itself can be anything so long as the virtual template configuration references it.

```
interface Loopback100
    ! Customize as needed for customer network
    ip address 172.16.4.1 255.255.240.0
```

When a tunnel forms, its interface will be based on the virtual-template configuration that IKEv2 profile references.

- Specifies the physical interface that will serve as the local tunnel endpoint (loopback 100 in this case).
- It also specifies things such as packet size and IPSec configuration.

```plaintext
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback100
  ip mtu 1400
  ip nat inside
  ip nhrp network-id 2
  ip nhrp redirect
  ip tcp adjust-mss 1360
  tunnel mode ipsec ipv4
  tunnel path-mtu-discovery
  tunnel protection ipsec profile default
```

The following is an example configuration for the addresses pool that the tunnels will use. This address pool is referenced by the authorization policy.

```plaintext
ip local pool FlexSpokes 172.16.4.2 172.16.19.254
```

The CLOUD access list defines the corporate networks that are advertised to the remote gateway. This access list is referenced in the IKEv2 authorization policy.

```plaintext
ip access-list standard CLOUD
  permit 192.168.100.0 0.0.0.255
  permit 172.31.0.0 0.0.255.255
  permit any
```

The following code snippet is optional NAT configuration for hiding the VPN network behind the public interface:

```plaintext
ip nat inside source list VPN_CLIENTS interface GigabitEthernet6 overload
  ip access-list standard VPN_CLIENTS
    permit 172.16.0.0 0.0.31.255
```

Each gateway that is added to the site-to-site VPN to the HER will need to have an entry added for that gateway to the HER.

```plaintext
crypto ikev2 keyring Flex_key
  peer <GW-SN>
    identity email <GW-SN>@iotspdev.io
    pre-shared-key <pre-shared-key>
```

Both CSRs must have the above configuration applied.
Full Configuration of CSR-1 Example

```
subscriber templating
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-54719960
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-54719960
  revocation-check none
  rsakeypair TP-self-signed-54719960
!
!
crypto pki certificate chain TP-self-signed-54719960
  certificate self-signed 01
  <redacted>
  quit
!
!
license udi pid CSR1000V sn 9RH2FU04834
license accept end user agreement
license boot level ax
diagnostic bootup level minimal
spanning-tree extend system-id
!
!
username <username> privilege 15 secret 5 <redacted>
!
redundancy
crypto ikev2 authorization policy default
  pool FlexSpokes
  route set interface
  route set access-list CLOUD
!
crypto ikev2 redirect gateway init
!
!
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname CSR-HER-1
!
boot-start-marker
boot system bootflash:csr1000v-universalk9.16.06.04.SPA.bin
```
Remote and Mobile Assets

Part IV: Sample Configurations

```plaintext
boot-end-marker
!
!
vrf definition management
!
address-family ipv4
exit-address-family
!
enable secret 5 <redacted>
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local none
aaa authorization network default local
!
!
!
aaa session-id common
!
!
ip name-server <DNS-1> < DNS-2>
ip domain lookup source-interface GigabitEthernet6
!
!
!
crypto ikev2 keyring field_keys
peer FTX2126200H
  identity email FTX2126200H@iotspdev.io
  pre-shared-key <redacted>
!
peer FTX22342071
  identity email FTX22342071@iotspdev.io
  pre-shared-key <redacted>
 peer FCW2142001M
  identity email FCW2142001M@iotspdev.io
  pre-shared-key <redacted>
!
peer FCW214400DK
  identity email FCW214400DK@iotspdev.io
  pre-shared-key <redacted>
 peer FCW2145000D
  identity email FCW2145000D@iotspdev.io
  pre-shared-key <redacted>
!
peer FTX223420AY
  identity email FTX223420AY@iotspdev.io
  pre-shared-key <redacted>
!
!
crypto ikev2 profile Flex_IKEv2
match fvrf any
match identity remote email domain iotspdev.io
identity local key-id <virtual IP Address>
authentication remote pre-share
authentication local pre-share
keyring local field_keys
```
Remote and Mobile Assets

Part IV: Sample Configurations

```
! Remote and Mobile Assets

dpd 250 10 on-demand

aaa authorization group psk list default
virtual-template 1
!
crypto ikev2 reconnect key 1 active <redacted>
!
crypto ikev2 cluster
standby-group dmz-group
slave max-session 10000
no shutdown
!
!
track 1 ip route 10.0.2.1 255.255.255.255 reachability
!
track 2 list boolean and
object 1 not
!
cdp run
!
!
interface Loopback0
ip address 10.5.0.1 255.255.0.0
!
interface VirtualPortGroup0
ip unnumbered GigabitEthernet3
no mop enabled
no mop sysid
!
interface GigabitEthernet3
description MANAGEMENT INTERFACE
vrf forwarding management
ip address 10.100.5.2 255.255.0.0
negotiation auto
cdp enable
no mop enabled
no mop sysid
!
interface GigabitEthernet5
description CONNECTION TO CORPORATE WAN
ip address 77.77.77.2 255.255.255.0
ip nat inside
standby 17 ip 77.77.77.1
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet6
description PUBLIC INTERFACE FOR FLEXVPN
ip address <CSR-1 Public IP> 255.255.255.240
ip nat outside
ip access-group BLOCK_TELNET_SSH in
standby 64 ip <Public VIP>
standby 64 priority 110
standby 64 name dmz-group
negotiation auto
cdp enable
no mop enabled
no mop sysid
!
```
interface GigabitEthernet7
description DEFAULT GATEWAY FOR DATACENTER VMS
ip address 10.2.0.2 255.255.0.0
ip nat inside
standby 30 ip 10.2.0.1
negotiation auto
no mop enabled
no mop sysid
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1400
ip nat inside
ip nhp network-id 2
ip nhp redirect
ip tcp adjust-mss 1360
tunnel mode ipsec ipv4
tunnel path-mtu-discovery
tunnel protection ipsec profile default
!
router ospf 1
router-id 10.1.0.2
redistribute connected subnets
redistribute static subnets
network 77.77.77.0 0.0.0.7 area 0
default-information originate
!
virtual-service csr_mgmt
!
ip local pool FlexSpokes 10.5.0.3 10.5.255.254
ip nat inside source list PAT-LIST interface GigabitEthernet6 overload
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 64.102.254.145
ip route vrf management 0.0.0.0 0.0.0.0 10.100.0.1
!
ip scp server enable
!
ip access-list standard CLOUD
  permit 10.2.0.0 0.0.255.255
  permit 10.5.0.0 0.0.255.255
  permit 10.50.0.0 0.0.255.255
ip access-list standard VPN_CLIENTS
  permit 10.0.0.0 0.255.255.255
  permit 172.17.92.0 0.0.0.255
  permit 100.0.0.0 0.255.255.255
  permit 192.168.0.0 0.0.0.255
  permit 10.2.0.0 0.0.255.255
!
ip access-list extended BLOCK_TELNET_SSH
deny tcp any eq 22
deny tcp any eq telnet
permit ip any any
ip access-list extended CAP
  permit ip any host 64.41.87.38
  permit ip host 64.41.87.38 any
ip access-list extended PAT-LIST
RADIUS Server

The RADIUS server is used for authenticating hotspot clients via 802.1X instead of pre-shared keys. For instructions on setting up a FreeRADIUS server on CentOS or RHEL, follow the guide at:


Fixed Wireless Infrastructure at the Station

In order to use the Workgroup Bridge function of GMM, a fixed wireless infrastructure must in place. The two important components to this infrastructure are the **Yard Switch** connected to the **Yard AP** and the **Wireless LAN Controller (WLC)**. Other parts of the WAN network design have no specific requirements as long as the Yard Switch has connectivity to the data center.

**Yard Switch**

This solution uses a FlexConnect configuration for its wireless network. This means that one network will be used for CAPWAP communication between the WLC and AP (for AP management), and a separate one will be used for user traffic over the WGB:

- The following configuration shows a trunked interface on the yard switch connected to the Yard AP. VLAN 901 is used for the CAPWAP tunnel to the WLC. This VLAN identifier can be anything, but it is important that it is set as the native VLAN on the Ethernet interface.
For both VLAN interfaces, an "ip helper-address" is configured to forward DHCP messages to the DHCP server in the data center. This IP address must be set appropriately for the desired DHCP server:

```
interface GigabitEthernet1/0/2
  description Connection to Yard AP
  switchport trunk native vlan 901
  switchport trunk allowed vlan 50,901
  switchport mode trunk
!
interface Vlan50
  description Network for the WGB
  ip address 172.17.92.1 255.255.255.0
  ip helper-address 10.2.5.2
!
interface Vlan901
  description Network for CAPWAP tunnel to WLC
  ip address 172.17.91.1 255.255.255.0
  ip helper-address 10.2.5.2
!
```

**Wireless LAN Controller**

The Wireless LAN Controller (WLC) is used for managing multiple LAPs from a single location. The first step in setting up the WLC is to set up the management interface. This interface is used by the WLC to form a CAPWAP tunnel to the LAP for communication and management. The management interface here is on a separate subnet and VLAN as it is a part of the data center. The LWAP APs are hanging off the yard network, which is a part of a separate subnet. The WLC communicates to the LWAP over the implemented WAN.

Set up the WLAN SSID for the yard network that will be used by the APs to connect to the vehicles.

**VLAN 50 is the VLAN that is used by GMM for the WGB. Because of this, the VLAN for WGB traffic on the switch must be the same.**

**Figure 49  WLAN SSID**
The following fields must be filled in:

- Enter the **Profile Name**.
- Enter the **SSID**.
- Set status to **Enabled**.
- Set Interface/Interface Group to **management**.
- Disable **Broadcast SSID** for security reasons.

**Figure 50   WLAN SSID Configuration**

![WLAN SSID Configuration](image)

Afterwards, click the **Security** tab and configure the security as either **PSK** or **802.1X**.

**PSK Configuration**

To configure PSK:

1. Select **WPA2 Policy**.
2. Select **AES** as the WPA2 Encryption.
3. Enable **PSK**.
4. Set PSK Format to **ASCII**.
5. Enter desired WGB network password into the following field.
802.1X Configuration

To configure 802.1X:

1. Navigate to the Security tab at the top of the web browser.

2. Add the RADIUS server that is to be used for 802.1X authentication/

3. Navigate to the Security tab within the SSID configuration.

4. Select 802.1X.
5. Navigate to the **AAA Servers** tab.

6. Select the server that was added in Step 2.

---

**Figure 53  802.1X Authentication Key Management**

![802.1X Authentication Key Management](image)

**Figure 54  Apply AAA Server to SSID**

![Apply AAA Server to SSID](image)
Fixed AP Deployment

In the Cisco Remote and Mobile Assets solution, the FlexConnect configuration is used. This allows the data traffic to be switched over the local network as opposed to going over the CAPWAP tunnel to WLC. This cuts down on inefficient pathing of data traffic and decreases the workload for the WLC. The FlexConnect base configuration is as follows:

**Figure 55  WLC Wireless Configuration**

Once the AP has been added, change the AP Mode to **FlexConnect**, under the **General** tab. The AP will then reboot.

**Figure 56  Change the AP Mode to FlexConnect**

Once in FlexConnect mode, change the configuration in the **FlexConnect** tab of the LWAP to map it to the correct VLANs for control and data traffic. All control traffic between AP and WLC is on native VLAN 901 in this configuration. The VLAN must be native since it will be not tagged with VLAN 901 by the LAP.

**Figure 57  FlexConnect VLAN Mapping**

7. To configure the WGB client traffic, select **VLAN Mappings**.
8. All WGB client traffic must flow on VLAN 50 as shown below.

**Figure 58  Yard AP VLAN Mapping**

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP88f0.31e8.b1fc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Radio MAC</td>
<td>50:87:89:9f:4d:50</td>
</tr>
</tbody>
</table>

**WLAN VLAN Mapping**

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>SSID</th>
<th>VLAN ID</th>
<th>NAT-PAT Inheritance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yard_RMA</td>
<td>50</td>
<td>no AP-specific</td>
</tr>
</tbody>
</table>

**Centrally switched Wlans**

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>SSID</th>
<th>VLAN ID</th>
</tr>
</thead>
</table>

**AP level VLAN ACL Mapping**

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Ingress ACL</th>
<th>Egress ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Group level VLAN ACL Mapping**

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Ingress ACL</th>
<th>Egress ACL</th>
</tr>
</thead>
</table>

Foot Notes

1. VLAN does not take effect for NAT-PAT enabled WLANs.

**Extending the Enterprise Network**

Part of the power of the Cisco Remote and Mobile Assets solution is the ability to extend the enterprise network all the way to the gateway for devices and hotspot clients. This allows for critical communication between these users/devices and the data center applications.

**WAN**

The following three WAN configuration options exist for connecting the gateway to a remote data center and/or the Internet:

- LTE
- Ethernet
- Workgroup Bridge
LTE

The cellular interfaces can be used as the WAN uplinks to the data center and general Internet. Both public and private APNs can be used, and dual LTE IR 829s can be configured as either active/standby or active/active.

- In the active/standby scenario, only one LTE interface will be in use at a given time. If Internet reachability goes down on that interface, both LTE interfaces are reset and the first to get an IP address back will be used.
- In the active/active scenario, both LTE interfaces are in use at the same time, and traffic is load balanced across them. However, site-to-site VPN cannot be configured with this feature because of technical limitations.

**WAN Interface**

The WAN setting is applicable only for gateways being claimed for the first time or being claimed after the factory reset.

<table>
<thead>
<tr>
<th>Primary APN (SIM 0)</th>
<th>Secondary APN (SIM 1)</th>
</tr>
</thead>
</table>

**Dual LTE**

Supported only by dual LTE gateway models. Any mode changes will interrupt network traffic.

- Default Load Balancing
- Custom Load Balancing

Ethernet

The Ethernet interface can also be used as the WAN uplink. This is useful for cutting down on data usage when possible, such as for demos or for remote gateways that will have a permanent ethernet link available.

To configure an Ethernet interface as the WAN uplink:

1. Disable WAN Interface. This will force the WAN configuration defined during provisioning to be used.
2. Use the GPT tool to provision the gateway, specifying the gigabit Ethernet 1 interface as the WAN uplink.

Workgroup Bridge

WGB allows a gateway and connected devices to use to an existing Wi-Fi network for Internet connectivity and communication with Cisco Kinetic. This feature is used to off-load cellular traffic to the Wi-Fi network.

This is useful when high volume of data, such as video data, needs to be transferred from the subtended device to a server in the corporate network or data center. Sending that data over a 4G cellular link can be slow and expensive.

When a gateway enters into the range of the WGB network, it will automatically receive a DHCP address and start routing traffic over the wireless network with minimal packet loss. However, when the gateway then leaves the WGB range it will take potentially a minute or two to restore cellular connectivity. This is due to the way GMM manages cellular connections.

To configure Workgroup Bridge:

1. Enable Workgroup Bridge.
2. Enter the SSID for the WGB network under **SSID**.
3. Enter the password for the WGB network under **Pre-shared Kay**.
Remote and Mobile Assets

Part IV: Sample Configurations

Figure 59  Configuring Workgroup Bridge

<table>
<thead>
<tr>
<th>WGB</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td></td>
</tr>
<tr>
<td>yard</td>
<td></td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>*********</td>
</tr>
</tbody>
</table>

LAN

Custom Subnet

If the Custom Subnet feature is enabled, then the configuration of the user wireless network can be customized. In this case, the gateway will provide DHCP service to subtended devices using the network specified in the Default Gateway IP and Default Gateway Netmask fields. The LAN IP entered will be the default gateway for connected devices. The DNS IP will point to the DNS server for the DHCP clients on the subtended network.

To configure a custom subnet:

1. Enable **Custom Subnet**.
2. Enter the network and subnet mask (e.g., 172.18.136.1/24).
3. Enter the IP address for the desired DNS server.
4. If some addresses are to be reserved, enter the first reserved address under **Exclusion Range start**.
5. Enter the last address under **Exclusion Range end**.

Figure 60  Configuring a Custom Subnet

<table>
<thead>
<tr>
<th>Custom Subnet</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

NAT will be turned ON for the default setting. If you need to turn OFF NAT or customize subnet range for individual GW’s, use “Advanced” Option.

- Default Gateway IP: 192.168.0.1
- Default Gateway Netmask: 255.255.255.0
- DNS IP (Optional): 8.8.8.8
- Exclusion Range (Optional): 192.168.0.2 - 192.168.0.10

If the Custom Subnet feature is disabled, then the wireless network will be given a default configuration:

- A /28 subnet in the 10.8.0.0/16 network range.
- The default router for the network will be the IP address of the gateway.
- The DNS server will be the DNS server provided to the gateway from the uplink interface.

Additionally, the Custom Subnet is configured to either use NAT or a routed mode of communication with the data center and Internet.

802.1x authentication is not supported for the WGB network itself.
Routed Mode

The routed mode advertises the subtended network out through the site-to-site Tunnel. If this is implemented, then devices in the data center will be able to reach subtended devices directly (with no need for port forwarding). The downside is that the subtended networks must now be unique. If they are not, IP overlap issues could occur where two different gateways hand out the same IP address to a subtended device. In that case, an application in the data center would potentially send traffic over the wrong tunnel to the wrong device.

To configure routed mode, the Custom Subnet must first be set to Advanced.

Figure 61  Configuring Routed Mode: Set Custom Subnet to Advanced

Afterwards:

1. Select Gateways in the GMM Portal.
2. Select the desired gateway from the list.
3. Click the Networking tab.
4. Click Advanced Configuration.
5. Click Site-to-site and Custom Subnet.
6. Disable NAT.

Figure 62  Configuring Routed Mode: Advanced Configuration
NAT Mode

The NAT mode keeps the desired Custom Subnet completely hidden behind the WAN interface (either the Site-to-Site Tunnel Interface or WGB Interface). This allows for the same Custom Subnet to be used for multiple subtended networks.

For NAT mode, the custom subnet can be configured as either Default or Advanced. If Advanced is selected (location outlined in Routed Mode), make sure that NAT is enabled, as indicated in the image below.

![Figure 63 Configuring NAT Mode](image)

In order for VMs in the data center to access devices on the custom directly, the appropriate port forwarding statements must be configured in GMM.

Port Forwarding

Port forwarding is used to communicate with subtended devices behind NAT on a gateway.

When a device is NAT’d behind a gateway (such as a camera), then all data will appear to come from the gateway itself. This means that when the application in the data center tries to respond, it will send traffic back to the gateway instead of the device. However, you can use site-to-site VPN to establish a tunnel from the corporate network to the gateway. Then use Port Forwarding to define the IP addresses and ports used to communicate with the subtended devices behind the gateway NAT. Then when the application in the data center tries to communicate on a specific port, that traffic will be forwarded from the gateway to the device. In order to configure Port Forwarding:

1. Enable Port Forwarding in the custom subnet configuration.
2. For each desired device, enter:
   - **Name**—Name of the device
   - **Gateway Port**—Gateway Port number used to communicate with the subtended devices
   - **Protocol**—TCP or UDP
   - **Device IP**—IP Address of the corresponding device
   - **Device Port**—Destination port on device
Wireless Hotspot

The Wi-Fi feature configures the gateway to provide a Wi-Fi hotspot for local wireless devices. The Wi-Fi network is bridged to the same network as the subtended network of the LAN ports.

The IR 829 internal AP can be configured in two different modes:

- Unified
- Autonomous

**Unified**

Unified mode allows for the internal AP to be completely managed by a Cisco WLC, in place of supplying an SSID and Authentication method manually.

To configure Unified Mode:

1. Set up the WLC as defined in Cisco Wireless LAN Controller, page 53.
2. Select **Unified AP**.
3. Enter the IP address of the desired WLC.

**Autonomous**

Autonomous mode allows for applying SSID and Authentication configuration to the internal AP. It also allows WGB to be used.

To configure Autonomous mode:

1. Select **Autonomous** under AP Mode.
2. Enable **Wi-Fi**.
Remote and Mobile Assets

Part IV: Sample Configurations

3. Select **Wi-Fi Authentication**:
   a. Pre-shared Key
   b. Dot1x

**Pre-shared Key**

If PSK is configured, any user trying to join the hotspot must enter a password that matches the defined PSK.

To finish the PSK configuration:

1. Enter the PSK in the field next to SSID.

   **Figure 67 Pre-shared Key Configuration**

**802.1x Authentication**

If 802.1x is configured, then all authentication will be handled by a designated RADIUS server or the WLC.

To finish the 802.1x configuration:

1. Enter the IP address of the RADIUS server under RADIUS Server 1 IP.
2. Enter the key for the RADIUS server under RADIUS Server 1 Key.

   **Figure 68 802.1x Configuration**

RADIUS Server installation instructions can be found in RADIUS Server, page 87.
SSID Options

The SSID name itself can either be manually defined or auto-generated (with an optional user-defined prefix). In either case, broadcasting the SSID can be enabled or disabled. If the SSID is broadcast, then it will show up as a selectable network for the hotspot client. If not, then the SSID will have to be entered manually for the client to join.

**Figure 69  Manually Defined SSID**

- **SSID Generation**
  - Manually Enter SSID & PSK
- **Default**
- **SSID**
  - Hotspot
- **SSID Broadcast**
  - ENABLED

**Figure 70  Auto-Generated SSID with Prefix**

- **SSID Generation**
  - Auto-Generate SSID & PSK (Recommended)
- **SSID Prefix**
  - `ssdi_prefix`
- **SSID Broadcast**
  - ENABLED

**Wired**

The LAN Ports configuration allows the gateway’s Gigabit Ethernet ports to be enabled or disabled. While disabled, the ports are shut down to avoid unauthorized access. If they are enabled, clients may connect via an Ethernet cable to the Gigabit Ethernet ports on the gateway. In the case a client has a statically assigned an IP address, it needs to fall within the **Exclusion Range** defined in Custom Subnet. Otherwise, the same IP address may end up existing on two separate devices. Conversely, clients that are configured for DHCP will receive a network configuration as defined in **Custom Subnet**.

**Figure 71  Enabling LAN Ports**

- **LAN Ports**
  - GigabitEthernet 1
  - GigabitEthernet 2
  - GigabitEthernet 3
  - GigabitEthernet 4
  - GigabitEthernet 1 can be used as a LAN interface only if the gateway’s Primary Link is Cellular.
Virtual Routing and Forwarding for Overlapping IP

VRF can be enabled in order to keep the routing table for the subtended network separate from the global routing table of the gateway. VRF is mandatory when the destination network for user traffic overlaps with the 10.0.0.0/8 range. Many subnets in this range are a part of the Kinetic infrastructure, and user traffic can possibly be sent to the wrong location if VRF is not enabled.

![Figure 72 Enabling Virtual Routing and Forwarding](image)

Custom Configuration Templates

GMM allows the use of Custom Configuration templates to apply additional Cisco IOS configurations. This chapter contains some examples of these configurations. All of these templates must be manually created by the customer and applied through the GMM support team.

- Firewall
- Quality of Service
- Ignition Sensing

The configurations must be reviewed and approved before they can be applied to an organization, and certain rules must be followed:

- Do not change any configuration related to CGNA
- Do not use/modify/delete the "admin" or "operator" user.
- Do not use/modify/delete profile names "Flex_IKEv2" or "CVPN_I2PF".
- Do not use/modify/delete tunnel interface numbers 1 or 2.
- Do not use/modify/delete tracking object numbers 2 or 4.
- Do not use/modify/delete dialer number 1, dialer-list 1 or Virtual-Template1
- Do not use/modify/delete VLAN 555
- Do not use/modify/delete route-maps "RM_Tu2" or "RM_WAN_ACL"
- Do not use/modify/delete ACL names "NAT_ACL", "GWIPS".
Additionally, there are some predefined variables that can be used in the flexible template:

- \texttt{gw.sn} - GW Serial Number
- \texttt{gw.model} - GW Model
- \texttt{gw.wan_if} - GW’s WAN interface
- \texttt{gw.wan_if_sec} - GW’s Secondary WAN interface (e.g. Dual LTE)
- \texttt{gw.subnet} - Subnet for GW’s 32 IPs
- \texttt{gw.netmask} - GW’s 32 IP’s subnet mask
- \texttt{gw.ip} - GW’s IP
- \texttt{gw.ip_prefix} - GW IP’s first 3 numbers, separated by "." (this makes calculating IPs easier)
- \texttt{gw.ip_suffix} - GW IP’s last byte
- \texttt{gw.gos_ip} - GW’s GuestOS IP
- \texttt{gw.lan_ip} - GW’s LAN IP
- \texttt{gw.lan_subnet} - GW’s LAN subnet

The following sections contain examples of custom configuration that can be enabled with GMM.

**Firewall**

The following code would permit an incoming connection destined for IOx App port 9443 from the WAN interface:

```
ip nat inside source static tcp \{gw.gos_ip\} 9443 interface \{gw.wan_if\} 9443
ip access-list extended filter-Internet
   permit tcp any any eq 9443
```

```bash
ip nat inside source static tcp {{gw.gos_ip}} 9443 interface {{gw.wan_if}} 9443
ip access-list extended filter-Internet
   permit tcp any any eq 9443
```
Quality of Service

The following QoS policy is meant to be an example of one that could be configured on a Cisco IR using the Kinetic GMM Custom Configuration feature. In general, the details of the QoS policy should align with the goals, specific applications, traffic patterns, and priorities of a customer; therefore, they will all be unique.

In the example below, the configuration consists of three basic parts:

1. The Class Map defines which types of traffic to match on for further processing, and places those types of matched traffic in specific classes which will each be treated differently. In this example, the class-map matches on the IP Precedence number (either 3, 4, or 5), and also matches on an Access Control List.

2. The Policy Map defines what kind of policy (limitation or action) should be applied to each traffic class as defined in the class map. Two policy maps are defined, and SUB-CLASS-34 is referenced by PNTM-A, which makes this a nested policy map. Within SUB-CLASS-34, the bandwidth for these traffic classes is limited to a value of 150 or 200 (in units of Kilobits Per Second). The PNTM-A policy also applies a shaping limit, priority queuing, and fair queuing to different classes.

3. The policy is finally applied to the Cellular interface on the gateway. The QoS policy will only take effect during times of congestion. If the interface is not congested, the traffic forwarded through the interface will not be limited.

For additional details about how to configure QoS on Cisco IOS, refer to the QoS section of the Cisco 800M Series ISR Software Configuration Guide:


```
class-map match-any CS5-EF
  match ip precedence 5
class-map match-any PREC-3
  match ip precedence 3
class-map match-any PREC-4
  match ip precedence 4
class-map match-any CS3-4
  match ip precedence 3 4
  match access-group 105

policy-map SUB-CLASS-34
  class PREC-3
    bandwidth 150
  class PREC-4
    bandwidth 200
policy-map PNTM-A
  class CS5-EF
    priority 100
  class CS3-4
    bandwidth 400
    shape average 400000
    service-policy SUB-CLASS-34
  class class-default
    fair-queue
    random-detect dscp-based
policy-map LTE-SHAPER
  class class-default
    shape average 1500000
    service-policy PNTM-A

! interface Cellular0
  service-policy output LTE-SHAPER
  access-list 105 permit udp any any eq mobile-ip
```
Ignition Sensing

With ignition sensing, the gateway can be configured to shut down when the engine is off for a predefined amount of time (in seconds) or when the voltage received by the gateway is below a certain threshold (in volts). Fractional voltage (such as 12.6) is configurable.

```plaintext
ignition off-timer 900
ignition undervoltage threshold 11
ignition enable
```

Headend Router Configuration

The following is a sample Python script that uses the GMM Restful APIs to generate the FlexVPN headend router configuration that can be pasted into the HER(s) to help ease configuration.

**Script to Generate HER Configuration**

```python
import requests
import json
import argparse

# Retrieve GMM Auth Token
def get_token(uid, pwd):
    token_resp = requests.post('https://us.ciscokinetic.io/api/v2/users/access_token',
                                json={'email': uid, "password": pwd})
    if token_resp.status_code != 200:
        print("Failed to receive GMM Auth Token with error: " + str(token_resp.status_code))
    else:
        data = json.loads(token_resp.content)
        access_token = data['access_token']
        print("User Access Token: " + access_token)
        print("")
        return access_token

# Build HTTP Header for Future Requests
def build_header(access_token):
    headers = {}  # Get Authorization
    headers['Authorization'] = 'Token ' + access_token
    headers['Accept'] = 'application/json'
    return headers

# Retrieve Gateway Status for our Orgs
def gwy_status(org_id, headers):
    url = 'https://us.ciscokinetic.io/api/v2/organizations/' + str(org_id) + '/gateways/
    gwy_list_response = requests.get(url, headers=headers)
    if gwy_list_response.status_code != 200:
        print("Retrieving Gateway List Failed with error: " + str(gwy_list_response.status_code))
    else:
        gateways = json.loads(gwy_list_response.content)
        print("GMM Gateway Summary:")
        print("Number of gwys UP: " + str(gateways['summary']['up']))
        print("Number of gwys DOWN: " + str(gateways['summary']['down']))
        print("Number of gwys CLAIMING: " + str(gateways['summary']['claiming']))
        print("Number of gwys IN_PROGRESS: " + str(gateways['summary']['in_progress']))
```
print("Number of gwys INACTIVE: " + str(gateways['summary']['inactive']))
print("Number of gwys FAILED: " + str(gateways['summary']['failed']))

print('""')
print('"GMM Gateway Status:"
for i in range(len(gateways['gate_ways'])):
  print("Gateway " + str(gateways['gate_ways'][i]['uuid']) + " Status: " +
  str(gateways['gate_ways'][i]['status']))
return gateways

def build_he_config(gateways, domain, psk):
  # Build HE Configuration
  print('""
  print("FlexVPN Hub Configuration:"
  print('"\n"
  print("ip access-list standard CLOUD"
  print(" permit 192.168.100.0 0.0.0.255")
  print(" permit 172.31.0.0 0.0.255.255")
  print(" permit any")
  print('"\n"
  print("crypto ikev2 keyring field_keys")
  for i in range(len(gateways['gate_ways'])):
    print(" peer " + str(gateways['gate_ways'][i]['uuid']) +
    print(" identity email " + str(gateways['gate_ways'][i]['uuid']) + "@" + domain)
    print(" pre-shared-key " + psk)
    print('""

def main():
  parser = argparse.ArgumentParser()
  parser.add_argument('-u', '--gmm_user_name', required=True, help="GMM User Name")
  parser.add_argument('-p', '--gmm_password', required=True, help="GMM Password")
  parser.add_argument('-oid', '--gmm_org_id', required=True, help="GMM Org Id")
  parser.add_argument('-psk', '--flex_vpn_psk', required=True, help="FlexVPN PSK")
  parser.add_argument('-d', '--domain', required=True, help="FlexVPN Identity email domain")
  args = parser.parse_args()
  gmm_uid = args.gmm_user_name
  gmm_pwd = args.gmm_password
  gmm_org_id = args.gmm_org_id
  flex_vpn_psk = args.flex_vpn_psk
  domain = args.domain
  gmm_access_token = get_token(gmm_uid, gmm_pwd)
  headers = build_header(gmm_access_token)
  gateways = gwy_status(gmm_org_id, headers)
  build_he_config(gateways, domain, flex_vpn_psk)
if __name__ == '__main__':
  main()
Getting Help

```bash
$ python3.6 gmm_gwy_status.py -h
usage: gmm_gwy_status.py [-h] -u GMM_USER_NAME -p GMM_PASSWORD -oid GMM_ORG_ID
                  -psk FLEX_VPN_PSK -d DOMAIN
optional arguments:
  -h, --help            show this help message and exit
  -u GMM_USER_NAME, --gmm_user_name GMM_USER_NAME
  GMM User Name
  -p GMM_PASSWORD, --gmm_password GMM_PASSWORD
  GMM Password
  -oid GMM_ORG_ID, --gmm_org_id GMM_ORG_ID
  GMM Org Id
  -psk FLEX_VPN_PSK, --flex_vpn_psk FLEX_VPN_PSK
  FlexVPN PSK
  -d DOMAIN, --domain
  FlexVPN Identity email domain
```

Running the Script

```bash
$ python3.6 gmm_gwy_status.py -u 'test@cisco.com' -p 'password' -oid 1234 -psk 'C!sc0123#' -d "iotspdev.io"
User Access Token: 23dad30abfddb17c.268jPhWrg5sd6xvis0-BoircW6Qq_fA5ReMfLe1xM

GMM Gateway Summary:
Number of gwys UP: 2
Number of gwys DOWN: 0
Number of gwys CLAIMING: 1
Number of gwys IN_PROGRESS: 0
Number of gwys INACTIVE: 1
Number of gwys FAILED: 0

GMM Gateway Status:
Gateway FTX00000001 Status: Healthy
Gateway FTX00000002 Status: Healthy
Gateway FTX00000003 Status: Inactive
```

FlexVPN Hub Configuration

```bash
!
ip access-list standard CLOUD
  permit 192.168.100.0 0.0.0.255
  permit 172.31.0.0 0.0.255.255
  permit any
!
crypto ikev2 keyring field_keys
  peer FTX00000001
    identity email FTX000000001@iotspdev.io
    pre-shared-key C!sc0123#
  peer FTX00000002
    identity email FTX000000002@iotspdev.io
    pre-shared-key C!sc0123#
  peer FTX00000003
    identity email FTX000000003@iotspdev.io
    pre-shared-key C!sc0123#
!
```
Appendix

This appendix includes the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordering Information, page 107</td>
<td>GMM gateway compatibility table and information on ordering Industrial Routers, the GMM subscription and services and support.</td>
</tr>
<tr>
<td>Common Gateway Issues, page 109</td>
<td>An aid to assist with typical issues faced when provisioning a gateway.</td>
</tr>
<tr>
<td>Firewall Ports for GMM to Gateway Communication, page 111</td>
<td>Port settings and IP protocols for gateways that are installed behind a firewall.</td>
</tr>
<tr>
<td>A Sample GMM Report, page 113</td>
<td>Sample CSV-downloadable report from GMM that provides a wealth of gateway information.</td>
</tr>
<tr>
<td>IOx and Fog Applications, page 114</td>
<td>Introduction to IOx and fog computing and where to find more information</td>
</tr>
</tbody>
</table>

### Ordering Information

An updated list of supported hardware and firmware versions is maintained at:

- [https://developer.cisco.com/docs/kinetic/#!supported-gateways-and-firmware/supported-gateways](https://developer.cisco.com/docs/kinetic/#!supported-gateways-and-firmware/supported-gateways)

To enable Cisco Kinetic GMM on IR809 and IR829 gateways, order this option under IR8x9 in the catalog:

- **Option PID: IR-CLOUD-MGMT**—Enable the gateway to be ready for cloud management.

Full ordering information is covered in the Ordering Guide:


When ordering new gateways for greenfield deployments, use one of the following base SKUs:

- IR807
- IR809
- IR829

Once the base SKU is selected, options for specific hardware models and Kinetic GMM subscription terms are made available. The available hardware SKUs supported in Kinetic GMM are listed below in **GMM Gateway Compatibility, page 107**.

### GMM Gateway Compatibility

GMM supports the management of Cisco IR 8x9 series gateways, which currently includes IR807, IR809, and IR829 models, as shown in **Table 10**:

**Table 10  GMM Gateway Compatibility**

<table>
<thead>
<tr>
<th>Region</th>
<th>IR807</th>
<th>IR809</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (US ATandT, Canada)</td>
<td>IR807G-LTE-NA-K9</td>
<td>IR809G-LTE-NA-K9</td>
</tr>
<tr>
<td>Europe</td>
<td>IR807G-LTE-GA-K9</td>
<td>IR809G-LTE-GA-K9</td>
</tr>
<tr>
<td>APJC and Latin America</td>
<td>--</td>
<td>IR809G-LTE-LA-K9</td>
</tr>
</tbody>
</table>
Because of the differences in LTE bands supported by different operators across the globe, we encourage you to consult in-country sales resources to validate ordering information for your country. Table 11 contains the available SKUs when this document was developed.

Table 11  Available SKUs by Region

<table>
<thead>
<tr>
<th>Region</th>
<th>IR829M (with mSATA + PoE Option, Single or Dual LTE)</th>
<th>IR829B (Single LTE, No mSATA or PoE)</th>
<th>IR829-2LTE (Dual LTE, PoE Option, no mSATA)</th>
<th>IR829GW (PoE option, no mSATA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (US AT&amp;T)</td>
<td>IR829M-LTE-EA-BK9</td>
<td>IR829B-LTE-EA-BK9</td>
<td>IR829-2LTE-EA-BK9</td>
<td>--</td>
</tr>
<tr>
<td>US-Verizon</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>IR829GW-LTE-VZ-AK9</td>
</tr>
<tr>
<td>Canada</td>
<td>IR829M-LTE-EA-AK9</td>
<td>IR829B-LTE-EA-AK9</td>
<td>IR829-2LTE-EA-AK9</td>
<td>IR829GW-LTE-NA-AK9</td>
</tr>
<tr>
<td>APJIC</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Australia, New Zealand, China</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Korea</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Latin America</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Panama</td>
<td>IR829M-LTE-LA-ZK9</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

Ordering information is covered in the Ordering Guide here:


GMM Subscription Details

GMM is available as part of the Cisco Kinetic platform subscription. Cloud-hosted GMM is sold based on the number of gateways under management. You can purchase a subscription for a 12, 36, or 60-month period. Since Cisco Kinetic GMM is a cloud-hosted platform, you will automatically receive periodic updates so you always have the latest version of the software. You can choose to prepay the subscription price for the entire term or on an annualized basis.

GMM Services and Support

Your GMM base software subscription entitles you to limited 12x5 phone/TAC support. The limited support includes access to trained TAC personnel via phone, web and email as well as continuous monitoring of the Kinetic Cloud Operations. You can also access online resources including the knowledge base and tutorials. No additional products, licenses or fees are required to access basic support services with the Cisco Kinetic GMM subscription. Enhanced support is available for an additional fee.
Common Gateway Issues

**Stuck in Registering for more than 10 mins**
This usually indicates that the gateway is not able to contact Cisco Kinetic:
- For cellular gateways, ensure that a SIM card was inserted and has a valid data plan.
- If using Ethernet gateways, verify that the required network ports are open and that no firewalls are blocking the gateway from reaching the Internet.

**Stuck in the In Progress State for more than 10 mins**
- Ensure that the gateway did not go offline and Internet connectivity is still present.
- Check the Gateway Event Logs under the Gateway Details page to see if the gateway registered successfully and was configured.
- Verify that the WAN interface configuration is correct in the template used to claim the gateway.

**Gateway is in Failed State**
- Ensure that the gateway did not go offline and Internet connectivity is still present.
- Check that the gateway model and model for the associated template are the same.
- Verify that the WAN interface configuration is correct in the template used to claim the gateway.

**GPS Troubleshooting**
If the gateway location is not being updated correctly on the map view:
- Wait for the update to occur. The gateway location is updated every 30 seconds.
- Verify that GPS is enabled in the Gateway Details > Current Config page.
- If GPS is not in enabled state, check if the gateway was claimed using a configuration that enabled GPS. This can be checked in the Gateway Event Logs. There will be an entry such as Gateway was configured using configuration xyz.
- Delete and reclaim the gateway with the correct configuration, if required.
- Ensure that the correct GPS antennas are attached to the gateway.

**Login Troubleshooting**
- Ensure that you or your user has a valid account in the portal.
- Click Forgot Password to reset a password.

**Private Subnet Troubleshooting**
If the devices connected to the gateway are not getting assigned the right DHCP IP addresses:
- If private subnet is not enabled, the devices will be assigned IP addresses from Cisco Kinetic.
- Verify that the private subnet is enabled in the Gateway Details > Current Config page.
- If private subnet is not enabled, check if the gateway was claimed using a configuration that enabled private subnet. This can be checked in the Gateway Event Logs. There will be an entry like Gateway was configured using configuration xyz.
Remote and Mobile Assets

Appendix

- Verify that the configuration details entered for configuration are correct.
- Delete and reclaim the gateway with the correct configuration, if required.

Customer VPN Troubleshooting

If the gateway is not able to establish a tunnel with the HER:
- Verify that VPN is enabled in the Gateway Current Config page.
- If the VPN is not enabled, check if the device was claimed using a configuration that enabled the Customer VPN. This can be checked in the Gateway Event Logs. There will be an entry like Gateway was configured using configuration xyz.
- Verify that the details entered for the VPN configuration are correct.
- Delete and reclaim the gateway with the correct configuration, if required.
- Verify that the configuration on your HER is correct, and that it allows the gateways to establish tunnels with the provided configuration.

Note: A known issue exists where site-to-site VPN tunnels and the site-to-site VPN tunnel IP Address in the Gateway Details page can take up to 30 mins to update after it is successfully enabled.

WGB Troubleshooting

If the gateway is not able to connect to the root access point:
- Verify that WGB is enabled in the Gateway Details > Current Config page.
- If it is not enabled, check if the gateway was claimed using a configuration that enabled WGB. This can be checked in the Gateway Event Logs. There will be an entry such as Gateway was configured using configuration xyz.
- Confirm that the details entered for the WGB configuration are correct.
- Delete and reclaim the gateway with the correct configuration, if required.
- Ensure that the correct antennas are attached to the gateway.
- WGB is supported only on the 5GHz radio. Verify that the root access point is compatible with this.
- Make sure the radio frequencies between AP and the WGB device are in the same domain and have a common frequency.
  - Use the command show controller Dot11 1 frequency to display the frequency channels.
  - Ideally, there will be many overlapping non-DFS channel between the IR829 gateway’s AP and the root AP.

Note: WGB is supported only on IR829 gateways that use cellular as the uplink (not supported on IR809 gateways and Ethernet enabled IR829 gateways.

Wi-Fi Troubleshooting

If you are not able to connect any devices to the Wi-Fi hotspot configured on the gateway:
- Ensure that the correct SSID and preshared key are entered into the device.
- Ensure that the correct antenna is attached to the gateway and that the device is within range.
- Verify that Wi-Fi is enabled in the Gateway Details > Current Config page.
- If Wi-Fi is not enabled, check if the gateway was claimed using a configuration that enabled Wi-Fi. This can be checked in the Gateway Event Logs. There will be an entry such as Gateway was configured using configuration xyz.
Delete and reclaim the gateway with the correct configuration, if required.

If WGB is also enabled on the gateway, then Wi-Fi works only on the 2.4 GHz radio.

**Wi-Fi is supported only on the IR829 gateways (not supported on IR809 devices).**

For additional information on troubleshooting:

- [https://developer.cisco.com/docs/kinetic/#!deploy-your-gateways/troubleshooting](https://developer.cisco.com/docs/kinetic/#!deploy-your-gateways/troubleshooting)

### Firewall Ports for GMM to Gateway Communication

Cisco Kinetic requires specific TCP/UDP network ports and IP protocols to be opened on the network firewall to communicate with the gateways. Please refer to Part IV: Sample Configurations, page 78 for the recommended settings.

#### Table 12  TCP/UDP Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Description</th>
<th>Required for Kinetic Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>UDP</td>
<td>IP of assigned DNS Server</td>
<td>GW must have access to DNS resolution service. Domain Name System (DNS) us.ciscokinetic.io eu.ciscokinetic.io</td>
<td>GMM and DCM</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>NTP Server: 129.6.15.30</td>
<td>Network Time Protocol (NTP)</td>
<td>GMM and DCM</td>
</tr>
<tr>
<td>500</td>
<td>UDP</td>
<td>US Cluster: 34.208.182.252 EU Cluster: 34.240.190.128</td>
<td>Bidirectional access is required for the Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)</td>
<td>GMM and DCM</td>
</tr>
<tr>
<td>4500</td>
<td>UDP</td>
<td>US Cluster: 34.208.182.252 EU Cluster: 34.240.190.128</td>
<td>Bidirectional access is required for IPSec NAT Traversal</td>
<td>GMM and DCM</td>
</tr>
<tr>
<td>8883</td>
<td>TCP</td>
<td>US Cluster: Name resolution of us.ciscokinetic.io EU Cluster: Name resolution of eu.ciscokinetic.io</td>
<td>Secure MQTT (MQTT over TLS) for the data pipeline. Required for Cisco Kinetic DCM only when publishing to the Kinetic cloud. You can use MQTT over Web sockets (TCP 443) instead.</td>
<td>DCM</td>
</tr>
</tbody>
</table>
Table 12  TCP/UDP Ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>US Cluster: Name resolution of mqtt-us.ciscokinetic.io</th>
<th>EU Cluster: Name resolution of mqtt-eu.ciscokinetic.io</th>
<th>Secure MQTT (MQTT over Web Socket) for the data pipeline. Required for Cisco Kinetic DCM only when publishing to the Kinetic Cloud. Can use MQTT over TLS instead.</th>
</tr>
</thead>
</table>
| 443  | TCP      | The DNS name us.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
|      |          | The DNS name eu.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
| 9123 | TCP      | US Cluster: Name resolution of us.ciscokinetic.io    | EU Cluster: Name resolution of eu.ciscokinetic.io   | Call-home registration. Required for all gateways shipped from Cisco November 15, 2018 or earlier, or if the gateway was provisioned using a GPT version 1.91.2.7 or earlier. |
|      |          | The DNS name us.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
|      |          | The DNS name eu.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
| 9124 | TCP      | US Cluster: Name resolution of us.ciscokinetic.io    | EU Cluster: Name resolution of eu.ciscokinetic.io   | Call-home registration. Required for all gateways shipped from Cisco on or after November 16, 2018 or if the gateway was provisioned using GPT version 1.91.2.8 or later. |
|      |          | The DNS name us.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
|      |          | The DNS name eu.ciscokinetic.io resolves to:         |                                                      | 54.71.117.77  
34.216.139.206  
52.11.218.197  
52.212.193.126  
54.194.175.23  
34.252.252.200 |
A Sample GMM Report

Figure 74 is a sample report:

### Table 13  IP Protocol Requirements

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Description</th>
<th>Required for Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>IP</td>
<td>US Cluster: 34.208.182.252</td>
<td>Encapsulating Security Payload (ESP)</td>
<td>GMM and DCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EU Cluster: 34.240.190.128</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Figure 74  Sample GMM Report

**Report Name** - Cell Report

**Data Range**: 2019-01-15 - 2019-01-16

**Report generated time**: 2019-01-16 21:38:23 UTC

<table>
<thead>
<tr>
<th>Gateway Name</th>
<th>Gateway Serial Number</th>
<th>Model</th>
<th>US-LTE ID</th>
<th>Group (c)</th>
<th>SubnetEffDevice - IP Address</th>
<th>SubnetEffDevice - VNI</th>
<th>SubnetEffDevice - MAC/Class ID</th>
<th>Carrier_1 IP Address</th>
<th>Carrier_1 IP Address</th>
<th>Carrier_1 IP Address</th>
<th>IRIE_1</th>
<th>CCCH_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japanish Deck</td>
<td>PCCW221050A5</td>
<td>DAE52</td>
<td>LTE-V2</td>
<td>NJM</td>
<td>100.163.16.102</td>
<td>156757325031109</td>
<td>91408305005448480</td>
<td>no carrier case</td>
<td>no carrier case</td>
<td>no carrier case</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTE2145001</td>
<td>DAE52</td>
<td>LTE-V2</td>
<td>NJM</td>
<td>3540836832851567</td>
<td>91408305005448480</td>
<td>100.123.15.76</td>
<td>no carrier case</td>
<td>no carrier case</td>
<td>no carrier case</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Demo ESP        | FTE2210091           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | no carrier case               | no carrier case         | no carrier case         | no carrier case         |        |       |

| Factory_HQ ESP  | FTE2210495           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| E2P2 LTE Site 2 | JWK2252001           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| SOF example     | PW2115001M           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Tissue Lab      | FTE21109011          | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Tissue perfest  | FTE2145003           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Tissue ESP      | FTE2210201           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Japanish Desk   | PCCW221050A5         | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Remote ESP      | FTE2210505           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

| Remote ESP      | FTE2210506           | DAE52 | LTE-V2  | NJM       | 100.122.10.109              | 91408305005448480     | VZW                           | no carrier case         | no carrier case         | no carrier case         |        |       |

113
Cisco IOx helps bring application execution capability at the network edge, close to the asset. This feature exercises the compute capabilities within the gateway to help enable a distributed compute architecture. Deploying IOx applications close to the source of the IoT data helps overcome challenges with high volumes of data and the need for automated, near-real-time system responsiveness.

Fog applications offer customers and ecosystem partners the ability to transform IoT sensor data and perform control functions within the distributed network infrastructure. With the support of IOx resident on routers, switches, and compute modules, the distributed IoT network functions as the compute environment for fog applications. With the secure connectivity services and common application framework offered by IOx and fog applications, customers can deliver business outcomes rapidly for their IoT initiatives.

Cisco IOx brings together Cisco IOS software, the industry-leading networking operating system, and Linux, the leading open-source platform. With Cisco IOx, your developers benefit from familiar processes and open-source tools prevalent with Linux while generating applications that execute on Cisco IoT network infrastructure.

Fog applications ready for execution on IOx-enabled infrastructure may be supplied by ecosystem partners and/or Cisco or developed with a range of common programming languages.

Examples of IOx/Fog applications across industry include:

- Manufacturing companies connect machines, transform sensor data, and perform real-time analytics to predict when maintenance is necessary and increase overall equipment effectiveness (OEE). Securely Connect Immediately Transform Deliver Insight MT Connect IOS Application Framework Linux IOx.

- Mobile network operators manage their cell tower assets remotely. With real-time insight from fog applications, they make sure of proper operation, prevent theft, and save money.

- Utilities drive up grid reliability using fog applications to transform SCADA data into real-time insight and control.

In most scenarios deploying IOx / Fog applications can also help with reducing WAN costs. Applications can be deployed to normalize the data at the edge, only transmitting changed data northbound and discarding similar data thus helping reduce wan bandwidth utilization and costs.

Running IOx applications closest to the source of IoT data in the fog or at the edge can help accelerate IoT business outcomes as we can more rapidly gain insights, make decisions, and take meaningful action.

IOx applications can also help with making near-real-time at the edge of the IoT network closest to the source of the IoT data thus helping reduce round-trip latency for certain control traffic and decisions which might be critical for certain time-sensitive use-cases.
Cisco IOx allows IoT application developers to work in the familiar Linux application environment with their choice of languages, programming models, and open-source development tools.

With Cisco IOx distributed applications, we can easily process high volumes of data in the fog and deliver closed-loop system control in real time. Cisco IOx offers consistent management and hosting across network infrastructure products, including Cisco routers, switches, and compute modules.

With an intuitive GUI for on-premises or cloud-based management, IOx lets you backup and restore application data. You can also perform upgrades and view troubleshooting logs. Cisco Kinetic GMM is the cloud-based management application that can be used to deploy IOx applications to each of your distributed edge gateways.

Built-in container security allows you to run only trusted applications with application signing and verification.

- For sample IOx applications, please refer to https://github.com/CiscoIOx
- For additional information on Cisco IOx, please refer to https://developer.cisco.com/site/iox/

### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>AR</td>
<td>Active Router</td>
</tr>
<tr>
<td>CAPWAP</td>
<td>Control and Provisioning of Wireless Access Points</td>
</tr>
<tr>
<td>CLB</td>
<td>Cluster Load Balancing</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>DMVPN</td>
<td>Dynamic Multipoint VPN</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPoL</td>
<td>EAP over LAN</td>
</tr>
<tr>
<td>EEM</td>
<td>Embedded Event Manager</td>
</tr>
<tr>
<td>GMM</td>
<td>Cisco Gateway Management Module</td>
</tr>
<tr>
<td>GPT</td>
<td>Cisco Kinetic Gateway Provisioning Tool</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HER</td>
<td>Headend Router</td>
</tr>
<tr>
<td>HSPA</td>
<td>High Speed Packet Access</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IR</td>
<td>Industrial Router</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISE</td>
<td>Cisco Identity Services Engine</td>
</tr>
<tr>
<td>LAP</td>
<td>Lightweight Access Point</td>
</tr>
<tr>
<td>LLG</td>
<td>Least Loaded Gateway</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>LWAP</td>
<td>Lightweight Access Point</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple-Input and Multiple-Output</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MQC</td>
<td>Modular QoS</td>
</tr>
<tr>
<td>mSATA</td>
<td>mini-Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NGE</td>
<td>Cisco Next-Generation Encryption</td>
</tr>
<tr>
<td>NHRP</td>
<td>Next Hop Resolution Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Keys</td>
</tr>
<tr>
<td>RaMA</td>
<td>Cisco Remote and Mobile Assets</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-Factor Pluggable</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identification Module</td>
</tr>
<tr>
<td>SVI</td>
<td>Switched Virtual Interface</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP address</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Route Forwarding</td>
</tr>
<tr>
<td>VTI</td>
<td>Virtual Tunnel Interface</td>
</tr>
<tr>
<td>vWLC</td>
<td>virtual Wireless LAN Controller</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WGB</td>
<td>Workgroup Bridge</td>
</tr>
<tr>
<td>WLC</td>
<td>Cisco Wireless LAN Controller</td>
</tr>
<tr>
<td>ZTD</td>
<td>Zero-Touch Deployment</td>
</tr>
</tbody>
</table>