## Contents

Remote and Mobile Assets—Technology Guidance ........................................... 1
  Overview ........................................................................................................ 2
  Requirements .................................................................................................. 2
  Design Considerations ..................................................................................... 4
    Selecting the Router ...................................................................................... 4
    Designing Your Solution .............................................................................. 6
    Target Customers and Markets ..................................................................... 6
  Cisco Industrial Router Portfolio .................................................................... 9
    Cisco IR807 Ruggedized Gateway ................................................................. 9
    Cisco IR809 Ruggedized Gateway ................................................................. 10
    Cisco IR829 Ruggedized Gateway ................................................................. 11
    Cisco IR1101 Ruggedized Gateway ............................................................... 12
  Select Hardware Features .............................................................................. 14
  Ordering Information ...................................................................................... 16
  Kinetic GMM Gateway Compatibility ............................................................. 17

Common Issues and Troubleshooting ............................................................... 18
  Common Gateway Issues .............................................................................. 19
  GPS Troubleshooting ..................................................................................... 19
  Login Troubleshooting .................................................................................. 19
  Private Subnet Troubleshooting .................................................................... 19
  Customer VPN Troubleshooting ................................................................... 20
  WGB Troubleshooting ................................................................................... 20
  Wi-Fi Troubleshooting .................................................................................. 20

Appendix A—Firewall Ports for Kinetic GMM to Gateway Communication .... 21
Appendix B—Hardware and Software Matrix .................................................. 25
Glossary ............................................................................................................ 26

Remote and Mobile Assets—Security ............................................................... 29
  Overview ........................................................................................................ 30
  Requirements .................................................................................................. 30
    Management Plane Security ......................................................................... 31
    Data Plane Security ...................................................................................... 31
    Gateway and Device Security ...................................................................... 32
  Architecture .................................................................................................. 32
  Design ............................................................................................................ 32
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing the Cisco Kinetic GMM Management Plane</td>
<td>32</td>
</tr>
<tr>
<td>- Encrypted IPSec Tunnel</td>
<td>33</td>
</tr>
<tr>
<td>- Certificate-based Authentication</td>
<td>33</td>
</tr>
<tr>
<td>- GMM Web UI Two-Factor Authentication</td>
<td>33</td>
</tr>
<tr>
<td>- Role-Based Access Control (RBAC)</td>
<td>33</td>
</tr>
<tr>
<td>- Logging and Auditing</td>
<td>33</td>
</tr>
<tr>
<td>Securing the Data Plane</td>
<td>33</td>
</tr>
<tr>
<td>- Introduction to IPSec VPNs</td>
<td>33</td>
</tr>
<tr>
<td>- Introduction to FlexVPN</td>
<td>34</td>
</tr>
<tr>
<td>- Benefits of Using FlexVPN</td>
<td>34</td>
</tr>
<tr>
<td>- Private versus Public Access Point Names</td>
<td>35</td>
</tr>
<tr>
<td>- PCI Compliance</td>
<td>35</td>
</tr>
<tr>
<td>- Gateway Remote Access (Remote VPN) Security</td>
<td>36</td>
</tr>
<tr>
<td>IoT Gateway and Device Security</td>
<td>36</td>
</tr>
<tr>
<td>- IEEE 802.1X Authentication for Wireless Clients</td>
<td>36</td>
</tr>
<tr>
<td>- Hardware Encryption</td>
<td>37</td>
</tr>
<tr>
<td>- ACT2—Hardware Root of Trust</td>
<td>37</td>
</tr>
<tr>
<td>- Image Signing and Secure Boot</td>
<td>38</td>
</tr>
<tr>
<td>Best Practices</td>
<td>38</td>
</tr>
<tr>
<td>Sample Security Configurations</td>
<td>39</td>
</tr>
<tr>
<td>Firewall</td>
<td>39</td>
</tr>
<tr>
<td>Glossary</td>
<td>39</td>
</tr>
<tr>
<td>Remote and Mobile Assets—Zero Touch Provisioning</td>
<td>43</td>
</tr>
<tr>
<td>Overview</td>
<td>44</td>
</tr>
<tr>
<td>Requirements</td>
<td>45</td>
</tr>
<tr>
<td>Architecture</td>
<td>46</td>
</tr>
<tr>
<td>Design Considerations</td>
<td>47</td>
</tr>
<tr>
<td>Gateway Provisioning</td>
<td>47</td>
</tr>
<tr>
<td>- Claiming your Gateways</td>
<td>47</td>
</tr>
<tr>
<td>- Authentication during the Gateway Registration and Claim Process</td>
<td>48</td>
</tr>
<tr>
<td>- Initial Registration and Claim Process</td>
<td>49</td>
</tr>
<tr>
<td>- Grouping your Gateways</td>
<td>49</td>
</tr>
<tr>
<td>- Gateway States and Configuration</td>
<td>49</td>
</tr>
<tr>
<td>- Template-based Configuration</td>
<td>50</td>
</tr>
<tr>
<td>- Advanced Templates for IOS Features</td>
<td>50</td>
</tr>
<tr>
<td>Management</td>
<td>52</td>
</tr>
<tr>
<td>- Remote Management using VPN</td>
<td>52</td>
</tr>
<tr>
<td>- Upgrading the Gateway Firmware</td>
<td>52</td>
</tr>
<tr>
<td>- Using Kinetic GMM APIs</td>
<td>52</td>
</tr>
<tr>
<td>- Firewall Ports for Kinetic GMM to Gateway Communication</td>
<td>52</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Package Format</td>
<td>139</td>
</tr>
<tr>
<td>Package Descriptor File</td>
<td>139</td>
</tr>
<tr>
<td>Package Configuration File</td>
<td>140</td>
</tr>
<tr>
<td>Application Artifacts</td>
<td>140</td>
</tr>
<tr>
<td>Implementation</td>
<td>140</td>
</tr>
<tr>
<td>Building a Dockerized IOx NodeJS Application and Deploying it Using Kinetic GMM</td>
<td>140</td>
</tr>
<tr>
<td>Installing Docker Tools and Images</td>
<td>140</td>
</tr>
<tr>
<td>Creating the Docker Image</td>
<td>141</td>
</tr>
<tr>
<td>Writing Package Descriptor File</td>
<td>142</td>
</tr>
<tr>
<td>Creating an IOx Application Package</td>
<td>143</td>
</tr>
<tr>
<td>Deploying the IOx Application to the Gateway using Cisco Kinetic GMM</td>
<td>144</td>
</tr>
<tr>
<td>Glossary</td>
<td>155</td>
</tr>
<tr>
<td>Remote and Mobile Assets—Field Deployment</td>
<td>159</td>
</tr>
<tr>
<td>Overview</td>
<td>160</td>
</tr>
<tr>
<td>Requirements</td>
<td>160</td>
</tr>
<tr>
<td>Architecture</td>
<td>161</td>
</tr>
<tr>
<td>Design</td>
<td>161</td>
</tr>
<tr>
<td>Deploying Gateways in the Field</td>
<td>161</td>
</tr>
<tr>
<td>Using the Kinetic GMM Mobile App to Claim the Gateway</td>
<td>162</td>
</tr>
<tr>
<td>Using the Kinetic GMM Web App to Claim the Gateway</td>
<td>165</td>
</tr>
<tr>
<td>Provisioning a Gateway with a Private APN</td>
<td>169</td>
</tr>
<tr>
<td>Offboarding/Removing a Gateway</td>
<td>169</td>
</tr>
<tr>
<td>Field Monitoring and Troubleshooting</td>
<td>170</td>
</tr>
<tr>
<td>Monitoring the Gateway</td>
<td>171</td>
</tr>
<tr>
<td>Gateway Logs</td>
<td>175</td>
</tr>
<tr>
<td>Best Practices</td>
<td>175</td>
</tr>
<tr>
<td>Troubleshooting the Gateway</td>
<td>175</td>
</tr>
<tr>
<td>Common Gateway Issues</td>
<td>175</td>
</tr>
<tr>
<td>Gateway Diagnostics</td>
<td>178</td>
</tr>
<tr>
<td>Installation Best Practices</td>
<td>178</td>
</tr>
<tr>
<td>General Considerations</td>
<td>178</td>
</tr>
<tr>
<td>Specific Considerations</td>
<td>180</td>
</tr>
<tr>
<td>Glossary</td>
<td>183</td>
</tr>
</tbody>
</table>
Remote and Mobile Assets—Technology Guidance

This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: [www.cisco.com/go/rama](http://www.cisco.com/go/rama)

- **Solution Brief**—An overview of the RaMA CVD and the available modules.
- **Design and Implementation Guide (DIG)**—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- **Security Module**—Describes how the RaMA solution was designed from the ground up with security in mind. Includes detailed descriptions of how the solution fits into the SAFE model, including securing the gateways, data plane, and management plane. Also includes a section on achieving PCI compliance.
- **Enterprise Network Integration Module**—Best practices for the enterprise headend focusing on resiliency, high-availability, load-balancing, and security. Includes detailed descriptions of FlexVPN and WAN redundancy mechanisms.
- **Remote Site Management Module**—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR 829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- **Fleet Management Module**—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- **Zero Touch Provisioning Module**—Use of Kinetic GMM by IT personnel for provisioning and managing Cisco Industrial Routers with a focus on secure, scalable deployment.
- **Field Deployment Module**—Use of Kinetic GMM by OT personnel for deploying Cisco Industrial Routers in the field, with minimal knowledge of the underlying networking technology required.
- **Edge Compute Module**—Overview of the edge compute capabilities in Cisco Industrial Routers in the form of IOx. Includes implementation examples for deploying Dockerized applications.
Overview

This module includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview, page 2</td>
<td>A brief summary of the Technology Guidance module.</td>
</tr>
<tr>
<td>Requirements, page 2</td>
<td>List of requirements to consider when deciding on which industrial router is most appropriate for a specific use case.</td>
</tr>
<tr>
<td>Architecture, page 3</td>
<td>A brief overview of the RaMA architecture focusing on where the industrial router portfolio fits into the solution.</td>
</tr>
<tr>
<td>Design Considerations, page 4</td>
<td>This section takes a close look at the hardware and software capabilities of the IR807, IR809, IR829, and IR1101 industrial routers as used in the RaMA solution. Recommendations are included for choosing the best platform for some common use cases.</td>
</tr>
<tr>
<td>Common Issues and Troubleshooting, page 18</td>
<td>How to diagnose and resolve common issues seen with WiFi, LTE, GPS, VPN, and more.</td>
</tr>
<tr>
<td>Appendix A—Firewall Ports for Kinetic GMM to Gateway Communication, page 21</td>
<td>Reference table for security design.</td>
</tr>
<tr>
<td>Appendix B—Hardware and Software Matrix, page 25</td>
<td>Reference table of validated hardware and software combinations. This applies to all other modules of the RaMA documentation.</td>
</tr>
<tr>
<td>Glossary, page 26</td>
<td>List of relevant acronyms and initialisms.</td>
</tr>
</tbody>
</table>

Overview

This module provides an in depth look at Cisco’s industrial routing portfolio which is central to the RaMA solution. This module can be used to help guide the design and implementation of the RaMA solution. Feature comparisons between the available models (for mobile and fixed applications) are presented, as well as recommendations for hardware use in several common use cases. Some industry-agnostic troubleshooting tips are provided, along with issues to look out for when designing and deploying the industrial routers in the RaMA solution. Finally, a hardware software matrix outlines all of the versions validated as part of the solution Cisco Validated Design.

Requirements

- Portfolio of secure industrial gateways
- Secure cloud-hosted gateway deployment and management
- Zero-Touch Deployment (ZTD) and Zero-Touch Provisioning (ZTP)
- WAN connectivity options (Ethernet, LTE, Dual-LTE, WGB)
- WiFi hotspot
- GPS and geo-Fencing
- Enterprise network integration
- Security
- Lower deployment and operating expenses
Remote and Mobile Assets—Technology Guidance

Requirements

Figure 1  Cisco Remote and Mobile Assets—Solution Architecture—Component View

Figure 1 highlights the four primary components of the Cisco RaMA solution, the 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 IOx provides the edge compute capability on supported IR gateways (IR809, IR829, IR1101). The ability to run microservices (from Cisco or third parties) enables data collection, processing, and forwarding at the edge of the network.

- Cisco Kinetic GMM is a cloud-hosted provisioning and management platform that enables ZTD and management of the edge routers. Kinetic 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, Kinetic GMM helps provision a FlexVPN tunnel from each of the edge gateways to the enterprise headend VPN router.

- Cisco Control Center works with cellular providers to enable customers to manage the SIM cards and associated data plans for IoT devices. Integration with Kinetic GMM streamlines the management of cellular-connected Cisco gateways.
Design Considerations

Getting started with the Cisco RaMA solution requires two steps:

- Selecting the industrial router model
- Designing the solution

Selecting the Router

Figure 2  Cisco IoT Gateway Portfolio

What’s Included

Leading IoT gateway portfolio for industrial use cases
- #1 in Industrial networking
- Wide range, purpose built for industrial use cases
- Modular options for future expansion

Internet-ready security as the foundation
- Full set of secure gateway features
- Protection using built-in sensors & 802.1x
- Native application security options

* Available options
Remote and Mobile Assets–Technology Guidance

Design Considerations

Cisco offers a wide range of industrial routers to meet a range of requirements and budgets. Table 1 lists some of the prominent features supported by each of the routers.

**Table 1** Industrial Router Options

<table>
<thead>
<tr>
<th>Router</th>
<th>IR807(^1)</th>
<th>IR809(^2)</th>
<th>IR829(^3)</th>
<th>IR1101(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td>Optimized for low power:</td>
<td>Compact, feature rich:</td>
<td>Single/Dual LTE with Wi-Fi, optional PoE and mSATA:</td>
<td>Highly modular design:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ports and Backhaul</strong></td>
<td>Two Fast Ethernet</td>
<td>Two RJ45 routed ports (10/100/1000 Mbps)</td>
<td>Four RJ45 with switch ports (10/100/1000 Mbps)</td>
<td>Four Fast Ethernet</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>
<td>Single and Dual LTE (Dual SIM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WAN SFP port</td>
</tr>
<tr>
<td><strong>Wi-Fi and WGB</strong></td>
<td>None</td>
<td>None</td>
<td>802.11</td>
<td>None</td>
</tr>
<tr>
<td><strong>Embedded Sensors</strong></td>
<td>GPS</td>
<td>GPS</td>
<td>GPS, Gyroscope, Accelerometer</td>
<td>GPS</td>
</tr>
<tr>
<td><strong>Edge Compute</strong></td>
<td>None</td>
<td>732 CPU units for edge compute</td>
<td>732 CPU units for edge compute</td>
<td>1000 CPU units for edge compute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>767MB memory</td>
<td>767MB memory</td>
<td>862MB memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512MB storage</td>
<td>512MB storage</td>
<td>512MB storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Additional 50GB or 100GB mSATA storage on IR829M models</td>
<td>Can add storage module with ability for mSATA SSD</td>
</tr>
</tbody>
</table>
Design Considerations

Table 1 Industrial Router Options (continued)

<table>
<thead>
<tr>
<th>Router</th>
<th>IR807(^1)</th>
<th>IR809(^2)</th>
<th>IR829(^3)</th>
<th>IR1101(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Consumption</td>
<td>■ 6.7w typical</td>
<td>■ 15w typical</td>
<td>■ 40w typical</td>
<td>■ 10w typical</td>
</tr>
<tr>
<td></td>
<td>■ 10w max</td>
<td>■ 19w max</td>
<td>■ 70w max with PoE option</td>
<td>■ 12w max</td>
</tr>
<tr>
<td>Other Features</td>
<td>IP30, Fanless</td>
<td>IP30, Fanless</td>
<td>IP40 (IP54 enclosure available), Fanless</td>
<td>IP30, Fanless</td>
</tr>
<tr>
<td>Dimensions (inches) 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>
<td>2.36 x 5.22 x 4.92 in North America and Europe</td>
</tr>
</tbody>
</table>


Designing Your Solution

Target Customers and Markets

Target customers for the Cisco RaMA solution have similar application requirements for connecting their assets, as shown in Table 2.

Table 2 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 3.

<table>
<thead>
<tr>
<th>Segment Category</th>
<th>Description</th>
<th>Sample Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected Machines</td>
<td>Enterprises with industrial equipment at distributed customer and indoor locations. Includes:</td>
<td>Real-time telemetry of machines at customer locations</td>
</tr>
<tr>
<td></td>
<td>▪ Conveyor belts, escalators, etc.</td>
<td>Preventative maintenance/control without a truck roll</td>
</tr>
<tr>
<td></td>
<td>▪ Indoor equipment</td>
<td>Flexible routing options based on available connectivity</td>
</tr>
<tr>
<td>Outdoor Equipment</td>
<td>Enterprises and public sector entities with industrial equipment in the field or at outdoor locations, including:</td>
<td>Ingress Protection (IP)-rated equipment to meet stringent temperature, dust, and operating specifications</td>
</tr>
<tr>
<td></td>
<td>▪ Oil and gas companies</td>
<td>Edge compute options for legacy protocols</td>
</tr>
<tr>
<td></td>
<td>▪ Roadways and traffic management</td>
<td>SCADA-ready</td>
</tr>
<tr>
<td>Remote Sites</td>
<td>Connectivity for remote and distributed sites, including:</td>
<td>Remote setup and operations by field workers</td>
</tr>
<tr>
<td></td>
<td>▪ Retail and distribution centers</td>
<td>Reliable data access and options for additional network services</td>
</tr>
<tr>
<td></td>
<td>▪ Kiosks</td>
<td>Simplified cloud management</td>
</tr>
<tr>
<td>Mobile Assets</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, including:</td>
<td>Extend enterprise network to vehicles</td>
</tr>
<tr>
<td></td>
<td>▪ Utilities</td>
<td>Enterprise application integration using edge compute</td>
</tr>
<tr>
<td></td>
<td>▪ Telco and cable</td>
<td>Enterprise VPN termination and unified Wi-Fi policies</td>
</tr>
<tr>
<td>Buses and Taxis</td>
<td>Enterprises that use vehicles as their primary means of service delivery, including:</td>
<td>Growing range of in-vehicle services (such as ticketing, Wi-Fi, video entertainment, and video cameras)</td>
</tr>
<tr>
<td></td>
<td>▪ Bus companies</td>
<td>Vehicle telemetry, performance tracking, and driver safety</td>
</tr>
<tr>
<td></td>
<td>▪ Taxi companies</td>
<td>Deploy and manage at scale with limited IT staff</td>
</tr>
<tr>
<td>Public Safety Vehicles</td>
<td>Cities and municipalities that use fleets of specialized vehicles for citizen and municipal services, including:</td>
<td>Lives depend on an always-on connectivity</td>
</tr>
<tr>
<td></td>
<td>▪ Police vehicles</td>
<td>Frequent increase in vehicle devices (such as computers, dash cams, and sensors)</td>
</tr>
<tr>
<td></td>
<td>▪ Ambulances</td>
<td>Multiple connectivity options (such as Single-LTE/Dual-LTE and Wi-Fi)</td>
</tr>
</tbody>
</table>
Because of the flexibility of the Industrial Routers and the Kinetic GMM software, the Cisco RaMA CVD describes a number of available options. Table 4 and Table 5 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 to use their edge gateways as a full extension of the enterprise.

All gateway configuration options shown throughout are implemented using Cisco Kinetic GMM config templates. Table 4 and Table 5 are examples that demonstrate the range of design options available through Kinetic 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 Kinetic GMM and manual configuration is not recommended. For use cases that require advanced IOS configuration not exposed via Base Kinetic GMM config templates, we recommend using the Advanced Templates feature within Kinetic GMM.

### Table 4  Remote Assets Use Cases

<table>
<thead>
<tr>
<th></th>
<th>Basic Connectivity</th>
<th>Advanced Connectivity, including Edge Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>IR807</td>
<td>IR1101</td>
</tr>
<tr>
<td>Wan backhaul</td>
<td>Single cellular</td>
<td>Single cellular standard</td>
</tr>
<tr>
<td></td>
<td>Single SIM</td>
<td>Optional dual cellular (with expansion module)</td>
</tr>
<tr>
<td></td>
<td>Wired Fast Ethernet</td>
<td>Dual SIM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5G ready</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wired Gigabit Ethernet</td>
</tr>
<tr>
<td>Edge device connectivity</td>
<td>Wired Fast Ethernet</td>
<td>Wired Fast Ethernet</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>
<tr>
<td>Lan addressing</td>
<td>Kinetic GMM assigned addressing and NAT</td>
<td>Custom subnet, routed mode, and VRF</td>
</tr>
<tr>
<td>Edge device authentication</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Compute onboard router</td>
<td></td>
<td>IOX</td>
</tr>
</tbody>
</table>
A collection of scripts and Advanced Templates has been posted to GitHub. This collection includes Python scripts that can be used to create these recommended templates for various use cases in Kinetic GMM. This regularly updated repository contains many of the examples shown throughout this CVD and more:
https://github.com/CiscoDevNet/iot-gateway-management

Cisco Industrial Router Portfolio

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

Cisco IR807 Ruggedized Gateway

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

Figure 3  Cisco IR807 Ruggedized Gateway

- 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, which makes it an excellent solution for use cases where a full featured router with edge compute is required and space is a constrained.
Remote and Mobile Assets—Technology Guidance

Design Considerations

Figure 4  Cisco IR809 Ruggedized Gateway

- 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.
Remote and Mobile Assets—Technology Guidance

Design Considerations

Figure 5  Cisco IR829 Ruggedized Gateway

- Cisco IR829 Datasheet:  

- Cisco IR829 Hardware Installation Guide:  

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.

- Built-in GPS systems to track vehicle fleets.

- 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.

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

Cisco IR1101 Ruggedized Gateway

The Cisco IR1101 Integrated Services Router Rugged (IR1101) is Cisco’s smallest modular industrial router. Designed in a highly modular form factor, it is an ideal solution for remote asset management across multiple industrial vertical markets.
Remote and Mobile Assets—Technology Guidance

Design Considerations

**Figure 6  Cisco IR1101 Ruggedized Gateway**

**Figure 7  Cisco IR1101 Expansion Module**

- Cisco IR1101 Datasheet:  

- Cisco IR1101 Hardware Installation Guide:  
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:

- Antenna should offer 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).

- We recommend the use of multi-element antennas (5-in-1, 3-in-1, 2-in-1) to avoid streams interfering with each other. If, instead, MIMO antennas that have a strong correlation coefficient were installed, the system may have trouble separating them (leading to interference).

- On the IR829, ensure physical spacing between antennas to allow 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.


SIM-based Auto-Carrier Selection (AutoSIM)

The router automatically detects the active SIM and configures its modem for the appropriate cellular carrier when an active SIM is inserted and powered up, which 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
Gyroscope/Accelerometer

The IR829 includes a built-in gyroscope and accelerometer that can detect linear acceleration and angular movement. This functionality could be used to detect equipment tampering or assist in automotive applications where movement is involved. Devices connected to 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. However, the configuration can be changed to take a reading once every six or 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 four GB of disk storage available in other IR829 models and is only visible and usable in IOx. 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: https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_IR800config_chapter_01011.pdf

Ignition Power Management

The Ignition Power Management feature helps keep the IR829 gateway up and running while the vehicle is stopped without draining the vehicle battery. Additional benefits of the Ignition Power Management system include:

- 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 users 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.
Remote and Mobile Assets—Technology Guidance

Design Considerations

- 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 9  Ignition Power Management Features**

- Zero boot up time (no cold start) because the platform stays powered up when the vehicle engine is turned off.
  - When ignition is turned off, the IR829 can remain operational for a pre-determined period of time. The pre-determined period is programmable between 60 to 7200 seconds (2H00) using IOS ignition off-timer command.

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

**Figure 10  Ignition Power Management**

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

To enable Cisco Kinetic GMM on Cisco gateways, order the following option 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 routers:

- IR807
- IR809
- IR829
- IR1101

Once the base router 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 in the next section.

Kinetic GMM Gateway Compatibility

Kinetic GMM supports the management of Cisco IR 8x9 series gateways, which currently includes the IR807, IR809, IR829, and IR1101 models as shown in Table 6, Table 7, and Table 8.

**Table 6 IR807 and IR809 Hardware SKUs**

<table>
<thead>
<tr>
<th>Region</th>
<th>IR807</th>
<th>IR809</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (US AT&amp;T, Canada)</td>
<td>IR807G-LTE-NA-K9</td>
<td>IR809G-LTE-NA-K9</td>
</tr>
<tr>
<td>US-Verizon</td>
<td>IR807G-LTE-VZ-K9</td>
<td>Refer to IR1101 versions (Table 8) or an acceptable IR807 version for Verizon.</td>
</tr>
<tr>
<td>Europe</td>
<td>IR807G-LTE-GA-K9</td>
<td>Refer to IR1101 versions (Table 8) or an acceptable IR807 version for Europe.</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 7 contains the available SKUs when this document was published.

**Table 7 IR829 Hardware SKUs**

<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>US-Verizon</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>IR829M-LTE-EA-BK9</td>
</tr>
</tbody>
</table>
Kinetic GMM Subscription Details

Kinetic GMM is available as part of the Cisco Kinetic platform subscription. Cloud-hosted Kinetic 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 to stay up-to-date with the latest version of the software. You can choose to prepay the subscription price for the entire term or on an annualized basis.

Kinetic GMM Services and Support

Your Kinetic 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. In addition, support includes the 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 Issues and Troubleshooting

For additional detailed troubleshooting procedures, refer to:
https://developer.cisco.com/docs/kinetic/#!gateway-diagnostics
Common Issues and Troubleshooting

Common Gateway Issues

**Stuck in Registering for more than 10 minutes.**
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 Ethernet-based gateways are used, 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 minutes:**
- 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 on 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 indicating the configuration that was applied to the gateway. Ensure that the proper configuration was applied.
- Ensure that the correct GPS antennas are attached to the gateway.
- Delete and reclaim the gateway with the correct configuration if required.

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 on the **Gateway Details -> Current Config** page.
Remote and Mobile Assets—Technology Guidance

Common Issues and Troubleshooting

- 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 indicating the configuration that was applied to the gateway. Ensure that the proper configuration was applied.
- 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 on 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 indicating the configuration that was applied to the gateway. Ensure that the proper configuration was applied.
- Verify that the details entered for the VPN configuration are correct.
- Verify that the configuration on your HER is correct and that it allows the gateways to establish tunnels with the provided configuration.
- Delete and reclaim the gateway with the correct configuration if required.

Note: A known issue exists where site-to-site VPN tunnels and the site-to-site VPN tunnel IP Address on the Gateway Details page can take up to 30 minutes 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 on 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. Note:
- Confirm that the details entered for the WGB configuration are correct.
- 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.
- Delete and reclaim the gateway with the correct configuration if required.

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

Note: For additional WGB troubleshooting information, see the Fleet Management module.

Wi-Fi Troubleshooting

If you are not able to connect any devices to the Wi-Fi hotspot configured on the gateway:
Remote and Mobile Assets—Technology Guidance

Appendix A—Firewall Ports for Kinetic GMM to Gateway Communication

- 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 on 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 indicating the configuration that was applied to the gateway. Ensure that the proper configuration was applied. 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

Appendix A—Firewall Ports for Kinetic 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. For the recommended settings, refer to the Zero Touch Provisioning module.

**Table 9** 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>450</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>
</tbody>
</table>
Table 9  TCP/UDP Ports (continued)

<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>888</td>
<td>TCP</td>
<td>US cluster: Name resolution of us.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>
<tr>
<td>3</td>
<td></td>
<td>EU cluster: Name resolution of eu.ciscokinetic.io</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The DNS name us.ciscokinetic.io resolves to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.71.117.77</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>34.216.139.206</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.11.218.197</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EU cluster: Name resolution of eu.ciscokinetic.io</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The DNS name eu.ciscokinetic.io resolves to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.212.193.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.194.175.23</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>34.252.252.200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 9  TCP/UDP Ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Description</th>
<th>Required for Kinetic Module</th>
</tr>
</thead>
</table>
| 443  | TCP      | US cluster: Name resolution of mqtt-us.ciscokinetic.io  

- EU cluster: Name resolution of mqtt-eu.ciscokinetic.io  

- The DNS name us.ciscokinetic.io resolves to:
  - 54.71.117.77  
  - 34.216.139.206  
  - 52.11.218.197

- The DNS name eu.ciscokinetic.io resolves to:
  - 52.212.193.126  
  - 54.194.175.23  
  - 34.252.252.200

- 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. |

| 912  | TCP      | US cluster: Name resolution of us.ciscokinetic.io  

- EU cluster: Name resolution of eu.ciscokinetic.io  

- The DNS name us.ciscokinetic.io resolves to:
  - 54.71.117.77  
  - 34.216.139.206  
  - 52.11.218.197

- The DNS name eu.ciscokinetic.io resolves to:
  - 52.212.193.126  
  - 54.194.175.23  
  - 34.252.252.200

- 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. |

GMM
### Table 9  TCP/UDP Ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>912 4</td>
<td>TCP</td>
<td>US cluster: Name resolution of us.ciscokinetic.io EU cluster: Name resolution of eu.ciscokinetic.io</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 10  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 EU cluster: 34.240.190.128</td>
<td>Encapsulating Security Payload (ESP)</td>
<td>GMM and DCM</td>
</tr>
</tbody>
</table>
Table 11 lists the individual component versions that have been validated to work together as part of the CVD test effort.

### Table 11 Validated Component Versions

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN HER</td>
<td>ASR1002-HX</td>
<td>IOS-XE 16.9.2</td>
</tr>
<tr>
<td>Mobile Gateway</td>
<td>Industrial Router 829</td>
<td>IOS Version 15.8(3)M2a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modem Firmware: SWI9X30C_02.20.03.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Embedded AP: 15.3(3)J1</td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>Industrial Router 807</td>
<td>IOS for IR807, IR809: 15.8(3)M2a</td>
</tr>
<tr>
<td></td>
<td>Industrial Router 809</td>
<td>IOS-XE for IR1101: 16.11.1</td>
</tr>
<tr>
<td></td>
<td>Industrial Router 1101</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>
<tr>
<td>Cisco Identity Services Engine (ISE)</td>
<td>Virtual machine</td>
<td>2.4.0.357</td>
</tr>
<tr>
<td>Microsoft Active Directory (AD)</td>
<td>Virtual machine</td>
<td>Windows Server 2016 version 1607</td>
</tr>
<tr>
<td>Cisco Prime Network Registrar (CPNR)</td>
<td>Virtual machine</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
<td></td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td></td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>Active Router</td>
<td></td>
</tr>
<tr>
<td>CAPWAP</td>
<td>Control and Provisioning of Wireless Access Points</td>
<td></td>
</tr>
<tr>
<td>CLB</td>
<td>Cluster Load Balancing</td>
<td></td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
<td></td>
</tr>
<tr>
<td>DMVPN</td>
<td>Dynamic Multipoint VPN</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
<td></td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
<td></td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection</td>
<td></td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
<td></td>
</tr>
<tr>
<td>EAPoL</td>
<td>EAP over LAN</td>
<td></td>
</tr>
<tr>
<td>EEM</td>
<td>Embedded Event Manager</td>
<td></td>
</tr>
<tr>
<td>GMM</td>
<td>Cisco Kinetic Gateway Management Module</td>
<td></td>
</tr>
<tr>
<td>GPT</td>
<td>Cisco Kinetic Gateway Provisioning Tool</td>
<td></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td></td>
</tr>
<tr>
<td>HER</td>
<td>Headend Router</td>
<td></td>
</tr>
<tr>
<td>HSPA</td>
<td>High Speed Packet Access</td>
<td></td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
<td></td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
<td></td>
</tr>
<tr>
<td>IR</td>
<td>Industrial Router</td>
<td></td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
<td></td>
</tr>
<tr>
<td>ISE</td>
<td>Cisco Identity Services Engine</td>
<td></td>
</tr>
<tr>
<td>LAP</td>
<td>Lightweight Access Point</td>
<td></td>
</tr>
<tr>
<td>LLG</td>
<td>Least Loaded Gateway</td>
<td></td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
<td></td>
</tr>
<tr>
<td>LWAP</td>
<td>Lightweight Access Point</td>
<td></td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple-Input and Multiple-Output</td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
<td></td>
</tr>
<tr>
<td>MQC</td>
<td>Modular QoS</td>
<td></td>
</tr>
<tr>
<td>mSATA</td>
<td>mini-Serial Advanced Technology Attachment</td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td></td>
</tr>
<tr>
<td>NGE</td>
<td>Cisco Next-Generation Encryption</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>NHRP</td>
<td>Next Hop Resolution Protocol</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
<td></td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Keys</td>
<td></td>
</tr>
<tr>
<td>RaMA</td>
<td>Cisco Remote and Mobile Assets</td>
<td></td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
<td></td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
<td></td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
<td></td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
<td></td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-Factor Pluggable</td>
<td></td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identification Module</td>
<td></td>
</tr>
<tr>
<td>SVI</td>
<td>Switched Virtual Interface</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP address</td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
<td></td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Route Forwarding</td>
<td></td>
</tr>
<tr>
<td>VTI</td>
<td>Virtual Tunnel Interface</td>
<td></td>
</tr>
<tr>
<td>vWLC</td>
<td>virtual Wireless LAN Controller</td>
<td></td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
<td></td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
<td></td>
</tr>
<tr>
<td>WGB</td>
<td>Workgroup Bridge</td>
<td></td>
</tr>
<tr>
<td>WLC</td>
<td>Cisco Wireless LAN Controller</td>
<td></td>
</tr>
<tr>
<td>ZTD</td>
<td>Zero-Touch Deployment</td>
<td></td>
</tr>
</tbody>
</table>
This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: www.cisco.com/go/rama

- Solution Brief—An overview of the RaMA CVD and the available modules.
- Design and Implementation Guide (DIG)—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- Technology Guidance Module—Overview of the available hardware options for IoT gateways in the RaMA solution, with recommendations on hardware platform and software features to use for common scenarios.
- Enterprise Network Integration Module—Best practices for the enterprise headend focusing on resiliency, high-availability, load-balancing, and security. Includes detailed descriptions of FlexVPN and WAN redundancy mechanisms.
- Remote Site Management Module—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- Fleet Management Module—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- Zero Touch Provisioning Module—Use of Kinetic GMM by IT personnel for provisioning and managing Cisco Industrial Routers with a focus on secure, scalable deployment.
- Field Deployment Module—Use of Kinetic GMM by OT personnel for deploying Cisco Industrial Routers in the field, with minimal knowledge of the underlying networking technology required.
- Edge Compute Module—Overview of the edge compute capabilities in Cisco Industrial Routers in the form of IOX. Includes implementation examples for deploying Dockerized applications.

This module includes the following sections:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements, page 30</td>
<td>Typical security requirements elaborated in the Cisco SAFE model and their applicability to securing the management plane, data plane, and gateway/devices.</td>
</tr>
<tr>
<td>Architecture, page 32</td>
<td>Highlights the key aspects of the security architecture.</td>
</tr>
</tbody>
</table>
Overview

The increasing number of sensors, actuators, and devices attached to remote and mobile assets greatly complicates security due to the increased attack surfaces. Protecting the networks and devices is paramount to ensuring the safety and continuity of business. The Cisco RaMA architecture has been developed with this in mind and has been validated in our labs and with the Cisco internal security audit team to help ensure it provides the safest environment for our customers across three attack vectors:

- Management plane security
- Data plane security
- Gateway and hardware security

Requirements

The Cisco RaMA architecture aligns with the Cisco SAFE security model and methods to simplify end-to-end security depending on the audience needs. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures, and designs, SAFE provides guidance that is holistic and understandable.

More information on the Cisco SAFE security reference architecture is available at:
https://www.cisco.com/go/safe

By aligning with the SAFE Places in the Network (PINs) of Threat Defense, Segmentation, Secure Services, and Management, the RaMA architecture provide the ability to segment data and management, encrypt traffic, and provide secure remote access to connected devices.
Remote and Mobile Assets—Security

Requirements

**Figure 1  Key to SAFE**

![Key to SAFE Diagram]

The Key to SAFE organizes the complexity of holistic security into PINs and Secure Domains.

These SAFE requirements optimize protection from potential vulnerabilities by requiring a security-centric IoT design that helps ensure that every element of the platform is secure, starting from the authentication of edge devices. In addition to secure device access, multiple secure connectivity options are required to ensure protection of enterprise data. Each layer of the IoT architecture must be secured to ensure security of both the management plane and the data plane.

**Management Plane Security**

- Use of an encrypted IP Security (IPSec) tunnel to provision and manage the edge gateways
- Certificate-based authentication during the gateway claiming process
- Cisco Kinetic® Gateway Management Module (GMM) Web-UI two-factor authentication
- Role-based access control
- Logging and auditing
- Multi-tenancy for cloud management

**Data Plane Security**

- Secure connectivity from the edge gateways up to the enterprise headend using FlexVPN to establish encrypted tunnels using IPSec and Internet Key Exchange Protocol version 2 (IKEv2).
- Support for Cisco AnyConnect Virtual Private Networks (VPNs) to enable secure remote access to devices behind the gateway using VPN from external networks.
- WPA2-protected Wi-Fi with Pre Shared Keys (PSK) or RADIUS-based authentication.
- No data goes to the management cloud. When a site-to-site VPN is deployed, all user data can be routed through the enterprise. Cisco recommends routing all traffic through the customer VPN headend if secure traffic is important.
- Addresses industry-specific security requirements such as the PCI DSS control objectives of building and maintaining a secure network and systems that protect card holder data and implement strong access control measures.
Remote and Mobile Assets—Security

Gateway and Device Security

- Use of IEEE 802.1x to authenticate wireless or Ethernet clients.
- Gateway functionality to enforce image signing and secure boot.

Architecture

Figure 2 illustrates the key security aspects of the RaMA architecture. Besides providing the required end-to-end solution-level security, the design goes much deeper than compliance with product standards. This provides a secure platform that can evolve over time to integrate with the larger umbrella of Cisco security products and services as they are deployed.

Figure 2  Enterprise Security Architecture

Securing the Cisco Kinetic GMM Management Plane

The cloud-hosted Cisco Kinetic GMM offers the following security elements:

- Encrypted IPSec Tunnel, page 33
- Certificate-based Authentication, page 33
Encrypted IPSec Tunnel

All provisioning and management of the edge gateways occurs 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 using a certificated-based authentication process. This helps prevent spoofing of the gateway and guards 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

User names and passwords are no longer a safe security method for online accounts. Data breaches occur daily and hackers are always inventing new ways to take over accounts. GMM supports two-factor authentication on its Web-UI to provide an extra layer of security. Users first enter their user name and password and are then required to provide a One-Time Password (OTP) that was sent to a different device.

Role-Based Access Control (RBAC)

Cisco Kinetic GMM provides several levels of access to the GMM management interface. Depending on the user’s role (administrator or operator), various features are either available or restricted.

Logging and Auditing

Keeping a record of all actions performed through Cisco Kinetic GMM, as well as events related to gateway status, helps in a post mortem analysis after a security incident. Similarly, alerts can be configured to be sent immediately when a specified operation or event is observed, allowing the proper individuals to respond accordingly.


Securing the Data Plane

Introduction to IPSec VPNs

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 addresses the task of ensuring the confidentiality, integrity, and authentication (CIA) of origin and secure key distribution for VPNs. Using a VPN secures the data plane and isolates it from the management and configuration of the gateway, which provides segmentation between management and data flow. All data that flows through the gateway flows through a customer-managed headend at the company data center or directly to the internet.

Some of the notable strengths of IPSec are its independence from the transport layer (UDP, TCP, or raw IP) and the simple replacement of one or more of its components (such as hash functions and cryptographic algorithms), so it can withstand brute force attacks while keeping current with the evolution of 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 help with interoperability.
- VTI brings a logical interface to IPSec deployments without the need for 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 establish tunnels between spokes in a hub-and-spoke scenario.

### Table 1 VPN Options

<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 Configuration</th>
<th>Per-peer QoS</th>
<th>Full AAA Management</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>CryptoMap</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 RaMA 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 the use of IKEv2, which is a more secure option than the original implementation (IKEv1).**
- **By design, IKEv2 is not backward compatible with IKEv1 since it provides increased security. IKEv2 requires reconfiguration of all IPSec VPNs.**

### 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–It is easy to configure using IKEv2 built-in, smart defaults, so there is no need to define policies, transform sets, etc.**
- **Cost effective–The FlexVPN hub-and-spoke design does not require NHRP (unlike DMVPN), which reduces WAN bandwidth utilization and costs due to reduced control plane traffic.**
- **Support for hardware encryption:**
Remote and Mobile Assets—Security

Design

- IKEv2 stability—It automatically resumes normal operation after a temporary interruption of a connection, such as after a power outage or when 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 consume 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 greater 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—it is 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 than software encryption.**

Private versus 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 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 and subsequently into the enterprise network. In most cases, the data traverses the public internet to get to the network, which always introduces the possibility of 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 traffic. If your RaMA applications or devices leverage application-level encryption or do not need access to the enterprise network for security or management, then Public or Private APN without FlexVPN may be an acceptable solution.**

PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card companies.

The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around card holder data to reduce credit card fraud.
The PCI DSS is organized into six logically related groups called “control objectives”.

### Table 2  PCI DSS Control Objectives

<table>
<thead>
<tr>
<th>PCI Control Objective</th>
<th>RaMA Design Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Build and maintain a secure network and systems.</strong></td>
<td>The RaMA solution is built around securing the entire management plane and fully addresses this control objective through management audit trails as well as secure device configuration.</td>
</tr>
<tr>
<td><strong>2. Protect card holder data.</strong></td>
<td>When using the FlexVPN capability, card holder data in motion is protected and compliant. Cisco recommends that any device or application behind the gateway be secured for data at rest. When using Private APNs, this requirement is not met.</td>
</tr>
<tr>
<td><strong>3. Maintain a vulnerability management program.</strong></td>
<td>Based on customer policies and procedures.</td>
</tr>
<tr>
<td><strong>4. Implement strong access control measures.</strong></td>
<td>Access to the management layer can be secured through two-factor authentication. While this does not address any applications or devices behind the gateway, the gateway itself does implement strong access control measures.</td>
</tr>
<tr>
<td><strong>5. Regularly monitor and test networks.</strong></td>
<td>Based on customer policies and procedures.</td>
</tr>
<tr>
<td><strong>6. Maintain an information security policy.</strong></td>
<td>Based on customer policies and procedures.</td>
</tr>
</tbody>
</table>

### Gateway Remote Access (Remote VPN) Security

To provide greater security, starting from the July 18th release, a one-time username and password with a set expiration time must be requested to use the Remote Access VPN feature. This is an enhancement from previous releases where the VPN credentials were fixed and common to all gateways. For more details, refer to Remote management using VPN: https://developer.cisco.com/docs/kinetic/#!remotely-access-gateways-and-devices/vpn

### IoT Gateway and Device Security

The Cisco RaMA solution allows greater flexibility for end user devices connected to the Cisco Industrial Router (IR). 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 in the same way as in the office increases acceptance and efficiency.

**Best Practices:**

- While the solution is generally edge-device agnostic, Cisco suggests that wireless devices connect using 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 ensure that unauthorized access is prevented and all user authentication can take place on a centralized authentication server like a RADIUS server deployed at the enterprise headquarters.

Cisco ISE or alternatives like FreeRADIUS and Open RADIUS can be used to authenticate 802.1x clients for access to the network. For further information on Cisco ISE, refer to: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

Hardware Encryption

Cisco IRs offer hardware-accelerated encryption to support a full range of security services such as hardware cryptography to significantly increase IPSec VPN performance. This allows the use of Cisco’s Next Generation Encryption (NGE), which evolves traditional encryption technology to meet today’s increasing security needs while improving scalability and efficiency. Figure 3 lists the technologies that are included in NGE.

Figure 3  Hardware Encryption Features on Cisco 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.
Remote and Mobile Assets—Security

Best Practices

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 burned-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 software booting is authenticated by the previous stack to ensure end-to-end integrity.

Figure 4 Industrial IoT Anti-Counterfeit Protection Steps

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 helps 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 reduces overall security.
- Cisco recommends that all data be encrypted using FlexVPN and not split tunneled. This ensures that your data can leverage all corporate security policies and not be a “back door” into your remote or mobile asset. This is a best practice and is not required for all conditions.
Cisco provides the ability to remotely update gateway and modem functions. Cisco highly recommends upgrading to the latest version to address any CVE or PSIRT advisories fixed in that release.

Sample Security Configurations

Firewall

The following custom configuration implements a simple whitelist firewall that is applied to the LAN interface in the inbound direction. This access-list permits specific outbound communication required by the LAN devices. All other types of traffic are blocked. Although not shown here, the gateway is configured with NAT overload, which inherently blocks inbound communication to the LAN unless NAT rules explicitly permit them. As discussed in the Remote Site module¹, the format shown here allows Cisco Kinetic GMM to dynamically substitute in values for the variables (indicated with the double curly braces) during provisioning.

```
ip access-list extended LAN_ACL
   permit tcp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} any eq domain
   permit udp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} any eq ntp
   permit tcp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} any eq www
   permit tcp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} any eq 1883
   permit tcp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} eq www any
   permit udp any eq bootpc any eq bootps
   permit icmp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} host {{ gw.lan_ip }}
   permit tcp {{ gw.lan_subnet }} {{ gw.lan_wildcard }} any eq 443
deny ip any any
!
interface {{ gw.lan_if }}
ip access-group LAN_ACL in
!
```

Refer to IoT Gateway and Device Security, page 36 for additional recommendations regarding the Cisco IOS firewall feature.

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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</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>
Remote and Mobile Assets—Zero Touch Provisioning

This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: www.cisco.com/go/rama

- Solution Brief—An overview of the RaMA CVD and the available modules.
- Design and Implementation Guide (DIG)—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- Technology Guidance Module—Overview of the available hardware options for IoT gateways in the RaMA solution, with recommendations on hardware platform and software features to use for common scenarios.
- Security Module—Describes how the RaMA solution was designed from the ground up with security in mind. Includes detailed descriptions of how the solution fits into the SAFE model, including securing the gateways, data plane, and management plane. Also includes a section on achieving PCI compliance.
- Enterprise Network Integration Module—Best practices for the enterprise headend focusing on resiliency, high-availability, load-balancing, and security. Includes detailed descriptions of FlexVPN and WAN redundancy mechanisms.
- Remote Site Management Module—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- Fleet Management Module—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- Field Deployment Module—Use of Kinetic GMM by OT personnel for deploying Cisco Industrial Routers in the field, with minimal knowledge of the underlying networking technology required.
- Edge Compute Module—Overview of the edge compute capabilities in Cisco Industrial Routers in the form of IOx. Includes implementation examples for deploying Dockerized applications.
Overview

This module includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview, page 44</strong></td>
<td>A brief summary of the RaMA Zero Touch Provisioning module describing the need for a method of deploying Cisco Industrial Routers with minimal human interaction, as well as the general steps of the zero touch deployment process.</td>
</tr>
<tr>
<td><strong>Requirements, page 45</strong></td>
<td>Requirements that should be considered when planning for zero touch provisioning.</td>
</tr>
<tr>
<td><strong>Architecture, page 46</strong></td>
<td>Describes where the zero touch provisioning process fits into the larger RaMA solution, as well as the goals of the architecture.</td>
</tr>
<tr>
<td><strong>Design Considerations, page 47</strong></td>
<td>A deep dive into the most important features of the RaMA solution related to deployment and management of the Industrial Routers using Kinetic GMM.</td>
</tr>
<tr>
<td><strong>Appendix—Sample Kinetic GMM Report, page 68</strong></td>
<td>Illustrates a sample Kinetic GMM report.</td>
</tr>
<tr>
<td><strong>Glossary, page 68</strong></td>
<td>List of relevant acronyms and initialisms.</td>
</tr>
</tbody>
</table>

Overview

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

**Provisioning:**
- Claiming gateways
- Grouping gateways
- Gateway state transitions
- Gateway configuration using templates
- Onboarding gateways using the Cisco Kinetic Gateway Management Module (GMM) mobile app

**Management:**
- Enabling GPS
- Managing access to Kinetic GMM including remote management using VPNs
- Gateway firmware upgrade
- Advanced IOS feature configurations using custom templates
- Gateway monitoring
- Control Center integration
- Using Kinetic GMM APIs

Zero-touch deployment (ZTD) allows gateways to be on-boarded and configured automatically without human intervention, such as deploying a trained technician on-site, thus eliminating most of the manual labor involved in adding gateways to a network.

ZTD allows the gateway to be installed directly into an environment, such as on a factory floor, inside a vending machine, or within a fleet vehicle, and for that physical installation to be the last hands-on involvement. When the gateway is powered-on, it requests an IP address via DHCP from either an enterprise DHCP server for a fixed connection or cellular provider(s) for mobile connections.
Once the gateway has connectivity, it calls home to a centralized configuration and management server that can be hosted either on-premises with an enterprise DC or in the cloud. This solution uses a Cisco Kinetic GMM hosted in the cloud. This central management and provisioning server then establishes a secure connection to the gateway and pushes to the gateway the user-defined configuration.

From this point onwards we can manage the gateway, perform software and firmware upgrades, modify the configuration, and monitor and troubleshoot from a centralized management and provisioning server, thus enabling ZTD and zero-touch provisioning (ZTP).

Requirements

The following are typical customer requirements for ZTD and ZTP:

- Simplified gateway on-boarding and provisioning
- Faster rollout—installation and deployment
- Better quality assurance by reducing human intervention
- Centralized Management and Provisioning Plane
- Security
- Ability to create standardized configuration templates for bulk provisioning
- Centralized monitoring, logging, troubleshooting, and notifications
- Inventory management, grouping, and tagging of resources
- Bulk software and firmware upgrades (on-demand and scheduled)
- Gateway status, resource utilization, and performance metrics
- GPS and geofencing
- Provide ability for remote gateway access
- Graphical user interface and Programmatic Interface (Restful APIs)
- Mobile application for field technicians

If an organization lacks a dedicated IT deployment team, an automatic provisioning solution can reduce the complexities of tracking, configuring, and managing multiple devices across locations and with varying user needs and permissions.

Automatic deployment solutions enable you to get devices up and running through a simplified process with little to no infrastructure to manage, ZTD solutions help you implement new technology, consolidate resources, and optimize rollout from procurement to refresh—all without downtime.

As described below, the Cisco Kinetic GMM satisfies all of the requirements above and a many more.
Remote and Mobile Assets—Zero Touch Provisioning

Architecture

Figure 1  Cisco Remote and Mobile Assets Architecture—Block View

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

Figure 2  Kinetic GMM Capabilities

Networking

- Remote/Local Touch Deployment
- Cellular Monitoring
- Cellular Coverage
- LTE Hotspot
- Wi-Fi Hotspot
- Full Routing of Subnetted Network
- Custom LAN Subnet
- Private IP for Subnetted Devices
- LAN Port Control
- Active/Active LTE
- NBI for LTE
- Custom iOS Configuration
- Primary/Secondary S2S VPN
- Unified AP
- Unique SSID per GW
- 802.1x Auth for WiFi
- 802.11 Management

Management

- Real-time GPS Tracking
- Cellular Monitor and Details
- Remote Debugging
- WiFi Offload with WGB
- Remote Commands
- 30 day GPS History
- Configuration Edits
- Menu Driven Diagnostics
- Report Center
- Alert Center
- Jasper Integration
- Customized User Persona
- Additional HW [R907/R829M/B]
- Org Level Audits
- SMS Support
- Scheduled Firmware Upgrade
- 3D Topography
- Configurable Gateway Recovery
- Customizable Display Columns
- Geo Fencing

Cellular Data Management
- API Integration between Control Center and Kinetic GMM
- View details about cellular plan usage per SIM card and associated gateway
- Modify SIM card status (activate/deactivate) from GMM directly

Cloud Based Management
- Template based gateway configuration
- Full functionality exposed through API
- GPS tracking and geo-fencing
- Advanced logging, alerts, and reports

Device Visibility
- End devices exposed as Assets in GMM
- Remote connectivity to gateway and attached devices
- Connectivity via Ethernet, WiFi, serial
Kinetic GMM drastically reduces 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-based Kinetic GMM.
2. Enter the gateway’s serial number into the Cisco Kinetic GMM dashboard to securely “claim” it.
3. Select a template from your library of configuration 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 connectivity; the rest is handled by Kinetic GMM. Bulk operations can be applied to handle volume provisioning for even greater efficiency. Once on-boarded, the gateway can also be managed using Kinetic GMM.

Benefits of Kinetic GMM include:

- Supports IR807, IR809, IR829, and IR1101.
- Allows customer to bring new gateways online in minutes instead of days with ZTP.
- 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 two geographies (US and EU).

For a high-level overview of Kinetic GMM, refer to:

- https://developer.cisco.com/docs/kinetic/#!gmm-overview/gmm-overview

For an overview of the Kinetic GMM architecture and its components, refer to:


Design Considerations

Gateway Provisioning

Claiming your Gateways

Figure 3 depicts the claiming process of the gateway with Kinetic GMM.
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.

- Kinetic GMM Management Tunnel Certificate which is signed by Comodo certificate authority.

- Self-signed Kinetic 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 Kinetic 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 Kinetic GMM server.

2. Next, the Kinetic GMM server requests the Cisco-signed gateway certificate. Kinetic 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 Kinetic 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 Kinetic GMM and the gateway.

5. Next, the gateway and the Kinetic GMM server perform a basic TLS handshake. The gateway again 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—a self-signed certificate—is not considered a major issue since this exchange happens within the context of the secure IPSec Management tunnel.

Grouping your Gateways

A useful feature of Kinetic GMM is its ability to group gateways based on their purpose such as asset type, location, or any other user-defined category. This allows gateways to be filtered based on their tags. To do this, the gateway should be configured to be managed by Kinetic GMM using GPT before it can be claimed by Kinetic GMM. A support request also needs to be sent to Kinetic GMM using the Cisco Kinetic portal to enable the gateway to be Kinetic GMM managed.

Gateway States and Configuration

A gateway undergoes several state changes as it moves from out-of-box to operational.
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

Figure 4  Kinetic GMM Edge Gateway Lifecycle

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kinetic Startup</td>
<td>Gateway that is received from manufacturing, or a gateway that has been</td>
</tr>
<tr>
<td></td>
<td>factory reset or a standard IR829 gateway that has been converted to a</td>
</tr>
<tr>
<td></td>
<td>Kinetic gateway using GT7 tool.</td>
</tr>
<tr>
<td>1st Claim</td>
<td>First time the gateway is claimed from “Kinetic Startup” state. Gateway</td>
</tr>
<tr>
<td></td>
<td>hard code the WAN (uplink) from configuration template to the boot up</td>
</tr>
<tr>
<td></td>
<td>configuration as the “Kinetic Base” state. Note: WAN configuration on</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>be claimed.</td>
</tr>
<tr>
<td>Claim</td>
<td>Initiate Kinetic configuration process. Claim is executed using “add</td>
</tr>
<tr>
<td></td>
<td>gateway” function on the Kinetic gateway page. Gateway returns to “Kinetic</td>
</tr>
<tr>
<td></td>
<td>Base” configuration and waits to be claimed.</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 “delete</td>
</tr>
<tr>
<td></td>
<td>gateway” function on Cisco Kinetic gateway page. Gateway returns to “Kinetic</td>
</tr>
<tr>
<td></td>
<td>Base” configuration and waits to be claimed.</td>
</tr>
<tr>
<td>Fallback</td>
<td>An operational gateway will fall back to “Kinetic Base” state when it</td>
</tr>
<tr>
<td></td>
<td>misses 4 consecutive heartbeat from Kinetic Gateway will automatically move</td>
</tr>
<tr>
<td></td>
<td>to the “Operational” state 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, refer to:

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 either applying a new template to an existing gateway or modifying the existing template associated with a gateway(s). In order to leverage advanced IOS feature configurations not exposed via Kinetic GMM, we can leverage Kinetic GMM’s Advanced Template Feature.

Advanced 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 IOS functionality not exposed via the Kinetic GMM UI. Kinetic GMM’s Advanced Templates feature helps unlock the full IOS feature set and makes it available for customized gateway 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 Kinetic GMM templates. Advanced Templates can also be used to do custom configurations on the embedded access point (AP) inside the IR829.

Although the configurations possible with Advanced Templates are nearly endless depending on your use case and networking, security, and QoS requirements, some common examples are described in Advanced Templates, page 64, including:

- Firewall (access-lists) configurations for restricting access to specific applications or networks
- Quality of Service
- Ignition management for fleet use cases

Note: For additional examples of Advanced Templates, refer to the following RaMA modules:
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

- The Fleet module contains a detailed example of using Advanced Templates in conjunction with an IOx microservice to deliver gateway metric monitoring for the Netmotion Diagnostics app.

- The Remote Sites module contains examples of how Advanced Templates can be used to enable remote access to devices and applications deployed behind the Kinetic GMM managed gateway.

- The Network Integration module contains an example of using custom variables in Advanced Templates to enter a unique pre-shared key for each gateway’s site-to-site FlexVPN configuration.

Since the Advanced Templates allow for any IOS command, they can very easily modify the working configuration required for Kinetic GMM to be able to establish connectivity to the gateway or compromise the security of the device. Hence, this feature should be exercised with care and due diligence.

<table>
<thead>
<tr>
<th>Best Practices for use of Custom Configuration Templates:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Does not change any configuration related to CGNA.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete the “admin” or “operator” user.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete profile names “Flex_IKEv2” or “CVPN_I2PF”</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete tunnel interface numbers 1 or 2.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete tracking object numbers 2 or 4.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete dialer number 1, dialer-list 1 or Virtual-Template1.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete VLAN 555.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete route-maps “RM_Tu2” or “RM_WAN_ACL”.</strong></td>
</tr>
<tr>
<td><strong>Does not use/modify/delete ACL names “NAT_ACL”, “GWIPS”.</strong></td>
</tr>
</tbody>
</table>

A collection of scripts and Advanced Templates has been posted to GitHub. This regularly updated repository contains many of the examples shown throughout this CVD and more:
https://github.com/CiscoDevNet/iot-gateway-management

Figure 5  Selecting the Template

![Selecting the Template](image)
Management

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 their PC and an elevator in another city. This allows for remote diagnostics to troubleshoot issues, determine a solution, or dispatch a repair technician with the correct parts for the issue.

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 Kinetic 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 Kinetic GMM. You can schedule upgrades or trigger them immediately. An upgrade is available if displayed under Firmware Upgrades.

The upgrade process takes up to two hours. The firmware image is first downloaded to the gateway and then installed. The gateway will be down during the actual firmware upgrade 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, refer to:


Using Kinetic GMM APIs

Customers can integrate Kinetic GMM functionality with their own management and provisioning system or automate a bulk gateway on-boarding and provisioning process using RESTful APIs rather than using the Kinetic GMM UI. Examples of this are available at:

Kinetic GMM API Usage and Documentation:

Kinetic GMM Generating API Keys:

Firewall Ports for Kinetic GMM to Gateway Communication

If the routers are located behind a firewall, Cisco Kinetic requires specific TCP and UDP network ports to be opened and IP protocols to be permitted. This allows Cisco Kinetic to communicate with the gateways. Refer to the Technology Guidance module for the required settings.
GPS and Geofencing

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

A geofence can be easily defined in Kinetic 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. A geofence can be added by specifying a predefined radius around a geographical location or drawing a custom area on the map.

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


Monitoring

Kinetic 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 viewing its overall health, claim status, and event logs and running diagnostics and verifying network connectivity. Customers can also generate reports, set up audit logs, and create alerts based on the events on the gateways.
Using Cisco Control Center for SIM Card Management

Cisco Control Center (formerly Jasper Control Center) is a cloud–hosted platform that helps customers manage cellular connectivity to their device. With Control Center, customers can access a portal for monitoring the status of devices that use Control Center–compatible 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 Control Center APIs to access 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 for that account. Kinetic GMM displays summary information listing 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.

The section below describes in detail how Cisco Control Center can be used to manage SIM cards.

Note: For Control Center Support, contact your cellular carrier that offers you access.

Viewing All Devices

The Device List is the typical start page for manually working with devices in the Control Center user interface. Here you see a list of all devices visible to the user, optionally filtered by user–specified search criteria. You can access it by clicking Devices  --> Device List.
Design Considerations

**Figure 8 Devices List with Feature Highlights**

This page has the same search and filtering tools you will find on all list pages, along with the ability to show and hide columns and move them to different locations. For a detailed description of these features, see: https://simcontrolcenter.wireless.att.com/assets/documentation/lang_en/enterprise/iot/Content/get_started/data_filter.htm

In addition, the Device List page offers several device-specific options, as shown in Table 1.

**Table 1 Device Features and Descriptions**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device details link</td>
<td>By clicking the ICCID link, users can launch a pop-up window with details about the device.</td>
</tr>
<tr>
<td>Actions menu</td>
<td>From the Actions menu you can quickly change a device's SIM status or rate plan. You can also access Diagnostics and Spotlight, allowing you to hide those columns on the summary page and make more space for other, more useful columns.</td>
</tr>
<tr>
<td>Diagnostics link</td>
<td>By clicking the Diagnostics icon for a device, users with appropriate privileges can launch a diagnostic tool to analyze current device connectivity. Note that not all users will have access to this feature based on permissions granted by their user role.</td>
</tr>
<tr>
<td>Spotlight link</td>
<td>By clicking the Spotlight icon for a device, users with appropriate privileges can launch the Spotlight diagnostic tool to view a comprehensive history and timeline of network and provisioning activity for the device. Note that not all users will have access to this feature based on permissions granted by their user role.</td>
</tr>
<tr>
<td>Identifiers</td>
<td>These columns display the device ICCID, MSISDN, and IMSI identifiers. You can click any ICCID link to drill down to the corresponding Device Details page.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>The SIM State and In Session columns provide information about whether the device can connect to the network and whether the device is in a live session at the current moment.</td>
</tr>
<tr>
<td>Usage and rating</td>
<td>These three columns (Cycle to Date Usage, Usage Limit Reached, and Rate Plan) provide information about the device's data usage during the current billing cycle. You can click the rate plan link for any device to get detailed information about the cost of services.</td>
</tr>
<tr>
<td>Live Update Indicator</td>
<td>By default, Control Center automatically pushes any device changes to the screen without requiring a manual page refresh. All changes appear in yellow. You can turn off live updates in the user profile.</td>
</tr>
</tbody>
</table>
Viewing Device Details

The Device Detail page provides additional information about a particular device. You can access the page by clicking on the linked ICCID for a device on the Device List page or anywhere else in the application where a linked ICCID is displayed.

**Figure 9  Device Detail Page with Feature Highlights**

Device Details

Primary device attributes appear at the top of the Device Detail page. This information includes the device identifiers (ICCID, IMSI, IMEI), the SIM status, the activation date, and whether the device is in session.

An NB-IoT value in the In Session field indicates that the device is connected and using the NB-IoT transport.

Current Session

If the device is currently in session, the current session block will be visible with details about the current data session.

Access to the Current Session information depends on your network configuration. Not all users will see this information.

Details include:

- **Session Start**—The date and time when the session began.
- **Device IP Address**—The IP address assigned to the device when the session began.
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

- APN—The access point name over which the device is currently connected.

Additional Information

If a user needs to see full details available about a device, clicking the **Additional Information** control expands a collapsible region of the page with the remaining attributes available for the device beyond those displayed in the detail block. Clicking the **Additional Information** icon again collapses the region to maximize the screen real estate.

Subtabs

Subtabs are available in the bottom section of the Device Detail page. Each subtab contains important related details. Click a subtab on the Device Detail page to see more reference information, as shown in **Table 2**.

<table>
<thead>
<tr>
<th>Subtab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection History</td>
<td>Contains the device connection history, listed by data session. The data session history is organized by billing period. By default the device’s unbilled history is displayed. The user can view the data session history for any other past billing period by selecting the target period from the Billing Cycle drop down filter. Connection history records are displayed as they are received by the Control Center platform.</td>
</tr>
<tr>
<td>Location History</td>
<td>Contains the device location history, and can only be viewed by users with the AccountLBSUser role. Whenever device location information is captured, a line is added to the Location History subtab. Only the last 30 days of data is stored. This subtab appears only if Location Based Services (ADD-ON) is enabled for the device.</td>
</tr>
<tr>
<td>Connections</td>
<td>Shows a graphical display of the device's connection history, organized by billing period.</td>
</tr>
<tr>
<td>Audit Trail</td>
<td>Shows a history of all changes made to the device’s detail information.</td>
</tr>
<tr>
<td>SMS -&gt; Undelivered Messages</td>
<td>Shows a history of SMS messages that were undeliverable.</td>
</tr>
<tr>
<td>SMS -&gt; SMS Live</td>
<td>Shows a list of all SMS messages sent between the device and Control Center as well as their status (received or failed).</td>
</tr>
<tr>
<td>SMS -&gt; Message History</td>
<td>Shows a list of SMS messages received by or sent from the target device in a specific billing cycle.</td>
</tr>
<tr>
<td>Rating</td>
<td>Shows the current settings that control the device’s rating.</td>
</tr>
</tbody>
</table>

SIM States

Each device has a status that determines its ability to establish data connectivity on the network and affects whether the device is billable. **Figure 10** shows a typical life-cycle for a device. You can transition a device from one state to another, subject to certain restrictions.
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

Figure 10  Typical Life-cycle for a Device

The services available to a device in each state are governed by the communication profiles associated with the device's communication plan. Control Center applies the OFF communication profile to inactive devices and the ON communication profile to active devices.

Table 3 describes typical connectivity and billing behavior for each SIM state. In general, a device is billable only when it is Activated. However, contractual commitments may specify that an enterprise pay for a device even if it is not active.

Table 3  SIM States and Descriptions

<table>
<thead>
<tr>
<th>SIM State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Ready</td>
<td>An Activation Ready device can establish a data connection, but is generally not considered billable. When an Activation Ready device makes a data connection or sends an SMS, Control Center automatically changes its status to Activated, causing the device to become billable. In the case of a data connection, the device state transition occurs as soon as Control Center receives a data CDR. The workflow is similar in the case of SMS and voice services, with Control Center processing SMS or voice CDRs. Depending on how your account is set up, you may or may not be able to move a device from Activated to Activation Ready.</td>
</tr>
<tr>
<td>Replaced</td>
<td>In certain situations, you may want to replace one SIM with another. The new SIM inherits information from the original SIM and the original SIM receives a Replaced state. You must request this change from the operator.</td>
</tr>
<tr>
<td>Global Intransit</td>
<td>A SIM receives the Global Intransit state when an operator transfer is pending. In this state, the SIM is billable under the primary operator only. For details, see Global SIM at: <a href="https://simcontrolcenter.wireless.att.com/assets/documentation/lang_en/enterprise/iot/Content/global/intro.htm">https://simcontrolcenter.wireless.att.com/assets/documentation/lang_en/enterprise/iot/Content/global/intro.htm</a>.</td>
</tr>
<tr>
<td>Global Transferred</td>
<td>A SIM with the Global Transferred state cannot pass traffic and is not billable. Control Center has transferred this SIM to a partner operator within a global alliance. For details, see Global SIM at: <a href="https://simcontrolcenter.wireless.att.com/assets/documentation/lang_en/enterprise/iot/Content/global/intro.htm">https://simcontrolcenter.wireless.att.com/assets/documentation/lang_en/enterprise/iot/Content/global/intro.htm</a>.</td>
</tr>
<tr>
<td>Trial</td>
<td>A Trial SIM is one you receive with a starter kit and is intended to be used during a Control Center product evaluation. Devices containing trial SIMs have network connectivity, but are not considered billable.</td>
</tr>
<tr>
<td>Activated</td>
<td>An Activated device can establish data connections and is considered billable.</td>
</tr>
</tbody>
</table>
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

SIM State Transitions

You can manually change the device SIM status from the Device List page using the Actions menu associated with the device you want to change. Click Devices -> Device List -> Actions drop-down menu-> Change SIM Status.

<table>
<thead>
<tr>
<th>SIM State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deactivated</td>
<td>The Deactivated state does not allow a device to establish data connections. Devices in the Deactivated state are generally not considered billable unless a commitment applies. Typically, Deactivated devices have been deployed, but they are temporarily inactive.</td>
</tr>
<tr>
<td>Inventory</td>
<td>The Inventory state does not allow a device to establish data connections. Devices in the Inventory state are generally not considered billable. Devices in the Inventory state behave similarly to those in the Deactivated state. Typically, devices in Inventory have not been deployed yet, while Deactivated devices have been deployed, but they are temporarily inactive.</td>
</tr>
<tr>
<td>Purged</td>
<td>The Purged state does not allow a device to establish data connections. A Purged device has been physically removed from the network by the operator, typically in response to a customer request or as part of a SIM replacement policy. Contact your operator to learn about their policies for moving a device to the Purged state.</td>
</tr>
<tr>
<td>Retired</td>
<td>The Retired state does not allow a device to establish data connections. A device in this state is generally not considered billable unless a commitment applies. Typically, a Retired device is permanently inactive and ready to be moved to a Purged state for removal from the network. If necessary, users can move a Retired device to a different SIM state.</td>
</tr>
</tbody>
</table>
| Test Ready | The Test Ready state allows a device to establish a data connection and use other services free of charge. SIMs in this state are not considered billable. By default, the Test Ready state provides each device with the following services, although the operator may configure these amounts differently:  
  - Data—20KB  
  - SMS—Two messages  
  - Voice—Two minutes  
As soon as the device reaches the configured limit for any service (data, SMS, voice, or other), the device will transition to the target state and no more free test traffic will be available for any service. Typically, the target state for SIMs exceeding their Test Ready threshold is either Activation Ready or Inventory. The operator can configure this transition to suit the enterprise business model. Depending on how the account is set up, you may or may not be able to move a device from Activated back to Test Ready. |
Assigning Rate Plans Manually

If a device is on a monthly plan, there are two quick ways to change the rate plan within the Devices category:

- Click **Devices** -> **Device List** -> **Actions** menu -> **Change Rate Plan**.

You can also edit the rate plan value in the **Edit Device** pop-up menu.

- Click **Devices** -> **Device List** -> **Device checkbox** -> **Actions** menu -> **Edit Selected** -> **Rate Plan** field.
Prepare for Deployment

A key benefit of the Cisco RaMA 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 section describes the process for preparing for ZTD from an IT user’s perspective. It includes the key steps required to set up the Kinetic GMM template and user accounts and, if required, to prepare an existing gateway to be claimed by Kinetic GMM using GPT.

**Note:** Refer to the Field Deployment module for an OT user perspective of the deployment of gateways in the RaMA solution.

**Figure 14  Prepare for Deployment**

1. Create Kinetic GMM template.

Other modules describe the technologies, architectures, and best practices for architecting and designing the Cisco RaMA solution. This will enable IT staff to create a Kinetic GMM Template with the required features and functionality.
Design Considerations

Cisco recommends that customers use Kinetic GMM templates rather than Cisco IOS to configure the gateways unless directed to IOS by Kinetic GMM support. This will prevent gateway configurations that could conflict with Kinetic 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. Kinetic 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, refer to: https://developer.cisco.com/docs/kinetic/#!gmm-overview

2. Enable Kinetic GMM access for field operators.

The Kinetic 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

3. Activate SIM cards.

Other modules 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.

4. Use the GPT process for existing gateways.

As described in Cloud Provisioning and Management (https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/RaMA/RaMA-DIG/RaMA-DIG.html#90940), new Cisco IRs that are purchased with the Kinetic GMM option selected are set up for Kinetic GMM at the factory prior to being shipped. Customers that want to enable Kinetic GMM for existing routers (and other routers that were not purchased with Kinetic GMM enabled) need to use the GPT to prepare these routers for Kinetic GMM.

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

Preparing to Use the Gateway Provisioning Tool

Prior to configuring the gateway using GPT, users 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 GPT:
https://software.cisco.com/download/home/286321160/type/286321251/release/

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)
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

- IR809—GigabitEthernet0 (GE0)
- IR829—GigabitEthernet1 (GE1)

4. Run GPT.

Write down the serial number of the gateways being set up using GPT. For additional help with GPT, refer to: https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/kinetic-gateway-management-module/213753-troubleshoot-common-provisioning-issues.html

Running the Gateway Provisioning Tool Process

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

- Gateway serial number
- Custom APN information (if required)
- Expected deployment geo (us.ciscokinetic.io for US or eu.ciscokinetic.io for Europe)
- Port in use for the Ethernet cable
- Gateway’s IP address (if static IP is required)
- Host IP of the PC that is connected to the gateway
- Whether the AutoSIM feature needs to be activated (refer to https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/RaMA/RaMA-DIG/RaMA-DIG.html#33072 for further information)
- Option for use of Cartridges for IOx or Custom IOS Configurations (the default is “No” unless instructed to do so by Kinetic GMM Technical Support)

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 Kinetic GMM Organization

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

Contact Kinetic GMM Technical Support by logging into Kinetic 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.

Recommended RMA Process

In the event that there is a hardware failure that requires the gateway to be replaced, it is important to have a documented RMA process in place to minimize downtime. Figure 15 illustrates the steps involved in replacing failed hardware.
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

**Figure 15  RMA Process**

1) Remove defective gateway from install location
2) Notify OT and ship gateway to IT department

1) Receive hardware from OT department
2) Remove SIM card(s)
3) Delete gateway from GMM, noting which template was applied
4) RMA the hardware with Cisco
5) Receive replacement gateway from Cisco, or use spare gateway from local inventory
6) Insert SIM into replacement gateway
7) Run GPT on gateway (if not already run)
8) Update any internal systems with new gateway’s serial number
9) Ship gateway to OT department

1) Physically install replacement gateway
2) Claim gateway in Kinetic GMM using same template from old gateway
3) Verify gateway comes online in Kinetic GMM

The steps described in the flowchart use many of the same basic processes for deploying a new gateway, but require a few extra steps. The OT and IT departments should have an established communication channel in place to make the process go smoothly.

**Advanced Templates**

Kinetic GMM allows the use of Advanced Templates to apply additional Cisco IOS configurations. The advanced templates are written in Freemarker markup (https://freemarker.apache.org/). This section contains some examples of these configurations. All of these templates can be added to Kinetic GMM Templates by the end user as long as their Kinetic GMM organization is enabled for Advanced Templates.

- **Firewall**
- **Quality of Service**
- **Ignition Sensing**

**Note:** For additional examples of Advanced Templates, refer to the Fleet and Remote Site modules. The Fleet module contains a detailed example of using Advanced Templates in conjunction with an IOx microservice to deliver gateway metric monitoring for the NetMotion Diagnostics app. The Remote Sites module contains examples of how Advanced Templates can be used to enable remote access to devices and applications deployed behind the Kinetic GMM managed gateway.

Refer to the official Kinetic GMM documentation on DevNet for additional details on the use of Advanced Templates: https://developer.cisco.com/docs/kinetic/#advanced-templates/create-advanced-templates-for-router-and-ap-configurations

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".
Remote and Mobile Assets—Zero Touch Provisioning

Design Considerations

- 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”.

Note: As a best practice, verify that an Advanced Template configuration works as planned and does not break Kinetic GMM functionality on a single, non-production gateway before rolling out the template to production use.

Figure 16   View of the Advanced Template in the GUI

Additionally, there are some predefined variables that can be used in the flexible template, as shown in Table 4.

Table 4  Currently Available Predefined Variables

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gw.sn</td>
<td>GW Serial Number</td>
</tr>
<tr>
<td>gw.model</td>
<td>GW Model</td>
</tr>
<tr>
<td>gw.wan_if</td>
<td>GW’s WAN interface (e.g., “GigabitEthernet0”, “Cellular0”)</td>
</tr>
<tr>
<td>gw.wan_if_sec</td>
<td>GW’s Secondary WAN interface (e.g. Dual LTE)</td>
</tr>
<tr>
<td>gw.subnet</td>
<td>Subnet for GW’s 32 IPs (a /27 address, e.g., “10.9.18.32”)</td>
</tr>
<tr>
<td>gw.sn</td>
<td>GW Serial Number</td>
</tr>
<tr>
<td>gw.model</td>
<td>GW Model</td>
</tr>
<tr>
<td>gw.wan_if</td>
<td>GW’s WAN interface (e.g., “GigabitEthernet0”, “Cellular0”)</td>
</tr>
</tbody>
</table>
### Table 4: Currently Available Predefined Variables (continued)

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gw.wan_if_sec</td>
<td>GW’s Secondary WAN interface (e.g., Dual LTE)</td>
</tr>
<tr>
<td>gw.subnet</td>
<td>Subnet for GW’s 32 IPs (a /27 address, e.g., “10.9.18.32”)</td>
</tr>
<tr>
<td>gw.netmask</td>
<td>GW’s 32 IP’s subnet (“255.255.255.224”)</td>
</tr>
<tr>
<td>gw.ip</td>
<td>GW’s IP (e.g., “10.9.18.33”)</td>
</tr>
<tr>
<td>gw.ip_prefix</td>
<td>GW IP’s first three numbers, separated by “.” (this makes calculating IPs easier, e.g., “10.9.18”)</td>
</tr>
<tr>
<td>gw.ip_suffix</td>
<td>GW IP’s last byte (e.g., “33”)</td>
</tr>
<tr>
<td>gw.gos_ip</td>
<td>GW’s GuestOS IP (e.g., “10.9.18.34”)</td>
</tr>
<tr>
<td>gw.lan_if</td>
<td>GW’s LAN interface name (e.g., “Gi1”, “Vlan1”, depending on model)</td>
</tr>
<tr>
<td>gw.lan_ip</td>
<td>GW’s LAN IP</td>
</tr>
<tr>
<td>gw.lan_subnet</td>
<td>GW’s LAN subnet</td>
</tr>
<tr>
<td>gw.lan_netmask</td>
<td>GW’s LAN netmask (e.g., “255.255.255.240”)</td>
</tr>
<tr>
<td>gw.lanWildcard</td>
<td>GW’s LAN wildcard (negative of lan_netmask for ACL, e.g., “0.0.0.15”)</td>
</tr>
<tr>
<td>gw.vpn.pri_ip</td>
<td>Site-to-Site VPN’s peer IP (primary)</td>
</tr>
<tr>
<td>gw.vpn.sec_ip</td>
<td>Site-to-Site VPN’s peer IP (secondary)</td>
</tr>
<tr>
<td>gw.sn</td>
<td>GW Serial Number</td>
</tr>
</tbody>
</table>

The following sections contain examples of custom configuration that can be enabled with Kinetic 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
```

#### 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 Advanced Template 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:

- 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.

- 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 queueing, and fair queueing to different classes.

- 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.
Design Considerations

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:

Below is the sample QoS configuration that can be applied using Kinetic GMM Advanced Templates:

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.

ignition off-timer 900
ignition undervoltage threshold 11
ignition enable
Appendix—Sample Kinetic GMM Report

Figure 17  Sample Kinetic GMM Report

<table>
<thead>
<tr>
<th>Report Name - Cell Report</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Gateway Name</th>
<th>Gateway Serial Numbers</th>
<th>Model</th>
<th>Wi-Fi SSID</th>
<th>Group(s)</th>
<th>Subscribed Device - IP Address</th>
<th>Subscribed Device - 802.11b</th>
<th>Subscribed Device - 802.11g</th>
<th>Subscribed Device - 802.11a</th>
<th>Carrier</th>
<th>Carrier 1 IP Address</th>
<th>MAE_1</th>
<th>DCCM_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregator-02</td>
<td>DEE-00933-725-22555</td>
<td>VSBW</td>
<td>AT&amp;T</td>
<td>33200000151199</td>
<td>09117032748261399</td>
<td>100.10.0.5</td>
<td>100.120.10.50</td>
<td>100.120.10.50</td>
<td>AT&amp;T</td>
<td>332100000151603</td>
<td>09117032748261399</td>
<td>100.10.0.5</td>
</tr>
</tbody>
</table>

| 02108-22TE | Bomm Lab | DEE-0257-0256-S805 | VSBW | AT&T | 09117032748261399 | 100.120.10.50 | 100.120.10.50 | 100.120.10.50 | AT&T | 332100000151603 | 09117032748261399 | 100.10.0.5 | 100.120.10.50 | 100.120.10.50 |

| EAP | Extensible Authentication Protocol |
| EAPoL | EAP over LAN |

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>
</tbody>
</table>

68
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEM</td>
<td>Embedded Event Manager</td>
</tr>
<tr>
<td>GMM</td>
<td>Cisco Kinetic 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>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>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>
Remote and Mobile Assets—Enterprise Network Integration

This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: www.cisco.com/go/rama

- Solution Brief—An overview of the RaMA CVD and the available modules.
- Design and Implementation Guide (DIG)—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- Technology Guidance Module—Overview of the available hardware options for IoT gateways in the RaMA solution, with recommendations on hardware platform and software features to use for common scenarios.
- Security Module—Describes how the RaMA solution was designed from the ground up with security in mind. Includes detailed descriptions of how the solution fits into the SAFE model, including securing the gateways, data plane, and management plane. Also includes a section on achieving PCI compliance.
- Remote Site Management Module—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- Fleet Management Module—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- Zero Touch Provisioning Module—Use of Kinetic GMM by IT personnel for provisioning and managing Cisco Industrial Routers with a focus on secure, scalable deployment.
- Field Deployment Module—Use of Kinetic GMM by OT personnel for deploying Cisco Industrial Routers in the field, with minimal knowledge of the underlying networking technology required.
- Edge Compute Module—Overview of the edge compute capabilities in Cisco Industrial Routers in the form of IOX. Includes implementation examples for deploying Dockerized applications.

This module includes the following sections:

<table>
<thead>
<tr>
<th>Overview, page 72</th>
<th>A brief summary of the RaMA Enterprise Network Integration module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements, page 72</td>
<td>Typical Enterprise Network Integration requirements including resiliency, redundancy, high-availability, load balancing, and security.</td>
</tr>
<tr>
<td>Architecture, page 73</td>
<td>Overall enterprise networking architecture to meet the above requirements.</td>
</tr>
</tbody>
</table>
Overview

This module describes the architecture, design options, and best practices to achieve network integration between the edge of the Internet of Things (IoT) fabric and enterprise networks.

- **Headend design:**
  - Headend router options (virtual and physical appliances) to achieve different levels of scalability
  - Resiliency, redundancy, high-availability, and load balancing
  - Integration with Cisco Identity Services Engine (ISE) and Active Directory (AD) for identity management and authentication
  - Integration with enterprise IP Address Management (IPAM) server and Domain Name Server (DNS)

- **Edge gateway design:**
  - Options for achieving WAN redundancy
  - Edge gateway routing options:
    - Split tunnel—Only traffic destined to enterprise networks traverses the tunnel. All other traffic is routed directly to the internet.
    - Full tunnel—All traffic (enterprise bound and internet bound) is tunneled back to the enterprise headquarters.

Requirements

- Secure connectivity from the edge devices to the enterprise headquarters.
- Extend reachability of enterprise networks and services to the edge of the IoT fabric.
- Redundancy, high-availability, and load balancing for edge-to-enterprise connectivity.
- Ability for edge devices and sensors to securely send data to applications and analytics software running within the enterprise headquarters.
Remote and Mobile Assets—Enterprise Network Integration

Architecture

- Access to management systems deployed at the enterprise headquarters.
- Ability to support either a full tunnel or split tunnel from the edge gateway.
- Ability to advertise only specific enterprise networks to the edge gateway.
- Payment Card Industry (PCI) compliance
- Ability to leverage corporate security tools and policies for data access at the edge.

Refer to the RaMA Security module for the complete security recommendations including the use of FlexVPN for the enterprise network integration:

The architecture diagram in Figure 1 highlights support for use cases that require extending enterprise network access in a highly secure manner to the edge of the IoT fabric. This architecture utilizes secure FlexVPN connectivity from the edge gateways to a cluster of VPN aggregators within the enterprise data center. This is optimal for enterprises that need to transfer sensitive and confidential information between edge devices and corporate headquarters or need to securely extend access to the edge for certain enterprise networks or services.

Design

VPN Headend Design

To securely extend enterprise connectivity from the enterprise headquarters to the edge gateways, this solution uses secure IPSec/FlexVPN connectivity. The components required to implement the enterprise headend portion of the design include:

- A cluster of highly available, redundant, and scalable routers to terminate the incoming FlexVPN connections from the edge gateways.
- Ability to integrate with Cisco ISE and AD for centralized identity management and authentication of IPSec VPN sessions.
- Optional Integration with enterprise DNS and IPAM servers.

Choice of Headend Router Platforms

Cisco offers a number of headend router options depending on scalability requirements:

- Small deployments—For a pilot deployment or one involving a few hundred gateways, we recommend using a cluster of Cisco CSR 1000v virtual appliances at the headend in order to terminate the FlexVPN connections coming in from the edge gateways.
- Medium deployments—For a deployment involving a few hundred to a couple thousand edge gateways, we recommend using a cluster of the physical Cisco ISR 4000 series or the Cisco ASR 1000 series of routers that provide higher scale and throughput capabilities.
- Large deployments—For a deployment scaling to thousands of edge gateways, we recommend using a cluster of the physical Cisco ASR 1000 series of routers which provide extreme scalability and throughput capabilities.
Remote and Mobile Assets—Enterprise Network Integration

Design

Figure 2  FlexVPN Scalable Headend Architecture—Platform Choices

VPN Head End Resiliency Options

Multiple methods are available to support VPN resiliency at the enterprise headquarters. As detailed in IKEv2 Load Balancing, page 78, this design proposes the use of a cluster of headend routers running Hot-Standby Router Protocol (HSRP) and Internet Key Exchange Protocol version 2 (IKEv2) load balancing to provide VPN resiliency at the enterprise headquarters.

Embedded Event Manager (EEM) scripts can 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.

The following sections describe design options to achieve headend redundancy and high-availability. For this CVD we validated Option 2, which provides physical site redundancy.

Figure 3  Option 1—Geographical Redundancy

- Locate the first headend router (HER), HER-1 @ DC1 @ Location-1.
- Locate the second HER-2 @ DC2 @ Location-2.
- Configure a different Pre-Shared Key (PSK) on each of the HERs.
- In the GMM Template, configure the HER-1 with its PSK and HER-2 with its PSK.
- If HER-1 fails, the tunnels are re-negotiated and get established to HER-2.
To achieve load balancing with this option, you can create two templates within GMM. For the first half of the gateways we can configure HER-1 as the primary and HER-2 as the secondary. For the second half of the gateways we can configure HER-2 as the primary and HER-1 as the secondary.

**Figure 4  Option 2—Physical Site Redundancy**

- **HSRP and IKEv2 load balancing cluster**
- **Single master node**
- **N-number of slave nodes**
- **Master keeps track of load on each slave**
- **Incoming IKEv2 request re-directed to the Least Loaded Gateway (LLG)**

**Enterprise Network Integration**

**Figure 5  Simplified Enterprise Network Integration**
Design

The core network components include:

- Data center infrastructure—This includes compute resources and networking resources like switches and routers, WLC, and enterprise firewalls.

- VPN headend—VPN headend cluster design and implementation to support scalability, redundancy, high-availability, and load balancing of incoming VPN sessions.

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

For the CVD, we validated the design with both a pair of Cisco CSR 1000v virtual appliances and a pair of Cisco ASR 1002–HX physical appliances.


- For a more detailed enterprise headquarters network design, refer to: https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides.html

FlexVPN Headend Design

We recommend using a pair of HERs running HSRP and IKEv2 load balancing in order to provide redundancy and load balancing for incoming Flex VPN sessions from the edge gateways at the enterprise headend side.


Figure 6  IKEv2 Load Balancing Cluster Design

IKEv2 Load Balancing

The IKEv2 load balancing feature enables the clustering of a group of routers for high-availability and distribution of incoming IKEv2 sessions among the routers that are part of the cluster. It redirects incoming FlexVPN/IKEv2 client requests to the least-loaded router based on system and crypto load factors.

Prerequisites for IKE-v2 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 IKEv2 load balancing include:

- The IKEv2 load balancing 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 only need to know the virtual IP address of the cluster.
- The entire crypto session is redirected to the least-loaded router in the cluster.

IKEv2 clustering provides 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 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.
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 “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:

- Hot-Standby Router Protocol (HSRP)
- CLB master
- CLB slave(s)
- CLB communication
- IKEv2 redirects mechanism

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 the 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 tested design used dual Cisco CSR 1000v virtual appliances 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 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 master. 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 for each new incoming IKEv2 connection.

**Integration with ISE for Centralized Identity Management and Authentication**

This design builds on the architecture described in *Enterprise Network Integration, page 76*, adding the following components to implement it:

- Cisco ISE for providing centralized authentication service.
- AD for centralized identity management service.
- Cisco Prime Network Registrar (CPNR) is used as an IPAM server for managing a pool of gateway tunnel IP addresses.
- AD as the DNS server for creating DNS records (e.g., Bus-1234 pointing to the corresponding gateway tunnel IP) for easy identification and connectivity to gateways using a common identifier.

The main advantages of this design are:

- Provides centralized identity management.
- Provides centralized authentication for incoming FlexVPN sessions.
- Drastically reduces the overhead to configure each of the headend routers by eliminating the need to add headend configuration corresponding to each on-boarded edge gateway.

Another advantage of this option is simplified asset inventory and management through user-defined asset identifiers (e.g., Bus 1234) used to easily identify the edge gateway. This provides a number of benefits especially for large deployments:
Remote and Mobile Assets—Enterprise Network Integration

Design

- Allows the Vehicle ID to be used for gateway authentication until the vehicle is put out of service or de-commissioned.
- Simpler maintenance and troubleshooting by allowing IT and field administrators to easily reach the gateway installed in the asset by using a common identifier rather than having to reference an Excel sheet or an inventory management system.
- Continued use of the same Vehicle ID for authentication even if the gateway is replaced.

**Note:** Even though the use case described in this CVD is for the fleet vertical, the same design principle can be applied to fixed-asset use cases such as a warehouse or a manufacturing plant floor. In these scenarios, the Vehicle ID can easily be substituted with a Machine ID, Robot ID, or any other Asset ID both for authentication and ease of identification/management. The only requirement is that there is a 1:1 mapping between the asset and the gateway to which it is connected.

This design will not work for use cases where there are multiple assets, such as multiple robots or machines, connected to the same edge gateway.

**Figure 8 Enterprise ISE/AD/IPAM/DNS Integration**

Enterprises might prefer this deployment option if they already have the Cisco ISE or are planning on deploying it. The advantage of this design is that ISE and AD act as a central point of authentication for all of the FlexVPN/IKEv2 sessions incoming from the edge gateways. This automates gateway identity management by pre-configuring ISE and AD to use them for session authentication. This also simplifies the headend configuration by reducing the need for the three lines of configuration required for each HER to recognize the edge gateways.

**Key Design Elements**

- The Vehicle ID is used as user name credential while negotiating the tunnel setup between the gateway and the headend router.
- The headend router in turn uses the Vehicle ID to authenticate with the Cisco ISE policy engine to determine if the tunnel setup should be permitted from this particular gateway.
Remote and Mobile Assets—Enterprise Network Integration

Design

- If the tunnel setup is permitted, then the gateway tunnel IP address to be used by that gateway is retrieved from the IPAM server by requesting the next available IP address from a subnet/pool of IP addresses reserved for use as gateway tunnel IP addresses.

- An A-PTR entry in a DNS server can be created which helps resolve the vehicle name to the gateway tunnel IP address, which facilitates connecting to the gateway located in the vehicle by using a DNS name such as Bus-1234 or Taxi-456.

- The gateway serial number is correlated to the Vehicle ID and is used to change the gateway name in GMM to the vehicle. This again facilitates the association of the gateway to the vehicle in which it is installed and helps IT and field technicians with management and troubleshooting.

Component Integration and Message Flow

Figure 9  Component Interactions and Message Flow

1. Perform the following:

- Configure users and credentials in AD. Configure an identity corresponding to each vehicle.

- Reserve a subnet/pool of IP addresses for gateway tunnel IP addresses in IPAM. The pool should be large enough to accommodate all of the gateways within the deployment.

- Configure ISE to integrate with AD.
Remote and Mobile Assets—Enterprise Network Integration

Design

2. EEM script retrieves Vehicle ID (VID) from a connected device (CANBUS, on-board management appliance, etc.). This VID maps to the username field in ISE/AD.

   Note: The specific EEM script mentioned here is outside the scope of this document as it is very specific to the connected device. When developing a custom script to perform this ID extraction, the EEM script should take the extracted ID and change the IOS configuration to replace the IKEv2 local identity (username). By default, a GMM configured gateway will use the gateway’s serial number for this local ID.

3. The IKEv2 profile in the HER references the remote email identity of @iotspdev.io. During the IKEv2 negotiation phase, each gateway sends an identity of the form Bus-<VID>@iotspdev.io. The HER uses an IKEv2 name mangler to strip out the domain name @iotspdev.io to retrieve just the Bus-<VID> as the username attribute for authentication with ISE.

4. The HER uses the credentials to authenticate the incoming IKEv2 session against ISE. It uses a pre-defined authentication password to access ISE and another password for each gateway as the PSK for the IKEv2 authentication.

5. ISE authenticates the IKEv2 session based on the user credentials provided by the HER and either accepts or rejects the session by consulting the authentication credentials populated in AD.

6. ISE responds by providing the gateway tunnel IP address retrieved from the IPAM server by requesting the Next Available IP address. ISE provides the IP address in the form of a FRAMED IP ADDRESS to the gateway.

7. HER responds back to the gateway with the tunnel IP address it needs to use.

8. (Optional): Populate DNS server with an A-record to map the Vehicle Name to the gateway tunnel IP address (e.g., Bus-1234 points to an IP address of 10.5.0.5). This optional step allows IT and field technicians to easily identify and connect to the gateway during management and troubleshooting.

9. (Optional): Configure GMM using either the UI or API to rename the gateway to something like Bus-1234 or Taxi-456. This optional step allows IT and field technicians to easily identify the gateway within GMM.

Sample User Account within Cisco ISE

- Name: Bus-1234
- Status: Enabled
- Email: Bus-1234@iotspdev.io
- Login password: ******
- FN: Kinetic
- LN: 1234
- User Custom Attributes: Tunnel IP Address
- User Groups: Buses

ISE User-Account Configuration

- Create an account for each vehicle under Identities -> Network Access Users (e.g., Bus-1234 or Taxi-456).
- The network access user name must match the VPN-ID coming in from a headend router.
- When the identity comes in via IKEv2 it will be in the form of an email such as Bus-1234@iotspdev.io.
- The IKEv2 name mangler can be used to strip out the domain @iotspdev.io, resulting in the VPN identity (Bus-1234) needed to authenticate with ISE.
Remote and Mobile Assets—Enterprise Network Integration

Design

- Each user is associated with a login password, which is the PSK used for tunnel negotiation along with the user name. This password is defined within the Authorization profile associated with the group of routers created in ISE. This is the password that needs to also be populated within the GMM gateway profile template.

- Each user account is associated with a specific group.

- An IPAM server is used to reserve an IP address for the gateway and also create a DNS record.

- A User custom attribute is used in the User Account settings to assign the tunnel IP address retrieved from the IPAM server.

- The IPAM server provides the next available IP address from the pool of reserved IP addresses.

Sample Cisco ISE Policy Set and Authorization Profile

- Policy Set
  - References Authorization Profile

- Authorization Profile
  - Access Type = ACCESS_ACCEPT
  - IP Address
  - IP Netmask
  - Tunnel Password = PSK
  - Cisco AV-pair = ipsecroute-set-interface
  - Cisco AV-pair = ipsecroute-set-access-list PERMIT_ANY

ISE Policy-Set Configuration

- Create an Authorization Policy Set for each vehicle category.

- Each authorization policy set is associated with a corresponding authorization profile.

- Each authorization profile corresponds to an IKEv2 profile created on the HER.

ISE Authorization Profile Configuration

- Define RADIUS attribute for VPN PSK.

- Use RADIUS attributes to assign Tunnel IP Address/Mask. This is how the Tunnel IP Address/Mask gets transmitted to the actual gateway.

IPAM Server Configuration

- Reserve a pool of tunnel IP addresses in IPAM server for each vehicle category.

- Returns the next available IP address from the pool.

DNS Server Configuration

- Create a DNS A-record pointing to the gateway tunnel IP address. For example: Bus-1234 points to gateway tunnel IP address 10.0.5.5.

Note: For additional details on implementing this use case, refer to Appendix A—Implementing Integration with ISE, page 87.
Edge Gateway Design

Gateway Cellular Redundancy Options

- Dual-LTE—This deployment model provides the highest resiliency with the use of two separate cellular radios each with their own SIM card from two separate providers.
- Single-LTE Dual-SIM—This deployment model provides resiliency by allowing the use of a backup 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.

Options for Edge Gateway Routing

Option 1—Split Tunnel

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 process traffic intended for the internet. The downside is that all traffic intended for the internet will be allowed. This design is suited for enterprises that want to forward all internet bound traffic directly to the internet without any inspection, filtering, blocking, or application of any other security policies.

Figure 10  Split Tunnel Routing at Edge Gateway
Option 2—Full Tunnel—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 can be implemented by enterprises that have strict network policies requiring total control over and requirements to inspect and filter all traffic. In this scenario, enterprise firewall rules can be applied and enforced within the enterprise data center before the traffic is forwarded to its intended 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 Web-Application Firewall (WAF) before routing the traffic to the public internet and apply and enforce rules regarding traffic that 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.

Best Practices

FlexVPN Headend Router Deployment Best Practices

- Deploy each of the Cisco CSR 1000v virtual appliances on separate virtualization hosts—possibly in separate racks—to protect against underlying host failure or power failure for a particular rack.
- For the physical Cisco ASR 100X routers, use applicable high-availability technologies like IOS-XE process redundancy, dual-route processors (RPs) for hardware control-plane redundancy, and dual ESPs.
- For the physical Cisco ASR 100X routers, it is best practice to deploy each physical appliance in a separate rack attached to a different power supply strip. It is also highly recommended to have dual power supplies in each of the physical routers connected to two different power strips within the rack so as to provide resiliency against failure of a particular power supply or an entire power strip.
We recommend using a pair of HERs running HSRP and IKEv2 load balancing in order to provide redundancy and load balancing for incoming Flex VPN sessions from the edge gateways at the enterprise headend side.

**General Best Practices**

- Configure a meaningful name for the gateway in GMM (e.g., Bus-1234, Robot-456, Machine-11, etc.) that helps with identification, management, and troubleshooting.
- Create a DNS entry for each gateway with a meaningful name pointing to the data tunnel IP address. Again this will help IT and field technicians to refer to the gateway by a meaningful name and be able to connect to the gateway using its DNS name rather than having to consult an Excel sheet or inventory management system to determine the data tunnel IP address for that gateway (e.g., ssh admin@Bus-1234).

**Appendix A—Implementing Integration with ISE**

When a gateway tries to connect to the customer’s data center, it is important to make sure that the gateway actually has permission to do so. Otherwise, unwanted devices could remotely gain access to the data center and allow someone to seriously damage the data center.

In the previous version of RAMA, the establishment of FlexVPN tunnels between gateways and the headend router (HER) was handled entirely by the HER. The authentication and authorization were both performed via local pre-shared key and the gateway tunnel IP address was supplied by a DHCP pool configured on the HER. This method benefited from ease of setup (only the HER was required to configure manually), but some of the downsides included:

- Not scaling well since specific CLI configuration would be required for every gateway.
- Network rules were limited to the capabilities of the HER.
- Device management was all CLI based.

This appendix presents the steps for allowing FlexVPN tunnels to instead be authenticated, authorized, and configured through a combination of ISE, Windows Active Directory (AD), and Cisco Prime Network Registrar (CPNR). The benefits of this design are:

- The external pieces are easily managed.
- Scales well.
- Enhanced customizability and security.

The logical flow of this design is as follows:
1. The tunnel is first authenticated locally via pre-shared key. The gateway and HER will check against the locally configured keyrings.

2. Once the initial authentication is successful, the HER will send an authorization request to ISE. This request will include a pre-shared key defined on the HER, as well as a username that is obtained from IKEv2 communication between the gateway and the HER.

3. ISE receives the authorization request and makes sure it is sent from an accepted network device. Once this has been verified, ISE takes the username/password it receives and queries AD to make sure they are valid.

4. ISE then authorizes the network connection, telling the HER to forward DHCP requests to CPNR. The CPNR then offers the next available IP address to be applied to the gateway tunnel interface, completing the flow.

The following sections assume that all systems have already been installed and focuses strictly on the relevant configuration for:

- IR 829 (gateway) via GMM
- HER (ASR 1000)
- ISE
- AD
- CPNR

### IR 829 GMM FlexVPN Configuration

There is nothing that needs to be done differently on the gateway to support this scenario (compared to the previous version). To configure the Site-To-Site VPN:

1. Enable “Site-to-Site VPN” in the GMM template.
2. Enter the Public IP Address of the HER.
3. Enter the Pre-shared key to be used. No other options are supported at this time.
4. Claim the gateway specifying this template.
HER Configuration

The HER serves as the FlexVPN hub. All desired gateways configured for site-to-site VPN will try to establish a connection with this hub and the major configuration sections are as follows:

- **AAA**
- Loopback Interface
- Virtual-Template
- IKEv2 Name-Mangler
- IKEv2 Profile

**AAA**

The AAA configuration is responsible for defining:

- Local and Remote authentication/authorization
- The RADIUS Server (ISE) for remote authentication/authorization
- Interface to use for ISE communication

```plaintext
aaa new-model
!
!
aaa group server radius ISE
  server name ISE24
  ip radius source-interface Port-channel1.30
!
aaa authentication login default local
aaa authorization exec default local none
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
!
!
aaa server radius dynamic-author
  client ISE_ADDRESS server-key PASSWORD
!
aaa session-id common
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 20 tries 2
radius-server deadtime 1
!
radius server ISE24
```
address ipv4 ISE_ADDRESS auth-port 1645 acct-port 1646
key PASSWORD
!

Loopback Interface

The loopback interface serves as the source interface for all the FlexVPN tunnels.

interface Loopback0
  ip address IP_ADDRESS NETMASK
  ip mtu 1400
!

Virtual-Template

Whenever the gateway tries to form a tunnel with the HER, a virtual tunnel interface will be created from referencing the virtual template.

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  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

ISE will supply additional configuration for the created virtual tunnel interface during the authorization process.

IKEv2 Name Mangler

The name-mangler extracts the username from the email address provided during local authentication. It is then used in the authorization request to ISE. As mentioned in Design, page 74, real world use cases may want to use a different string as the username (such as the vehicle ID, robot ID, etc.) instead of the gateway’s serial number (as is shown in this example). We recommend using a custom EEM script to extract this ID from the connected device and change the IKEv2 local identity configuration on the gateway.

crypto ikev2 name-mangler PSK
  email username

IKEv2 Profile and IKEv2 Keyring

The authorization profile is used to define the authentication/authorization mechanisms based off the email domain in the IKEv2 messages from the gateway. The authentication method is pre-shared key via a local keyring, while the authorization method is a request to ISE (containing the name-mangler username and a predefined password). A user account must be created on AD that matches the username /password since ISE is going to reference AD instead of a local ISE database.

crypto ikev2 profile Flex_IKEv2
  match fvrf any
  match identity remote email domain iotspdev.io
  identity local key-id public_ip_address
  authentication remote pre-share
  authentication local pre-share
  keyring local field_keys
  dpd 250 10 on-demand
  aaa authorization user psk list FLEX name-mangler PSK password AD_password
  aaa accounting psk FLEX
virtual-template 1
!
crypto ikev2 keyring field_keys
peer SIMULATED
  identity email domain iotspdev.io
  pre-shared-key password
!

Sample Configuration

!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname ASR1K-A-Top
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
enable password lab
!
aaa new-model
!
!
aaa group server radius ISE
  server name ISE24
  ip radius source-interface Port-channel1.30
!
aaa authentication login default local
aaa authorization exec default local none
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
!
!
aaa server radius dynamic-author
  client ISE_IP server-key ISE_PASSWORD
!
aaa session-id common
!
!
ip name-server DNS_IP
ip name-server vrf Mgmt-intf DNS_IP
ip domain lookup source-interface Port-channel1.251
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-3103357051
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3103357051
revocation-check none
rakeypair TP-self-signed-3103357051
!
!
crypto pki certificate chain TP-self-signed-3103357051
certificate self-signed 01
30820330 30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
3112F30 20603555 04031326 49F5312D 5365C66C 2D536967 6E65646D 43657274
6F66666F 6174652D 33333333 33353730 3531331E 170D3133 30323138 31323139
30431A74 DD333330 31333130 30303030 305A3031 312F302D 06035504 050D0132
35332D53 65C662D 5365C66C 65624D43 65726466 66656661 74656D69 66656661
35333333 31330820 22300006 02AA8648 86F70D01 01010500 0382010F 03080201
0A028201 010CD21 042E0780 271C5A8B 6F786CE3 E2030BB0 8F93AA0 01AEC893
0B56DC40 F37F53A3 B22C448 C44C4C97 19F2B197 051D4C12 026256CA 5163957B
DA825C78 45C7D488 31DA745C 74F3A57B 0C66DE3 0C65656F 43657274
42F5255E 41D4CF86 78B7E24C 32936A23 F74F81C7 2C4042A8 FF908B63 2F7B6560
E0F3FDE0 4E880475 34B5353E F791DD9F C2579785 D55FC92 958B9701 B38A0498
85B03F72 5EAA566 B8496C6C 0C0CP72C 79F8CBA4 00018C5 6866676F 5E0A5BC5
9E177F1D 9C1773BA 96DC339F 74922551 3CB56661 05A00769 049BCAF1 226C2D5D
76B91D7F 737B86B4 1B088E1C B71842D 44758889 265FD66C D1DEAA12 05F0AE67
8B3128BD 13510203 01003A1 53303130 0F603055 1D310101 FF040930 303010FF
301F6063 551D3204 18301680 147C873 4CC8BD1C A85558A 470C2E56 B35F4A4B
AD310D06 03515106 01460A14 7DC8734C 0CB01CAA E5558A47 0C2E56BE 53FA4BAD
300D0609 2A6488F7 F70D0101 05050030 82010100 18BC525B 26286D6C FC1582CA
5DF46D43 1DDFA8D2 D3A3342 0A09FD5C 978C157F 79426760 7C46C197 292C1EB9
3D3BA370 6ECD2C64 82C558B 05F136CD 04CA0468 DC560E01 E6A4F205 7C831ED5
367C457A D083F498 2AADA3ED 4533F433 FF676C9F D94E99FF 89040404 E38A5A5E
C483320 2C8B5962 F49999B4 49AFC53D 02D34319 93C2B54D 578E6D03 5670A9E2
F82AE545 26F1438 E82D12AB 14D4D46C 7747A9F8 B9DF7F78 54FCDC7 90974585
1B951E27 337D5721 7CA38D0F 8F84882E EB35325E 5725F572 C1E7B7D9 057C6B24
540B11B2 F887B289 A31A02EF CC134D6E BAFD67D3 65C34D4C B3C1B154 FF9D5349
477F9AB4 91537DA4 848A9F0B EC34AEDE 597966E5
quit
!
license udi pid ASR1002-HX sn JAD23030BSP
license accept end user agreement
license boot level adventerprise
no license smart enable
!
spanning-tree extend system-id
diagnostic bootup level minimal
!
!
username USERNAME privilege 15 password 0 PASSWORD
!
redundancy
mode none
!
crypto ikev2 name-mangler PSK
email username
!
crypto ikev2 authorization policy default
route set interface
croute set access-list CLOUD
!
crypto ikev2 authorization policy IXIA_AUTH_POLICY
pool IxiaPool
route set interface
Remote and Mobile Assets—Enterprise Network Integration

Appendix A—Implementing Integration with ISE

crypto ikev2 authorization policy IXIA_AUTH_POLICY2
  pool IxiaPool2
  route set interface
  !
crypto ikev2 redirect gateway init
  !
crypto ikev2 keyring field_keys
  peer SIMULATED
    identity email domain iotspdev.io
    pre-shared-key PASSWORD
  !
  !
crypto ikev2 profile Flex_IKEv2
  match fvrf any
  match identity remote email domain iotspdev.io
  identity local key-id PUBLIC_IP
  authentication remote pre-share
  authentication local pre-share
  keyring local field_keys
  dpd 250 10 on-demand
  aaa authorization user psk list FLEX name-mangler PSK password AD_PASSWORD
  aaa accounting psk FLEX
  virtual-template 1
  !
  !
crypto ikev2 reconnect key 1 active cisco12345
  !
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
  ip mtu 1400
  !
interface Port-channel1
  no ip address
  no negotiation auto
  !
interface Port-channel1.1
  !
interface Port-channel1.30
  encapsulation dot1Q 30
  ip address 10.2.0.2 255.255.0.0
  ip nat inside
  standby 30 ip 10.2.0.1
  !
interface Port-channel1.77
  encapsulation dot1Q 77
  ip address 77.77.77.2 255.255.255.0
ip nat inside
standby 77 ip 77.77.77.1
!
interface Port-channel1.251
encapsulation dot1Q 251
ip address PUBLIC_IP NETMASK
ip nat outside
ip access-group BLOCK_TELNET_SSH in
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
channel-group 1
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
channel-group 1
!
interface GigabitEthernet0/0/2
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/3
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/4
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/5
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/6
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/7
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 10.100.5.7 255.255.0.0
negotiation auto
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1400
ip nat inside
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel mode ipsec ipv4
path-mtu-discovery
ipsec 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
!
ip nat inside source list PAT-LIST interface Port-channel1.251 overload
ip forward-protocol nd
no ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 GATEWAY_IP
ip route 10.10.2.0 255.255.255.0 10.10.1.4
ip route 10.11.0.0 255.255.0.0 10.10.0.4
ip route 10.14.0.0 255.255.0.0 10.10.3.4
ip route 10.50.0.0 255.255.0.0 10.100.0.1
ip route 10.100.0.0 255.255.0.0 GigabitEthernet0
ip route vrf Mgmt-intf 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 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 any eq 22
  deny tcp any any eq telnet
ip access-list extended PAT-LIST
  permit ip 10.2.0.0 0.0.255.255 any
  permit ip 172.17.92.0 0.0.0.255 any
  permit ip 192.168.0.0 0.0.0.255 any
  permit ip 10.5.0.0 0.0.255.255 any
  permit ip 192.169.0.0 0.0.0.255 any
  permit ip 10.0.0.0 0.0.255.255 any
  permit ip 192.168.5.0 0.0.0.255 any
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 20 tries 2
radius-server deadtime 1
!
radius server ISE24
  address ipv4 ISE_IP auth-port 1645 acct-port 1646
  key PASSWORD
!
control-plane
Windows Active Directory

In this scenario, Windows Active Directory is referenced by ISE to determine if the gateway is authorized on the network. In order to do this, one must:

1. Enable a Windows Machine as an Active Directory Domain Controller.
2. Add a “group” that will contain entries for any appropriate gateways.
3. Create a “user” entry for each gateway and add it to the group.

Set Up Windows as a Domain Controller

For instructions for setting up Windows Server as a Domain Controller, refer to:

Create an AD Group and User Accounts

In order to create the requisite AD Group and User accounts:

1. Open Server Manager.
2. Select AD DS from the leftmost column, right click the server name, and select Active Directory Users and Computers.
3. Expand the domain.

4. Right click the Users folder.


6. Give the group a name, a scope, and a Security group type.
A Security group type is used to provide access to resources, while a Distribution group type is used to create e-mail distribution lists.

**Figure 16 Configure the Group**

![Configure the Group](image)

**Create Users**

1. Back in the **AD Group and User accounts** window, right-click the **Users** folder again but navigate to **New -> User** this time.
Figure 17  Add a User

2. Enter the username that the gateway will send in the authentication request (such as the gateway serial number) for the First Name and User Logon Name fields

3. Click Next.
4. Enter a password for the user. This password must match the password that will be sent in the authorization request from the HER to ISE.

   Uncheck **User must change password at next logon**.

5. Click **Next**.
6. Verify that the information is correct and select **Finish**.

7. Repeat for every user.
Add Users to Group

1. Locate and right-click the previously created group in the Active Directory Users and Computers window.

2. Select Properties.
3. Select the **Members** tab.

4. Click **Add**.
5. Enter the object names of all of the users.

Once all of the users have been added, ISE will be able to query the AD group for any username defined in the authorization request and subsequently permit or deny access.

After AD is finished being configured, CPNR must be set up in order to provide DHCP services for future tunnel connections.
Cisco Prime Network Registrar

The Cisco Prime Network Registrar is used for DHCP services to provide the gateway tunnel interface with an IP address. For the steps to install CPNR, refer to:


Once CPNR is up and running, the DHCP pool must be configured.

Configuring the DHCP Pool

The DHCP pool is going to provide the next available IP address to the gateway tunnel interface once it has been authorized to join the network. In order to create one:

1. Navigate to Design -> DHCPv4 -> Scopes.

2. Click the button to the left of the X to add a scope.
3. Enter the **Scope Name**, **Subnet**, and **Primary Subnet**.
   - The **Subnet** must match the network of the **Tunnel Source Loopback Interface** on the HER.
   - The **Primary Subnet** should be the network on which the CPNR is going to be receiving DHCP requests.

![Figure 26 Add DHCP Scope](image)

4. Make sure the mode is **Advanced** in the top right corner.
   
   This will allow for the configuration of specific DHCP options

![Figure 27 Advanced CPNR Configuration](image)

5. Select **Create New Embedded Policy** under the newly created DHCP scope.

![Figure 28 Create New Embedded Policy](image)

6. Under **DHCPv4 Options** select [3] **routers (IP address)**, enter the IP address of the HER loopback interface as the value, and select **Add Option**.
   
   This will provide the gateway tunnel interface with a default gateway pointing to the HER tunnel interface.
Remote and Mobile Assets—Enterprise Network Integration

Appendix A—Implementing Integration with ISE

Figure 29  DHCPv4 Options

<table>
<thead>
<tr>
<th>DHCPv4 Options</th>
<th>Name</th>
<th>Number</th>
<th>Legacy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>[3] routers (IP address)</td>
<td></td>
<td></td>
<td>And</td>
<td>Add Option</td>
</tr>
</tbody>
</table>

Now that both AD and CPNR are configured, it is time to configure ISE.

ISE Configuration

AD Join Point

Since AD is going to be used as the user database (instead of locally defined users), it must be added to ISE as an AD Join Point. The steps to add an AD Join Point are as follows:

1. Navigate to Administration -> Identity Management -> External Identity Sources.
2. Select Active Directory and then click Add.

Figure 30  Add an AD Join Point

3. Enter the Join Point Name (AD hostname) and the Active Directory Domain.

   This hostname must be resolvable via DNS in the given domain.

Figure 31  Provide the Name and Domain

4. Select the newly created AD Join Point under Active Directory.

   Tick the box and select Join.
5. Enter the valid AD **username** and **password** and click **OK**.

If everything worked, then the AD Join Point will successfully join and it will be time to add the HER as a Network Device.

**Network Devices and Groups**

When the authorization request is sent from the HER to ISE, ISE must first check to see if the HER is a trusted device. To do this, a corresponding Device must be created and placed in a Network Device Group. To do this, the steps to do so are as follows:

1. Navigate to **Administration > Network Device Groups**.
2. Create a new group called **FlexVPN_HUBS** and nest this under **All Device Types**.

3. Navigate to **Administration > Network Devices**.
Figure 36  Network Devices

4. Create a new Network Device.
   - Add a descriptive name for the HER.
   - Add IP address.
   - Select **Device Type** as **FlexVPN_HUBS**.
   - Tick **RADIUS Authentication Settings**.
   - Specify the **Shared Secret** as specified in the AAA configuration on the Hub.
   - Click **Save** when complete.
Authorization Profile

The Authorization Profile outlines what actions ISE should take if the Authorization Rule Condition (defined in the Policy Set section) is met. To configure the Authorization Profile:

1. Navigate to Policy -> Policy Sets -> Results.

2. Expand Authorization, select Authorization Profiles, and then Add.
3. Give the Authorization Profile a descriptive name and add the below Advanced Attribute Settings.

- cisco-av-pair = ip:interface-config=ip unnumbered TUNNEL_SOURCE_INTERFACE
- cisco-av-pair = ipsec:group-dhcp-server=CPNR_IP_ADDRESS
- cisco-av-pair = ipsec:route-set=interface
- cisco-av-pair = ipsec:route-set=access-list ACL_DEFINED_IN_HER
- cisco-av-pair = ipsec:dhcp-giaddr=HER_TUNNEL_SOURCE_IP

The Advanced Attribute Settings outline configuration that will be used in the Virtual Tunnel Interface that is created as the tunnel is forming.
4. Click **Save**.

**Policy Sets**

The policy set will define the logical flow of the authorization request. It will first check against an authentication ruleset for the HER itself to make sure that the HER is permitted. Afterwards (if the authentication is passed), an authorization ruleset will be checked against using the FlexVPN session username and password. In order to create a policy set, perform the following:

1. Navigate to **Policy** -> **Policy Set**.
2. Define a new **Policy Set** with a descriptive name, e.g., RAMA_FLEXVPN.

3. Click the arrow under “view”, expand the “Authentication Policy”, and add an authentication rule.

4. Specify the **Condition** as:

   DEVICE:Device Type EQUALS All Device Types#FlexVPN_HUBS

5. Set the Use value as the AD Joint Point.
6. Expand the Authorization Policy.


8. Specify the Condition as:
   
   RAMA_AD:ExternalGroups EQUALS rama.local/Users/buses
   
   This tells ISE to check if the user is found under the AD Group created in the earlier section.

9. Under Results, select the Authorization Profile that was created earlier.
Troubleshooting

ISE

The best place to determine the status of the flow is in ISE.

   This will display a list of all of the authorization attempts.

Figure 46   RADIUS Live Logs

2. Select the latest attempt you would like to inspect.
   This will display which step that the attempt failed at. This could include such things as:
   - Not initiating from a valid network device,
   - Not having a matching authentication/authorization ruleset,
   - Not finding the gateway in AD
   - Etc.

Figure 47   Live Log Overview
### Result

<table>
<thead>
<tr>
<th>State</th>
<th>ReauthSession:L2L44066FE95ZO2L40C99E6B1ZH11941194ZL44B4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>CACS:L2L44066FE95ZO2L40C99E6B1ZH11941194ZL44B4:RAMA-ISE/347306525/61932</td>
</tr>
<tr>
<td>cisco-av-pair</td>
<td>ip:interface-config=ip unnumbered loopback0</td>
</tr>
<tr>
<td>cisco-av-pair</td>
<td>ipsec:group-dhcp-server=10.2.5.11</td>
</tr>
<tr>
<td>cisco-av-pair</td>
<td>ipsec:route-set=interface</td>
</tr>
<tr>
<td>cisco-av-pair</td>
<td>ipsec:route-set=access-list CLOUD</td>
</tr>
<tr>
<td>cisco-av-pair</td>
<td>ipsec:dhcp-giaddr=10.5.0.1</td>
</tr>
<tr>
<td>LicenseTypes</td>
<td>Base license consumed</td>
</tr>
</tbody>
</table>
Additionally, ISE has a TCP Dump feature to allow for the capture of all packets coming in. This can then be exported as a PCAP file and inspected in Wireshark. To do so, navigate to Operations -> Troubleshoot -> Diagnostic Tools.

2. Click TCP Dump.
   - Select the ISE host.
   - Choose the Network Interface that communicates with the HER.
   - Select Format type.
If all steps have succeeded in ISE, then CPNR can be checked to determine whether or not an appropriate IP address is being leased.

**CPNR**

The steps to check the DHCP logs in CPNR are as follows:

1. Select the button at the top left of the page to open a hidden column.

2. Navigate to **Deploy -> DHCP -> DHCP Server.**

Figure 52  DHCP Server

Figure 53  CPNR Logs

Local DHCP Server
Appendix B—Scripted HER Configuration

This appendix details the configuration of the HER to allow remote gateways to authenticate and establish FlexVPN tunnels. This setup is an alternative to that described in Appendix A—Implementing Integration with ISE, page 87.

The Python script below will connect to the Kinetic GMM API and retrieve the required details for any gateways that exist in the specified Kinetic GMM organization and are configured with a site-to-site VPN. This retrieved information (such as the gateway serial number and pre-shared key) will be used to build a text configuration file that can be copied and pasted into the IOS-XE-based HER configuration. This approach is especially helpful for scenarios where large numbers of remote gateways are being managed or the script can be triggered as part of the workflow when onboarding new gateways to keep the HER configuration current.

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: ", token_resp.status_code)
    else:
        data = json.loads(token_resp.content)
        access_token = data['access_token']
        print("User Access Token: ", access_token)
        return access_token

# Build HTTP Header for Future Requests
def build_header(access_token):
    headers = {}
    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: ", gwy_list_response.status_code)
    else:
        gateways = json.loads(gwy_list_response.content)
        print("GMM Gateway Summary:" + str(gateways['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']))
        return gateways

def build_he_config(gateways, domain, psk):
    # Build HE Configuration
    print("FlexVPN Hub Configuration:" + str(gateways)"")
```
```python
print('!')
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('!')
print('crypto ikev2 keyring field_keys')
for i in range(len(gateways['gateways'])):
  print(' peer ' + str(gateways['gateways'][i]['uuid']))
  print(' identity email ' + str(gateways['gateways'][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()
```

The script also supports a help function as demonstrated below:

```
$ 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
```

The output below shows the result of running the script with the required input parameters:
Remote and Mobile Assets—Enterprise Network Integration

Appendix C—Unique FlexVPN Pre-shared Keys Using Advanced Templates

$ python3.6 gmm_gwy_status.py -u 'test@cisco.com' -p 'password' -oid 1234 -psk 'C!sc0123#' -d "iotspdev.io"
User Access Token: 23dad30abfdabble7c.268jPhWry5ado6xvis0-BoiircW6Qq_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

The text configuration file below is an example of the output of the script which can be copied and pasted into the HER. In this example, three peers are added, however the script will work for any number of gateways in the Kinetic GMM organization. The CLOUD access-list is used to define which enterprise subnets/routes are advertised over the FlexVPN tunnel to the remote gateways.

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 FTX00000001@iotspdev.io
  pre-shared-key C!sc0123#
  !
peer FTX00000002
  identity email FTX00000002@iotspdev.io
  pre-shared-key C!sc0123#
  !
peer FTX00000003
  identity email FTX00000003@iotspdev.io
  pre-shared-key C!sc0123#

Appendix C—Unique FlexVPN Pre-shared Keys Using Advanced Templates

As discussed in detail in the Zero Touch Provisioning module, Cisco Kinetic GMM offers the use of Advanced Templates to push customized configuration options (that are not otherwise exposed in the GMM UI) to the managed gateways. Included in Advanced Templates is the ability to use variables to allow GMM to fill in the bits of configuration that will be unique per gateway (such as the gateway’s WAN IP, interface name, or serial number). Another variable type is the custom variable, which allows a user to input text later which will get inserted into the configuration for the router at provisioning time. This custom variable value can either be the same for all gateways using the template or unique for each gateway.

One application of these custom variables is a case where an organization wants to deploy FlexVPN for site-to-site VPN connectivity between the managed gateways and their enterprise VPN head end. Instead of using a common preshared key for all gateways, the organization wants to be able to enter a unique PSK for each gateway to authenticate to the VPN headend. This appendix walks through the configuration and validation of this use case.

1. Define an advanced router template. This assumes that the VPN headend IP address is always the same.
2. In your base template, configure the site-to-site VPN details with IP address and a “dummy” password that will later get replaced automatically with the unique value. Note that since this “dummy” password is not configured in the head end, there is no risk that sessions will be established using this temporary password.

3. In the base template, point to the Advanced Router Template. Make sure to select “Distinct per Gateway”.
4. Once the template is defined, you can customize it per gateway with the new PSK. On the Gateway page, select (check) one gateway and click **Networking > Advanced Configuration**.
5. Click **Advanced Router Template**.
6. Fill in the unique PSK for this gateway and click **Save**.

7. Make sure the headend configuration (keyring) matches the value configured here and it should work.

    peer FTX2302Z0DB
    identity email FTX2302Z0DB@iotspdev.io
    pre-shared-key uniquePWhere

8. Confirm tunnel2 up:

    IR829_FTX2302Z0DB#show crypto ikev2 client flexvpn

    **Profile : Tunnel1**
    Current state:ACTIVE
    Peer : 34.208.182.252
    Source : Cellular1/0
    Ivrf : IP DEFAULT
    Fvrf : IP DEFAULT
    Backup group: Default
    Tunnel interface : Tunnel1
    Assigned IP address: 172.17.52.80

    **Profile : Tunnel2**
    Current state:ACTIVE
    Peer : 72.163.4.161
Source: Cellular1/0
ivrf: IP DEFAULT
fvrf: IP DEFAULT
Backup group: Default
Tunnel interface: Tunnel2
Assigned IP address: 10.5.79.215

Note: Site-to-Site VPN PSK shown under the GW's “Current Config” in GMM will still show the “REPLACEME” or dummy password, not the unique password.

### 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>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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------</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>
Remote and Mobile Assets—Edge Compute

This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: [www.cisco.com/go/rama](http://www.cisco.com/go/rama)

- **Solution Brief**—An overview of the RaMA CVD and the available modules.
- **Design and Implementation Guide (DIG)**—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- **Technology Guidance Module**—Overview of the available hardware options for IoT gateways in the RaMA solution, with recommendations on hardware platform and software features to use for common scenarios.
- **Security Module**—Describes how the RaMA solution was designed from the ground up with security in mind. Includes detailed descriptions of how the solution fits into the SAFE model, including securing the gateways, data plane, and management plane. Also includes a section on achieving PCI compliance.
- **Enterprise Network Integration Module**—Best practices for the enterprise headend focusing on resiliency, high-availability, load-balancing, and security. Includes detailed descriptions of FlexVPN and WAN redundancy mechanisms.
- **Remote Site Management Module**—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- **Fleet Management Module**—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- **Zero Touch Provisioning Module**—Use of Kinetic GMM by IT personnel for provisioning and managing Cisco Industrial Routers with a focus on secure, scalable deployment.
- **Field Deployment Module**—Use of Kinetic GMM by OT personnel for deploying Cisco Industrial Routers in the field, with minimal knowledge of the underlying networking technology required.
Remote and Mobile Assets—Edge Compute

Overview

This module includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview, page 132</td>
<td>This section provides an overview of the contents of this module.</td>
</tr>
<tr>
<td>Requirements, page 132</td>
<td>This section provides an overview of the typical customer requirements around edge computing within an IoT fabric.</td>
</tr>
<tr>
<td>Architecture, page 133</td>
<td>This section covers the proposed high level architecture of how edge computing is accomplished in the RaMA solution.</td>
</tr>
<tr>
<td>Design, page 133</td>
<td>This section provides an overview of the edge computer capabilities embedded within the Cisco Industrial Router portfolio and the Cisco I0x microservice framework. It also covers some of the key design aspects and considerations around the create of microservices applications in step-by-step procedures.</td>
</tr>
<tr>
<td>Implementation, page 140</td>
<td>This section demonstrates how to deploy and upgrade an I0x application and manage the app life-cycle using Cisco Kinetic GMM.</td>
</tr>
<tr>
<td>Glossary, page 155</td>
<td>List of relevant acronyms and initialisms.</td>
</tr>
</tbody>
</table>

Overview

This module provides an overview of the edge compute capabilities embedded within the Cisco Industrial Router portfolio and the Cisco I0x microservice framework for developing containerized applications. These containerized applications can be deployed at the edge of the IoT fabric to help extract IoT data from devices connected behind the gateway and transform that data for upstream consumption.

This module also covers how the cloud-hosted Cisco Kinetic GMM can be used to centrally deploy and manage the entire deployment life-cycle of an I0x application to edge gateways in a scalable fashion. This involves the entire process from deploying the applications, starting, stopping and restarting the application, upgrading to a later version of the application, and finally deleting the application if no longer needed.

The implementation section of the module describes the step-by-step process of developing a Docker container image encapsulating some sample code, creating an I0x deployment package, and then finally deploying the application to the edge gateway using Kinetic GMM. It then illustrates how a developer can package and deploy and updated version of the application in a seamless manner as well as monitor and log application activities within the Kinetic GMM UI.

Disclaimer: While this document describes best practices and details on deploying and utilizing I0x for customized microservices, custom microservices are neither created nor supported by Cisco. The customer assumes all responsibility and risk associated with the development and use of such custom microservices.

Requirements

- Transformation of IoT edge generated data into business outcomes
- Rapid system integration and edge application management
- Availability of an Application Development Framework
- Ability to centrally deploy and manage the entire application life-cycle
- Support for Native Docker Tooling
- Distributed edge compute
- Availability of development and test sandboxes
Remote and Mobile Assets—Edge Compute

Architecture

- Secure communications

Architecture

Figure 1  Distributed Edge Compute and IOx Microservice Application Architecture

The key design guidelines for creating edge compute solutions include:

- Devising methods of managing the information or sensor data received by the gateway via local processing and preparing it for transmission over the network backhaul.
- Enabling effective bandwidth utilization, as desired, through local processing at the edge to transform, compress, or reformat data for upstream consumption.
- Supporting real-time data processing for low-latency applications.
- Converting or adapting legacy protocols to provide the information northbound via IP-based protocols or APIs.
- Determining the location of decision making based upon data received—on the gateway device, on the local network, or at the head end.
Key Components of a Solution Using Edge Computing

Key Components enabling Edge Computing include the IoT edge gateway, the IOx framework for creating edge software, and Kinetic GMM for managing the edge applications. Each is described in more detail below.

IoT Edge Gateway Routers

IoT edge gateways are a critical component to the success of your IoT operations because they provide the ability for your IoT network to connect to local devices, applications, and ultimately to your cloud services. Cisco provides IoT gateways that also provide a layer of security to protect your IoT devices and to help prevent your IoT devices from being hacked. Cisco’s IoT gateways can also function as a standalone device, processing data directly from sensors via WiFi, wired, or serial input connections providing a battle-hardened device for the data you want to process at the edge.

There are three Cisco Industrial router models that provide Edge Compute capabilities with an ability to run IOx applications at the edge of the IoT fabric:

- The IR829 is a fleet-targeted mobile gateway that addresses most use cases for fleets. The goal is to provide an off-the-shelf solution for the widest possible number of fleet applications with the fewest number of SKUs and least amount of custom developments possible. This Fleet Gateway is a ruggedized router integrating WiFi and Cellular radios.

- The IR809 targets markets such as Distribution Automation, ATM, POS, Telemetry, Enterprise Fleet, mobile machine-to-machine (M2M), bill boards, and so forth. IR809 brings in 4G LTE capabilities to small form factor M2M routers.

- The IR1101 is like the IR829 and is a general-purpose industrial router but lacks WiFi capability. Additionally, there are essential IOx differences in the IR1101 that are important to note. This information is provided below.

These routers ship with one Cisco provided IOXVM (virtual machine which enables IOx on the platform). All IOx applications run within this virtual environment. In certain cases, a customer may decide to install a custom operating system on the platform. In this situation, IOx support ceases to exist on the platform (and for the customer).

Figure 2  IOx Framework

The Cisco IOx framework provides a powerful platform for your Ops and App Developers to easily deploy applications to your IoT gateways. Cisco IOx utilizes Docker tooling to allow your development teams to build applications in a standard format that is familiar to cloud-native application developers. The Cisco IOx application environment combines the power of the Cisco IOS and the Linux OS to provide highly secure networking. This enables you to execute IoT applications in the fog or at the edge with secure connectivity to the Cisco IOS software and get powerful services for rapid, reliable integration with IoT sensors and the cloud. Cisco IOx enables development and deployment of IoT business and control applications at the edge.

By bringing application execution capability to the source of the IoT data, customers can overcome challenges with high volumes of data and the need for automated, near-real time system responsiveness. Cisco IOX offers consistent management and hosting across network infrastructure products, including Cisco routers, switches, and compute modules. Cisco IOX allows application developers to work in the familiar Linux application environment with their choice of languages and programming models with familiar open-source development tools.
Kinetic GMM for IOx Life-Cycle Management

Building on Cisco IOx is Cisco Kinetic. Kinetic takes the best of Cisco IOx application management, adds IoT gateway management and automates/manages it for you as a cloud service allowing you to scale our operations. This provides ease of use for your Ops teams by allowing for both:

- Auto-provisioning of Cisco IoT gateway devices
- Easily connecting your gateways to your Kinetic account

Fog apps (for edge computing) are Cisco IOx applications that run on a Cisco gateway and transmit data from devices to the Cisco Kinetic cloud or other data destinations. Applications can be deployed and managed with the Cisco Kinetic Gateway Management Module (GMM).

Refer to Figure 4 for the deployment steps for an edge/fog application:

Figure 4 depicts the high-level steps involved as part of the IOx deployment life-cycle.
Remote and Mobile Assets—Edge Compute

The Edge/fog application download process is embedded in the overall management of the gateway. When a gateway is powered on, it communicates with GMM to download provisioning information and update/download Edge/Fog applications and ensure that the connected sensors are detected by the gateway. This way, a field technician can easily deploy a gateway that with minimal hands-on effort.

Beyond just the deployment of IOx applications, Cisco Kinetic GMM can be used to manage the entire life-cycle of an IOx application, including:

- Centrally deploy an IOx application to a set of edge gateways.
- Change the state of an IOx application (start/stop/restart).
- Monitor the status of IOx applications.
- Upgrade IOx application to the latest version.
- View container and application logs.
- Monitor events related to IOx application deployment.

The advantage of using Cisco Kinetic GMM is that you can now centrally deploy and manage the application on hundreds of gateways from a centralized pane of glass without having to log in or connect to each of the gateways individually. IOx applications can be deployed to a set of gateways, helping save deployment time and cost.

IOx Framework Details

The IR809/829 gateway routers ship with one Cisco provided IOXVM (virtual machine which enables IOx on the platform). All IOx applications run within this virtual environment. In certain cases, a customer may decide to install a custom operating system on the platform. In this situation, IOx support ceases to exist on the platform (and for the customer).

These routers ship with one Cisco-provided IOXVM which enables IOx on the platform. All IOx applications run within this IOXVM.

In certain cases, a customer may decide to install a custom operating system on the platform. In this situation, IOx support ceases to exist on the platform (and for the customer).

Figure 5  IOx Architecture for IR8x9

Both the IR829 and the IR809 use the Intel Rangeley Dual-Core CPU, 2GB DDR3 memory, 8MB SPI Bootflash, and 8GB (4GB usable) eMMC bulk flash.

The hypervisor is provided by LynxWorks and it runs on the bare metal hardware upon which IOS and a Guest OS (e.g., Linux) run as two separate virtual machines (VMs).

The hypervisor presents underlying hardware to virtual machines (IOS and Guest OS) as a subset of actual physical hardware. The allocation of devices to VMs is provided by a configuration to the hypervisor. The VMs access a virtual CPU, pre-configured memory regions, pre-divided flash disk storage, and other hardware devices. LynxSecure Separation Kernel v. 5.1 has been selected as a hypervisor.
Each PCI device can be owned exclusively by one VM in the hypervisor architecture. However, IOS and the Guest OS need to access some shared devices, for example eMMC flash. The solution is a Virtual Device Server (VDS), which is a separate VM that owns shared devices. IOS and Guest OS access the virtual devices emulated in hypervisor. The hypervisor and VDS then coordinate access to the shared devices. The VDS also provides communication channels between VMs using emulated Ethernet interfaces.

IOS acts as a gateway to network resources for the Linux partition, using IP and a virtual switch connection provided to the hypervisor. IOS and Linux each operate as a Guest OS of the hypervisor.

The network path from IOXVM to IOS is available via an emulated Ethernet link between them. Either IPv4 or IPv6 protocol can be run on the Ethernet link.

The IOXVM runs CAF and other IOx infrastructure elements on the host Linux and hosts all the LXC applications.

**Table 1  IR8x9 Platforms–Key Resource Requirements**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IOS Image</strong></td>
<td>The minimum IOS version required for IOx support is 15.6(1)T1.</td>
</tr>
<tr>
<td><strong>Application Types Supported</strong></td>
<td>IR800 platforms support PaaS, LXC, and Docker type applications.</td>
</tr>
<tr>
<td><strong>Application Resources Limit</strong></td>
<td>IR800 platforms have a total of 732 units of CPU and 767 MB of memory for applications. Docker type applications can have maximum of 42 layers per application. At any time, IOx supports hosting 100 layers in total for all Docker applications installed on the device.</td>
</tr>
<tr>
<td><strong>Application Networking</strong></td>
<td>IR8x9 platforms support NAT and bridge mode for application networking.</td>
</tr>
<tr>
<td><strong>Device Resources</strong></td>
<td>There are two serial ports (async0 and async1) available for applications. USB storage and USB serial capabilities for application are supported on this platform.</td>
</tr>
<tr>
<td><strong>Application Security</strong></td>
<td>IR8x9 platforms support application signature verification, which is enabled by default.</td>
</tr>
<tr>
<td><strong>IOx Services</strong></td>
<td>IOx services is enabled for IR800 platforms. IOx services like GPS, Motion, Host Device Management, and more are supported out-of-the-box.</td>
</tr>
</tbody>
</table>

**Note:** IOx developer documentation is available on Cisco DEVNET at: [https://developer.cisco.com/site/iox/](https://developer.cisco.com/site/iox/)

Self-provisioning developer sandboxes are available for training and testing. Developer sample code and how-to guides are also available.

IOx services sample applications and tutorials: [https://github.com/CiscoIOx/iox-services-samples/](https://github.com/CiscoIOx/iox-services-samples/)

IOx SDE—IOx SDE is an Ubuntu VM (14.04) with all the tools (Docker, ioxclient) required to build an IOx application package pre-installed. Download and import it as a VM to get started.

Login Credentials for IOx SDE VM:

Username: root

Password: ioxsde

**Note:** Use the NAT mode if VM does not obtain the IP address in bridge mode.

Download SDE V1.7.0: [https://developer.cisco.com/files/iox-sde.ova](https://developer.cisco.com/files/iox-sde.ova)

The IR1101 modular gateway also supports hosting IOx applications. However, the IOx architecture for the IR1101 differs from other Cisco platforms that use the hypervisor approach. IOx runs as a process on the IR1101 versus as a virtual machine on others. Additionally, the only type of container supported on the IR1101 is the LXC container.
Remote and Mobile Assets—Edge Compute  

Design  

Note: The IOx application build procedure for the IR1101 is slightly different due to it having an ARM 64-bit processor. So certain steps must be followed using the Cisco IOx SDE to use a virtualization layer on an x86_64-bit build machine that enables an ARM 64-bit environment to run on that machine. By emulating an ARM 64-bit CPU in this way, you can cross compile code for an ARM 64-bit IR1101 target device without explicitly using a cross compiler. For details refer to: https://developer.cisco.com/docs/iox/#!phase-2-building-an-iox-application-for-the-ir1101/building-an-iox-application-for-the-ir1101

Note: The IOx platform support page is located at: https://developer.cisco.com/docs/iox/#!platform-support-matrix/platform-support-matrix

IOx Application Resource Profile  

IOx nodes may have different CPU architectures, so it becomes very complex to characterize an application’s performance or requirements on each of them. IOx attempts to bring consistency and uniformity by using the notion of resource profiles. A resource profile encapsulates a set of resources (CPU, memory, etc.) under a unique name in a consistent fashion across all Cisco IOx platforms.

The intent of resource profiles is to allow developers to obtain some level of consistency when they test their applications on one platform and want to deploy the same applications on other platforms. Currently, only CPU and memory are characterized under a resource profile.

Resource Profile Definitions  

Currently, the pre-defined resource profiles in Table 2 are provided. However, the exact set of profiles supported on a specific platform is a function of the available resources on that platform. Also, if one of the pre-defined resource profiles do not meet your requirements, you can always define your own custom profile based on the resources required for your application.

Table 2 Pre-defined Resource Profiles

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Memory(mb)</th>
<th>CPU (units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.tiny</td>
<td>32</td>
<td>100</td>
</tr>
<tr>
<td>c1.small</td>
<td>64</td>
<td>200</td>
</tr>
<tr>
<td>c1.medium</td>
<td>128</td>
<td>400</td>
</tr>
<tr>
<td>c1.large</td>
<td>256</td>
<td>600</td>
</tr>
<tr>
<td>c1.xlarge</td>
<td>512</td>
<td>1200</td>
</tr>
</tbody>
</table>

Memory assignment is platform agnostic and can be directly assigned based on the application requirements irrespective of the platform. However CPU resources are highly platform dependent and performance may vary based on the underlying CPU architecture.

To abstract these disparate characteristics to application developers and provide a uniform and consistent view, CPU resources are expressed in the form of “units”. This means an app with “x” CPU units would have similar performance on all Cisco supported heterogeneous platforms.

The CPU unit values for a platform are obtained by executing standard benchmarking tools on that platform and assigning a unit value based on their relative score when compared against a standard base platform.

To get a relative idea of what those units could mean in comparison to a standard CPU, here is a sample comparison with a generic x86 Intel platform:
Based on the benchmarking results, an x86-based 64 bit Intel Xeon processor with one core of CPU @ 2GHz will have 10000 CPU units. Based on this value developers can extrapolate and test an application in their devnet sandbox environment based on the same CPU characteristics and check the CPU units required for an app.

A note about resource bounds:

- The CPU units allocated to an app are the minimum guaranteed. This means that at any given point in time depending upon the number of applications running, an app under consideration will get the guaranteed CPU units and may even get more than that if there is no other contention for CPU units.

- Memory, however, is a **hard limit**. That is, at no point in time will the application get more memory than what is defined. Going beyond this limit typically results in a KILL signal to the application.

### Table 3 Resources Available on Devices

<table>
<thead>
<tr>
<th>Platform</th>
<th>CPU Architecture</th>
<th>CPU (Units)</th>
<th>Memory (MB)</th>
<th>Storage (MB)</th>
<th>Supported Application Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR829/IR809</td>
<td>Intel 64 bit (x86_64)</td>
<td>732</td>
<td>767</td>
<td>512-1800</td>
<td>PaaS, LXC, Docker</td>
</tr>
<tr>
<td>IR1101</td>
<td>ARM 64-bit (aarch64)</td>
<td>1000</td>
<td>862MB</td>
<td>512MB</td>
<td>LXC, Docker</td>
</tr>
</tbody>
</table>

### IOx Application Package

#### Anatomy of an Application Package

An IOx application package consists of:

- One package descriptor file named package.yaml, which should be in the root of the package.

- Zero or one application configuration file named package_config.ini. If present, it should be in the root of the package.

- Zero or one application manifest named package.mf. If present, it should be in the root of the package.

- Zero or one certificate containing signing information named package.cert. If present, it should be in the root of the package.

- One tar.gz envelope containing application or service artifacts with the name artifacts.tar.gz. These artifacts may be binaries, application code, application libraries, virtual disks, rootfs, etc. More details are provided in the following sections.

#### Package Format

An IOx application package should be packaged in one of the following file formats: “tar” or “tar.gz”.

#### Package Descriptor File

The contents of this file capture application and service metadata, requirements, etc., in a YAML format. It should be named “package.yaml”. The specifications of this file are covered in [https://developer.cisco.com/docs/iox/#:~:text=package,-descriptor%2Fiox-package-descriptor](https://developer.cisco.com/docs/iox/#:~:text=package,-descriptor%2Fiox-package-descriptor)
Implementation

Package Configuration File

In order to bootstrap applications or services present in the package, IOx framework supports externalizing this content into a separate .ini file and provides mechanisms to edit and update the contents of this file during the provisioning of the application. This file contains sections with key, value pairs adhering to .ini file format. The name of the file if present should be package_config.ini. The administrative tools provide mechanisms to modify this file with the correct values during the installation process so that the application can be bootstrapped with the correct values.

Application Artifacts

All app artifacts are maintained in its own tarball, which offers a cleaner separation of application artifacts. This inner envelope will always be a tar.gz and is named artifacts.tar.gz. This will typically be generated by tooling (ioxclient, SDK, etc.).

Implementation

Building a Dockerized IOx NodeJS Application and Deploying it Using Kinetic GMM

This section describes how to use Docker tooling to create an IOx application. Specifically, it shows how to create a Docker image to run a simple Node.js-based HTTP server and create an IOx application from it.

Figure 6 Using Docker Tools to Generate IOx Applications

Using docker tools to generate IOx applications

Installing Docker Tools and Images

The development machine should have the following installed:

- ioxclient (version > 1.4.0)
  ioxclient download: https://developer.cisco.com/docs/iox/#iox-resource-downloads
- Docker >= version 1.12 (version 1.26 preferred)
  Install Docker for Mac: https://docs.docker.com/docker-for-mac/install/
The sample application code is maintained at: https://github.com/CiscoIOx/docker-nodejs.git

Clone this sample code and use branch master.

This is a simple Node.js-based HTTP server that performs the following:

- Sets up signal handlers to shutdown gracefully.
- Inspects CAF_APP_LOG_DIR environment variable and sets up logging to a file accordingly.
- Starts HTTP server on port 8000.
- Logs the source of request and responds with "Hello World!".

Creating the Docker Image

This section describes how to create a Docker image with the above application in it. The process involves using alpine:3.3 as the base image, installing Node.js, and setting up the application.

The following Dockerfile accomplishes these tasks:

FROM alpine:3.3

RUN apk add --update nodejs
COPY server.js /server.js

EXPOSE 8000
CMD ["node", "/server.js"]
Remote and Mobile Assets—Edge Compute

Implementation

**Figure 10  Building the Docker Image**

```
SAZAD-M-C48Q:docker-nodejs Sameer$ docker build -t samplenode:1.0
Sending build context to Docker daemon 65.02kB
Step 1/5 : FROM alpine:3.3
 ---> 867ca1bf801a
Step 2/5 : RUN apk add --update nodejs
 ---> Running in 322bcefe5627
fetch http://dl-cdn.alpinelinux.org/alpine/v3.3/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.3/community/x86_64/APKINDEX.tar.gz
(1/4) Installing libgcc (5.3.0-r0)
(2/4) Installing libstdc++ (5.3.0-r0)
(3/4) Installing libuv (1.7.5-r0)
(4/4) Installing nodejs (4.3.2-r1)
Executing busybox-1.24.2-r2.trigger
OK: 29 MB in 15 packages
Removing intermediate container 322bcefe5627
 ---> 830723b68aa
Step 3/5 : COPY server.js /server.js
 ---> afa9ad21dc99
Step 4/5 : EXPOSE 8000
 ---> Running in 684fcdb49a5
Removing intermediate container 684fcdb49a5
 ---> 1f4c8b8b1e38
Step 5/5 : CMD ["node", "/server.js"]
 ---> Running in 7090b44b042
Removing intermediate container 7090b44b042
 ---> ebba2d5aea4c
Successfully built ebba2d5aea4c
Successfully tagged samplenode:1.0
```

**Figure 11  Viewing the Docker Image**

```
SAZAD-M-C48Q:docker-nodejs Sameer$ docker images
REPOSITORY               TAG               IMAGE ID             CREATED              SIZE
samplenode               1.0               ebbab2d5aea4c        7 seconds ago        24.6MB
```

Run the image locally and test to ensure it is functioning correctly.

**Figure 12  Verifying the Docker Image Locally on the Development Server**

```
SAZAD-M-C48Q:docker-nodejs Sameer$ docker run -it -p 8000:8000 samplenode:1.0
Setting up logging to file server.log
Server running at http://0.0.0.0:8000/
Request from 172.17.0.1
Response sent..
Request from 172.17.0.1
Response sent..
```

If the server sends a response to an incoming request, then the Docker image and the application should be working correctly.

**Writing Package Descriptor File**

Once the Docker image has been created, the developer needs to write a package descriptor file specifying requirements for the application. Here is a sample package.yaml file:

```
descriptor-schema-version: "2.2"

info:
  name: SampleNodeApp
```
Remote and Mobile Assets—Edge Compute

Implementation

description: "Simple Docker Style app that runs a nodejs server"
version: "1.0"
author-link: "http://www.cisco.com"
author-name: "Cisco Systems"

app:
  # Indicate app type (vm, paas, lxc etc.,)
cpuarch: "x86_64"
type: docker
resources:
  profile: c1.small
  network:
    -
      interface-name: eth0
      ports:
        tcp: [8000]

# Specify runtime and startup
startup:
  rootfs: rootfs.tar
  target: ["node", "/server.js"]

The following are important to note for compatibility:

- Descriptor schema version is 2.2, which is the minimum version that supports Docker style apps.
- Note that the cpuarch is x86_64. Alpine-based apps can only run on x86_64 bit machines.
- App type is docker.
- The required port (8000) to be opened is specified under network->ports.
- rootfs.tar is the name of the file containing the Docker image (output of Docker save command). More details are provided in the following sections.
- Command to be run when starting up the app is ["node", "/server.js"]. Note that server.js was copied to "/" of rootfs.

Creating an IOx Application Package

Once the required Docker image (samplenode:1.0) and package.yaml are created, create an IOx application package from these artifacts. ioxclient (>= 1.4.0) provides a convenience command that generates an IOx application package from a Docker image and package.yaml file.
Figure 13  Creating the IOx Application Package

SAZAD-M-C480:docker-nodejs Sameer$ ioxclient docker package samplenode:1.0
Current active profile: 889-1
Command Name: docker-package
Using the package descriptor file in the project dir
Validating descriptor file package.yaml with package schema definitions
Parsing descriptor file.. Found schema version 2.2
Loading schema file for version 2.2
Validating package descriptor file..
File package.yaml is valid under schema version 2.2
Generating IOx package of type docker with rootfs consisting of layers
Replacing symbolically linked layers in docker rootfs, if any
No symbolically linked layers found in rootfs. No changes made in rootfs
Removing emulation layers in docker rootfs, if any
The docker image is better left in its pristine state
Updated package metadata file: /Users/Sameer/docker-nodejs/.package.metadata
No rsa key and/or certificate files provided to sign the package

Generating the envelope package
Checking if package descriptor file is present..
Skipping descriptor schema validation..
Created Staging directory at: /var/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/693267774
Copying contents to staging directory
Creating an inner envelope for application artifacts
Including rootfs.tar
Generated /var/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/693267774/artifacts.tar.gz
Calculating SHA1 checksum for package contents..
Parsing Package Metadata file: /private/var/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/693267774/.package.metadata
Updated package metadata file: /private/var/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/693267774/.package.metadata
Root Directory: /private/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/693267774
Output file: /var/folders/jp/49h_w8vd1rb25lps0f1pbc0000g0/T/001268101
Path: .package.metadata
SHA1: 53e8ff9f911dd88384bd390e21534672528ba13d17
Path: artifacts.tar.gz
SHA1: 11cc365eb2a53d3627a1168c14a07f1b2b86cd9
Path: envelope_package.tar.gz
SHA1: b95eac38d324732d623458ce3c580d41cf3f314
Path: package.yaml
SHA1: b528e357860e8253da12646a45723e95e80ef9d8
Generated package manifest at package.manifest
Generating IOx Package..
Package docker image samplenode:1.0 at /Users/Sameer/docker-nodejs/package.tar

The package.tar file is an IOx application package that can be used to deploy on an IOx platform.

Note: The package.yaml uses rootfs.tar as the name of startup->rootfs. This is essential, since ioxclient saves the Docker image with the name roots.tar.

Deploying the IOx Application to the Gateway using Cisco Kinetic GMM

To deploy the IOx application to the gateway, follow these steps:

1. Upload the IOX Application tar file onto Kinetic GMM.

   Log in to the Kinetic GMM UI using your credentials. Click Applications -> Add Application. Select the package.tar file created above. Click Import.
2. Verify that the upload was successful.

Once the upload is successful, the application should show in the Available state under the **Applications** tab.

3. Install the application onto a gateway.

- Select the SampleNodeApp application and click **Install**. In the pop-up window, select the appropriate application resource profile. In this case, the c1.small profile providing 200 CPU units and 64 MB RAM should be sufficient.
- Select the gateway or gateways on which you want this application to be installed from the drop-down menu.
- Leave the interface Name as default “eth0”.
- For the network name, select **IOx-nat0** since access to the Node.js application from outside is required. Internally, the Node.js application listens on port 8000. Externally map this to the desired port. In the example below, it is mapped it to an external port of 8000. Hence the Node.js application can also be accessed on port 8000 externally.

**Note:** For more information about IOx application networking, refer to: [https://developer.cisco.com/docs/iox/#!application-networking/application-networking](https://developer.cisco.com/docs/iox/#!application-networking/application-networking)

- Click **Install** to begin installation of the IOx application onto the selected gateway(s). In the example below, a single gateway is selected on which to install this application.
4. Monitor the deployment.

Once you click Install, you can navigate to the Instances tab and see the application state and status as “Deploying”.

In a few minutes you should see your application in the “Running” state. It will also display a corresponding IP address/port combination on which the application can be externally accessed.

A similar application status can be viewed under the Gateways tab by clicking the appropriate gateway on which the application has been installed and navigating to Apps. You can also view the application state in the Summary tab.
5. Viewing the Gateway Event Log.

In case of any deployment errors, you can view the logs on the **Event Log** tab.

6. Externally accessing the application.

One way to access the Node.JS IOx application is to VPN into the router using the Kinetic GMM management tunnel and access the application on the specified IP address and port.

In order to VPN to the router, navigate to the **Gateways** tab, select the gateway in question, and click **VPN**.

A pop-up window displays the requisite information needed to connect to the gateway using the Cisco AnyConnect VPN application. You need to enter your credentials to view the decrypted password.
Open up your AnyConnect Client and connect to the gateway using a secure VPN tunnel.

Once connected, open a web browser and connect to the gateway on the IP address and port specified for the IOx application that was deployed above. You should see the message “Hello World!”
Figure 24  Verifying IOx Application Accessibility

Hello World!

Note: In a similar way, you should be able to access the IOx application from your enterprise if you have configured Enterprise Network Integration as part of your deployment. Refer to the Enterprise Network Integration module for more details.

7. Viewing Application and Container logs.

Navigate to the **Apps** tab for the gateway on which the IOx application is deployed and click the application. Expand the **Application Logs** tab by clicking the + (plus) icon.
Remote and Mobile Assets—Edge Compute

Implementation

8. Building an updated version of the IOx application.

You can modify the application so that it responds with “Hello World! Welcome to my IOx Application” instead of just “Hello World!”. Do this by modifying the “response.end” line in the server.js file.

```javascript
// Configure our HTTP server to respond with Hello World to all requests.
var server = http.createServer(function (request, response) {
    console.log("Request from " + request.headers["x-forwarded-for"] || request.connection.remoteAddress)
    response.writeHead(200, {"Content-Type": "text/plain"});
    response.end("Hello World! Welcome to my IOx Application\n"客运 signs text.sent.");
});
```

Create a new Docker image with a version tag of, for example, “2.0”.

Figure 25  Inspecting Application and Container Logs

Figure 26  Making Modifications to the IOx Application Code
Remote and Mobile Assets—Edge Compute

Implementation

**Figure 27 Building Docker Image with Updated Code**

```bash
SAZAD-M-C48Q:docker-nodejs Sameers docker build -t samplenode:2.0 .
Sending build context to Docker daemon 9.38MB
Step 1/5 : FROM alpine:3.3
  ---> a6fc16bfa81a
Step 2/5 : RUN apk add --update nodejs
  ---> Using cache
  ---> 836073b6b0aa
Step 3/5 : COPY server.js /server.js
  ---> ff9474067b00
Step 4/5 : EXPOSE 8000
  ---> Running in 41a1cd81ef67
Removing intermediate container 41a1cd81ef67
  ---> a3dd8959de4a
Step 5/5 : CMD ["node", "/server.js"]
  ---> Running in e6baa1eb2038
Removing intermediate container e6baa1eb2038
  ---> a07d79f697d7
Successfully built a07d79f697d7
Successfully tagged samplenode:2.0
SAZAD-M-C48Q:docker-nodejs Sameers

<table>
<thead>
<tr>
<th>REPOSITORY</th>
<th>TAG</th>
<th>IMAGE ID</th>
<th>CREATED</th>
<th>SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.0</td>
<td>a07d79f697d7</td>
<td>5 seconds ago</td>
<td>24.6MB</td>
</tr>
<tr>
<td>samplenode</td>
<td>1.0</td>
<td>ebba2d5ae4c</td>
<td>20 hours ago</td>
<td>24.6MB</td>
</tr>
</tbody>
</table>
```

Change the application version number in the package.yaml file to "2.0".

**Figure 28 Updating Version in package.yaml**

```yaml
descraper-schema-version: "2.2"

info:
  name: SampleNodeApp
  description: "Simple Docker Style app that runs a nodejs server"
  version: "2.0"
  author-link: "http://www.cisco.com"
  author-name: "Cisco Systems"
```

Build an updated version of the package.tar file with the updated version of the application. Make sure to use the updated tag of "2.0" for the Docker image.
There is now an updated version of the package.tar file based on the updated Docker image of samplenode:2.0.

9. Upgrading the deployed application to version 2.0 using Kinetic GMM.

Navigate to **Applications** and click the application you want to upgrade.
Figure 30  Upgrading to the Newer Version of the IOx Application onto Kinetic GMM

Click the **Upgrade** button and you see a pop-up screen where you can upload the updated version of the package.tar file that was built in the previous step. You see a small warning at the bottom of the pop-up screen indicating that all of the IOx applications will be upgraded to the newer version on all applicable gateways. Check the box **I understand the risks. Proceed with editing** and click **Upgrade**.

Figure 31  Uploading Updated IOx Application onto Kinetic GMM

Once the upgrade is successful, the application version is updated to “2.0”.

Figure 32  Verifying Updated Version of IOx Application
It is also configuring the updated version of the IOx application on any associated gateways.

**Figure 33  Gateway Being Updated with Newer Version of IOx Application**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sam-829-LTE</td>
<td>Configuring</td>
</tr>
</tbody>
</table>

Once version 2.0 of the application is rolled out to all the associated gateways, AnyConnect VPN to any one of them and verify that the updated version of the application is running.

**Figure 34  Verifying Newer Version of IOx Application Successfully Running**

Hello World! Welcome to my IOx Application

10. Stopping the application.

To stop the application, click the check box next to the application and click **Stop App**.

**Figure 35  Stopping IOx Application**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Status</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SampleNodeApp</td>
<td>Running</td>
<td>Stopping</td>
<td>10.9.130.2</td>
<td>tcp 8000</td>
</tr>
</tbody>
</table>

**Figure 36  Verifying IOx Application in Stopped State**

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SampleNodeApp</td>
<td>Stopped</td>
</tr>
</tbody>
</table>

In a similar manner you can click the checkbox next to the application and click **Start App** to start the application.

11. Uninstalling the application.

To uninstall the application, click the check box next to the application and click **Uninstall**. A pop-up screen is displayed asking you to confirm that you really want to uninstall the application. You can confirm by clicking the **Delete** button. You see the status message “Removing” and within a short time you will see that the application has been uninstalled from your gateway.
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>
</tbody>
</table>

Figure 37  Uninstalling an IOx Application on a Gateway

Are you sure you want to uninstall this application?

Delete  Cancel

Figure 38  Confirming Deletion of IOx Application from a Gateway

Figure 39  Verifying that IOx Application Being Removed from the Gateway
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------</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>
Remote and Mobile Assets—Field Deployment

This module is part of the larger Remote and Mobile Assets (RaMA) Cisco Validated Design (CVD). Refer to the other modules for additional details about certain aspects of the architecture that are touched on in this module. All of the RaMA CVD modules are available at: www.cisco.com/go/rama

- **Solution Brief**—An overview of the RaMA CVD and the available modules.
- **Design and Implementation Guide (DIG)**—Overall document for architecture, design, and best practice recommendations for remote and mobile asset deployments.
- **Technology Guidance Module**—Overview of the available hardware options for IoT gateways in the RaMA solution, with recommendations on hardware platform and software features to use for common scenarios.
- **Security Module**—Describes how the RaMA solution was designed from the ground up with security in mind. Includes detailed descriptions of how the solution fits into the SAFE model, including securing the gateways, data plane, and management plane. Also includes a section on achieving PCI compliance.
- **Enterprise Network Integration Module**—Best practices for the enterprise headend focusing on resiliency, high-availability, load-balancing, and security. Includes detailed descriptions of FlexVPN and WAN redundancy mechanisms.
- **Remote Site Management Module**—Best practices for remote site connectivity, covering the use of the full range of Cisco Industrial Routers (IR 807, IR 809, IR829, IR 1101) as the managed gateway, providing wired and cellular connectivity for southbound devices as well as numerous northbound interfaces. This module also covers best practices for inbound connectivity for devices behind the gateway including isolation of management and data planes and whitelisting of applications and devices.
- **Fleet Management Module**—Architecture for mobile applications in which the IR829 acts as the managed gateway and provides wired and wireless connectivity for southbound devices, as well as numerous northbound interfaces (LTE, Wireless Workgroup Bridge, GPS). Use of edge compute in the form of Cisco IOX is also included.
- **Zero Touch Provisioning Module**—Use of Kinetic GMM by IT personnel for provisioning and managing Cisco Industrial Routers with a focus on secure, scalable deployment.
- **Edge Compute Module**—Overview of the edge compute capabilities in Cisco Industrial Routers in the form of IOx. Includes implementation examples for deploying Dockerized applications.
Overview

This module includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview, page 160</td>
<td>Summary of how field personnel can quickly and easily deploy the RaMA solution.</td>
</tr>
<tr>
<td>Requirements, page 160</td>
<td>Requirements for the Field Deployment module.</td>
</tr>
<tr>
<td>Architecture, page 161</td>
<td>Highlights to the key aspects of the Field Deployment architecture.</td>
</tr>
<tr>
<td>Design, page 161</td>
<td>Detailed instructions on how to deploy the RaMA solution using Operational Technology (OT) or non-IT personnel.</td>
</tr>
<tr>
<td>Best Practices, page 175</td>
<td>Field Deployment bests practices, tips, and responses to frequently asked questions.</td>
</tr>
<tr>
<td>Glossary, page 26</td>
<td>List of relevant acronyms and initialisms.</td>
</tr>
</tbody>
</table>

Overview

The RaMA solution takes advantage of the flexibility, security, and power of industry-leading Cisco routers while simplifying deployment so that IT personnel are not needed to deploy hundreds to thousands of gateways. This module guides field operations staff on how to use simple tools—rather than complex IT tools—to deploy these gateways.

The RaMA solution leverages powerful management tools such as the Cisco Kinetic Gateway Management Module (GMM) to apply IT and security policies to the gateway, yet provides a simple and easy-to-use tool to deploy gateways in the field.

Requirements

Field deployment requirements for RaMA include:

- Support for all Cisco Industrialized gateways such as the IR807, IR809, IR829, and the IR1101
- Simple web-based tools to provision and deploy gateways
- Mobile app (Android, IOS) based
- Support the ability to download complex routing and applications
- Support the ability to manage SIM cards including the abilities to:
  - Enable and disable SIMs
  - Set and modify rate plans
  - Set and modify data limits
- Support for public and private Access Point Network (APN)
- Ability to monitor the health, status, and location of gateways
- Ability to track LTE/3G cellular usage
- Ability to do remote diagnostics on gateways to determine root cause of problems
- Ability to de-provision gateways so they can be used in future projects
- Ability to complete the provisioning process using a mobile phone without the need for a computer
Architecture

Figure 1 illustrates key aspect of the RaMA Field Deployment architecture.

**Figure 1  RaMA Field Deployment Architecture**

The Field Deployment architecture includes the following components:

- Cisco IR gateways such as IR807, IR809, IR829, and IR1101
- Kinetic Cloud Gateway Management
- Apple IOS- or Android-based mobile application

The architecture leverages two cloud-based tools from Cisco, Control Center and Kinetic Gateway Management. All SIM and gateway management traffic is encrypted between the managed devices and the cloud-based tools.

Design

A key benefit of the RaMA 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 bulk gateway deployments across geographically-dispersed locations. This section describes the process from a field operator perspective, without delving too deeply into technical details.

Deploying Gateways in the Field

By following the steps below, field users can deploy a new Cisco Industrial Router into production in a few minutes.
1. Install the gateway and accessories.

The Technology Guidance module 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:**

- **IR1101:**

2. Verify the SIM card(s).

The Zero Touch Provisioning module 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 zero touch deployment (ZTD).**

3. Claim the gateway.

Claiming a gateway will complete the process to provision it based on the configured template and make it 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 Kinetic GMM Mobile App to Claim the Gateway**

Follow these steps to claim a gateway with the Kinetic GMM Mobile Application:

1. Download the Kinetic 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 Kinetic 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.

1. Use the Mobile app to scan the barcode on the router, which starts the claiming process.

   For information on locating your serial # barcode, refer to:
   https://developer.cisco.com/docs/kinetic/#!gateway-serial-location

2. Select the Type of Gateway, then click **Next**.
Remote and Mobile Assets—Field Deployment

Design

3. Select from a 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.

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.

**Figure 6   Web UI**

The same four steps are used to claim a gateway with the Kinetic GMM Web Application:

1. Log into the Kinetic 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 to the following URL using your Kinetic 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.

1. Navigate to the Claim Gateway screen.

   Once successfully logged into the Kinetic GMM web portal, click **Gateway** on the left and then select **Gateways**.
2. Next, select **Claim Gateway**.

3. Enter the Gateway information.

   For more information on locating your serial number barcode, see: [https://developer.cisco.com/docs/kinetic/#!gateway-serial-location](https://developer.cisco.com/docs/kinetic/#!gateway-serial-location)

   The claim gateway screen will provide a choice of gateway models (IR807, IR809, or IR829). The address information is optional. Once selected, click **Next**.
4. Select from the 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**.
5. 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, Kinetic 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)
- 1101—FastEthernet (FE1)

Ensure the 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 gateway in a few minutes.
Remote and Mobile Assets—Field Deployment

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


**Figure 12 Offboarding/Removing a Gateway**

1. **Deactivate the Gateway in Kinetic 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 Kinetic GMM. The SIM can be reactivated later through Control Center.

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 RaMA solution offers a number of tools for non-IT users in the field to use during monitoring and troubleshooting, which greatly reduces IT support requirements.
Monitoring the Gateway

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

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

Gateway Status

Figure 14 provides an overall view of the key information available through the Kinetic GMM console, including location and status of the gateways. This screen is available when users click Dashboard on the Kinetic GMM console.

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 the GMM guide:

https://developer.cisco.com/docs/kinetic/#!overview/overview
For more information on GPS tracking and Geofencing, refer to:

Reports

Kinetic GMM provides a simple reporting tool to track cellular and gateway inventory. To access these reports, users log into the Kinetic GMM portal and click **Tools -> Reports**.
Users can then select the type of report required (Inventory or Cellular Usage) and specify required information, recurrence, and the report name.

**Figure 17  Report Selection**

A CSV file of the report can be downloaded by clicking the red CSV button.

**Figure 18  Download CSV File of Report**

For more information on reports, refer to: [https://developer.cisco.com/docs/kinetic/#!view-reports](https://developer.cisco.com/docs/kinetic/#!view-reports)

**Kinetic GMM Alerts**

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

- SIM removal
Remote and Mobile Assets—Field Deployment

Design

- Geofencing
- Gateway rebooted
- Gateway Health up/down
- VPN Down
- Work Group Bridge Down
- Change in Gateway template

Setting up an alert is simple. Users click **Tools -> Alerts** on their Kinetic GMM Dashboard.

**Figure 19  Setting up an Alert**

When **Add Alerts** is clicked, Kinetic 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.
Remote and Mobile Assets—Field Deployment

Best Practices

Figure 20  Kinetic GMM Prompt for Alert

Gateway Logs

Gateway logs can be accessed through the screen in Figure 21.

Figure 21  Accessing Gateway Logs

For more information on creating alerts, refer to:

https://developer.cisco.com/docs/kinetic/#create-alerts

Gateway Logs

Gateway logs can be accessed through the screen in Figure 21.

For additional information on gateway logs, refer to:


Best Practices

Troubleshooting the Gateway

Common Gateway Issues

- Stuck in Registering for more than 10 minutes—This usually indicates that the gateway is not able to contact Cisco Kinetic.
Remote and Mobile Assets—Field Deployment

Best Practices

- For cellular gateways, ensure that a SIM card was inserted and has valid data plan.
- If using Ethernet gateways, verify that the required network ports are open and that there are no firewalls blocking the gateway from reaching the internet.

**Stuck in the In Progress state for more than 10 minutes:**
- 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 \(\rightarrow\) 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 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 \(\rightarrow\) 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 entry like “Gateway was configured using configuration xyz”.
- 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 head end router:**
- 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 entry like “Gateway was configured using configuration xyz”.

176
Remote and Mobile Assets—Field Deployment

Best Practices

- 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 head end router is correct and that it allows the gateways to establish tunnels with the provided configuration.

Note: There is a known issue 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 minutes to update after it is successfully enabled.

- Work Group Bridge (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 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 entry such as “Gateway was configured using configuration xyz”.
  - Delete and reclaim the gateway with the correct configuration, if required.
  - If Work Group Bridge (WGB) is also enabled on the gateway, then Wi-Fi works only on the 2.4 GHz radio.

Note: 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)
Gateway Diagnostics

For additional information on gateway logs, refer to: https://developer.cisco.com/docs/kinetic/#!gateway-status-and-logs-gateway-status-and-logs

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

Figure 22 Gateway Diagnostics

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).

Installation Best Practices

General Considerations

Before starting, plan the installation carefully so it will meet the following requirements:

- The installation must be safe for the operator and passengers within the vehicle.
Remote and Mobile Assets—Field Deployment

Best Practices

- The installation allows for convenient access by the operator, as applicable (i.e., the Ethernet ports, console cable, sim cards, ability to view LEDs).
- The mobile radio is mounted in a location assuring the vehicle occupants’ safety and out of the way of passengers and auto mechanics.
- The equipment is installed away from the airbag deployment areas.
- The equipment is protected from water damage.
- The installation is neat and allows easy service access.

Before the starting the installation, it is imperative to discuss with the customer the exact location in the vehicle where equipment is going to be installed. This will prevent hours of rework and reinstallation.

The test vehicle has the router and Raspberry Pi installed so it is behind the rear seat of the GMC Canyon truck. It is accessible as the rear seat folds down to allow full access to ports and antenna connections.

Figure 23  Test Vehicle Installation—1
Specific Considerations

Power Source Location and Considerations

- Some vehicles operate on 24 VDC, so it is important that the location chosen is a 12 VDC source. If a 12 VDC source is not available, a converter will need to be installed.

- Ensure that the location chosen is a main power source and will allow the addition of added terminals.

- If an auxiliary fuse block is going to be used, ensure that the location chosen for the block will guard against possible short circuits (see Figure 25).
Some vehicles, trucks in particular, will have studs on the firewall that may be used to pass power without the need for a through hole. These can be used only if verified that they are not used to connect data cables or wires.

**Ignition Sense Location and Considerations**
- Chose an ignition sense that will not interfere with the safety-related systems of the vehicle.
- The ignition sense wire (white or blue wire) connection determines how or when power is applied to the mobile router. The white wire is sometimes referred to as the “white ignition switch wire” or the “ignition sense input wire”. Regardless of the configuration, the router’s main DC power input (red A+ wire) must be connected through an in-line fuse to unswitched vehicle DC power. The red wire must be connected to raw battery power (positive battery terminal) via the supplied fuse.
- It is important to use the proper crimp tool for crimping any terminals or fuse holder

**Power On/Off Using Vehicle Ignition**
- For the mobile router to be powered on and off with the vehicle’s ignition, the ignition sense wire needs to be connected to one of switched power sources, typically known as accessory power.
- In this configuration, the white or blue wire connects to a switched power source, typically identified as “Accessory” power, that switches on and off with the vehicle’s ignition switch/key. The accessory source is normally found in the vehicle’s interior fuse block.
- The source chosen should have nothing to do with the vehicle’s safety systems. Refer to the vehicle’s owner’s manual when choosing an appropriate accessory source.

**Ground and Return Location and Considerations**
- Care should be taken to ensure the location chosen is truly to vehicle ground.
- The location chosen should not be in an area that is prone to moisture retention.
- Ensure that the location will protect the terminal from being bumped and allow the connection to loosen.
- The location must allow a through bolt with a nut and lock washer or be at a factory ground.
- Chose a location that will allow the ground lead to be as short as possible.

**Antenna Mounting Considerations**
- Antenna location must be chosen based on the installation instructions and in consideration of other items installed on the vehicle’s roof.
- There must be at least a 24” separation between the antenna and any other roof mounted equipment (see Figure 26).
- If the antenna being used requires a ground plane, the location chosen must provide an acceptable ground.
Data, Antenna, and Power Cable Routing Considerations

- Cables should not be routed under vehicle carpeting where the feet of occupants’ rest.
- Plan the cable runs so as to protect the cables from chafing, crushing, moisture, or overheating.
- Routing under the dash should not interfere with, or pass through, the steering column, brake pedal, clutch pedal, or the accelerator mechanisms.
- Carefully chose the location where the wiring will exit the passenger compartment and enter the engine compartment.

Splicing Requirements

Splicing the 12 VDC (A+) wire is not allowed. For other wires, if a splice must be installed such as to extend the wire, the following requirements must be followed:

- When wire is routed through hidden locations such as door jams, under the dash or, otherwise hidden from view use a solid run.
- Any splice installed must be visible to future service technicians. The best way to accomplish this is to cut off the wire back near the equipment connector and splice on a new wire.
- The splice wire used must have insulation rated for use in an engine compartment.
- Estimate the length of the run and determine required wire gauge.
- The gauge of the wire used must be based on the length of cable run for a load of approximately 5 Amps and maximum allowable voltage drop of 200 mV at peak load. If larger gauge wire is not required the same gauge shall be used, but never a smaller gauge.
- When splicing a wire that could be exposed to moisture use a butt splice encased within heat shrink tubing to seal the connection.

Battery Connection Requirements

- The 12 VDC power source should be the battery if possible. Other sources may be used if a battery connection is not available or feasible. Acceptable sources are the input to the main relay/fuse panel in the engine compartment, other main 12 VDC terminal, or installation of an auxiliary fuse block.
- An inline fuse holder is used for the mobile router to protect the equipment and the vehicle from a possible short circuit or excessive current draw. The fuse amperage must be according to the manufacturer's specifications. The fuse holder is water resistant to protect the fuse from the elements and avoid the possibility of corrosion. For optimum safety, the fuse should be placed as close to the battery as possible.
- If an auxiliary fuse block is being installed, the conductor used to connect it to 12 VDC should be gauged large enough to support the current flow of all the equipment that is fed by the block. The gauge of the cable to be used must be based on the length of cable run for a load of approximately 40 Amps and maximum allowable voltage drop.
of 200mV at peak load. In most cases this conductor consists of #6 AWG or #8 AWG wire. The insulation of this conductor must be properly rated for engine compartments. An inline fuse holder must be installed on this wire near the battery. The fuse holder must be water resistant and the amperage of the fuse installed should be rated large enough to handle the total current flow of the block. In most cases the fuse rating is 40 or 50 amps.

- The test vehicle utilized by AMK Services for this testing used a 60-amp fuse for the load which included a power inverter, a Raspberry Pi (Linux device), and multiple laptop at times. All needed equipment would need to be load rated and the fuse and wiring would need to be matched correctly to safely handle the load.

**Figure 27  Test Vehicle Battery Connections**

<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>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>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>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>